MOSCOW FORENSICS DAY '25



VALERIA VAKHRUSHINA

"DICTIONARY OR MASK: HOW MK BRUTE FORCE WORKS"

MKO SYSTEMS LLC

MFD

VALERIA VAKHRUSHINA

Head of MK Brute Force development
MKO Systems LLC





MK BRUTE FORCE

THE MOST COMMON PASSWORDS

PASSWORD	TIME TO CRACK	TIMES USED
123456	less than a second	4,524,867
admin	less than a second	4,008,850
12345678	less than a second	1,371,152
123456789	less than a second	1,213,047
1234	less than a second	969,811
12345	less than a second	728,414
password	less than a second	710,321

https://softmart.by/news/samyie-chasto-ispolzuemyie-paroli-v-mire

THE MOST REPEATED PATTERNS IN PASSWORDS

1qaz2wsx

1qazxsw

1qaz2wsx

2wsx3edc

1q2w3e4r

zaq12wsx

20

MOST USED PASSWORDS IN RUSSIA

https://ru.safetydetectives.com/blog/most-hacked-passwords-in-the-world-ru/

password1	medvedev
gfhjkm (password)	vputin
1q2w3e4r5t6y	soto4ka
Hjccnz (Russia)	leningrad
rossia	qwerty
cyfqgth (sniper)	baltika9
putin01	laikos
habibufc	zxcvbnm
russia2018	eskander

Home phone number

Mobile phone number

PASSWORD AS A WAY TO PROTECT DATA

- Change your passwords regularly
- A password must be at least 20 characters long and include digits, upper- and lowercase letters and special characters
- Avoid using data such as birthdays, names or common words
- Do not use the same password for several sites
- **SWITCH TO KEYS THAT UNLOCK A DEVICE OR AN APP WITH A FINGERPRINT, A FACE SCAN OR A PIN**

CHOOSE A METHOD:

- Dictionary
- Mask

Dictionary

A dictionary attack uses a pre-built list of possible passwords.

Sources: leaks, wordlist generators, OSINT, internal data, AI-based password generators and so on

Dictionary based on personal data

A dictionary generated from the data obtained in the extraction, including significant dates, full names and so on

Mask

26 Latin letters (uppercase) + 26 Latin letters (lowercase) + 10 digits + special characters

Mask

A 10-character password
Lowercase

+ + Uppercase

3,656+
trillion

possible combinations

Mask

- ?l = abcdefghijklmnopqrstuvwxyz
- ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?d = 0123456789
- ?h = 0123456789abcdef
- ?H = 0123456789ABCDEF
- ?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
- ?a = ?l?u?d?s

name**?a?a?a?a**

?a?a?a?aname

BUT THE TIME FOR CRACKING IS LIMITED

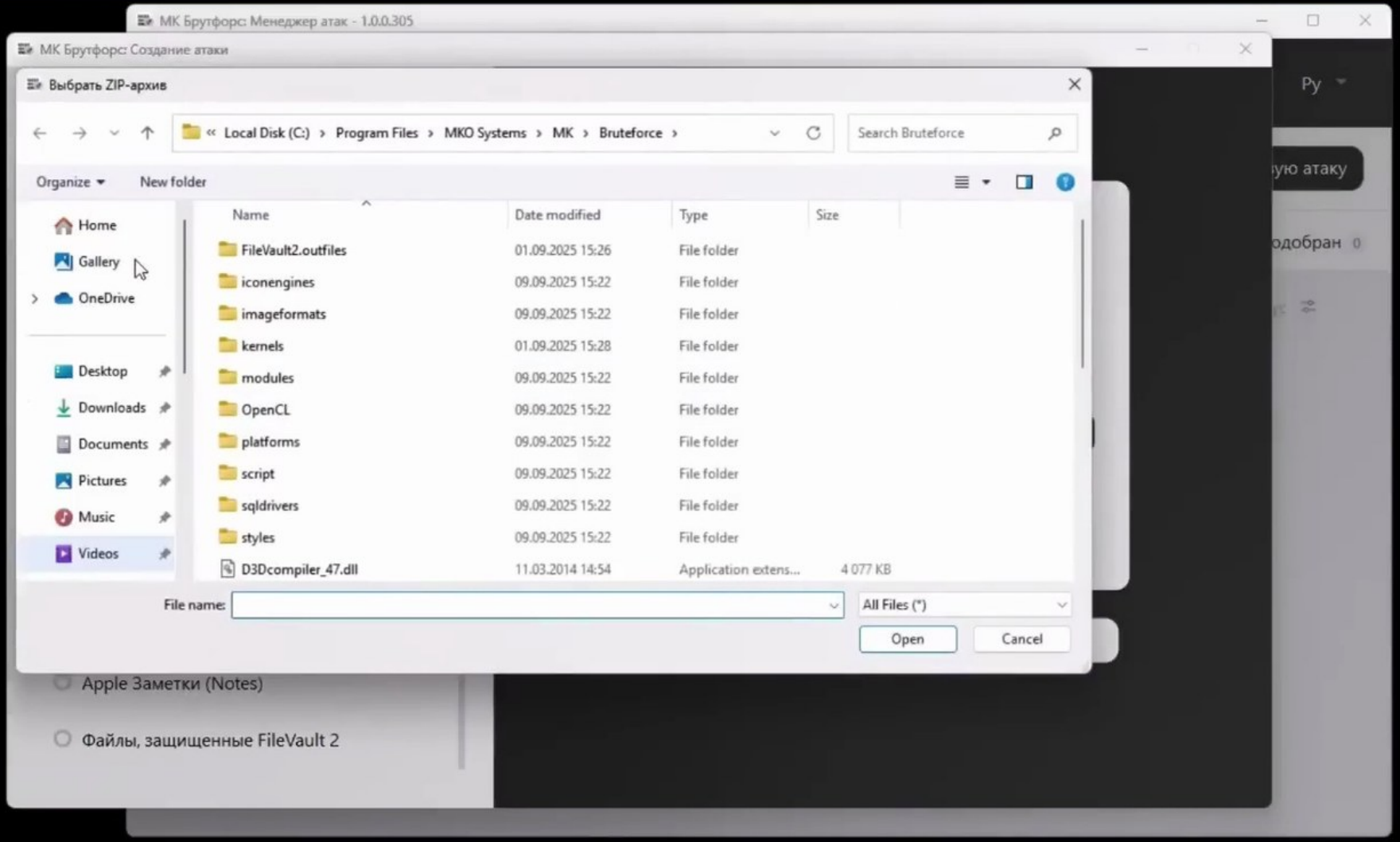
GPU/CPU power

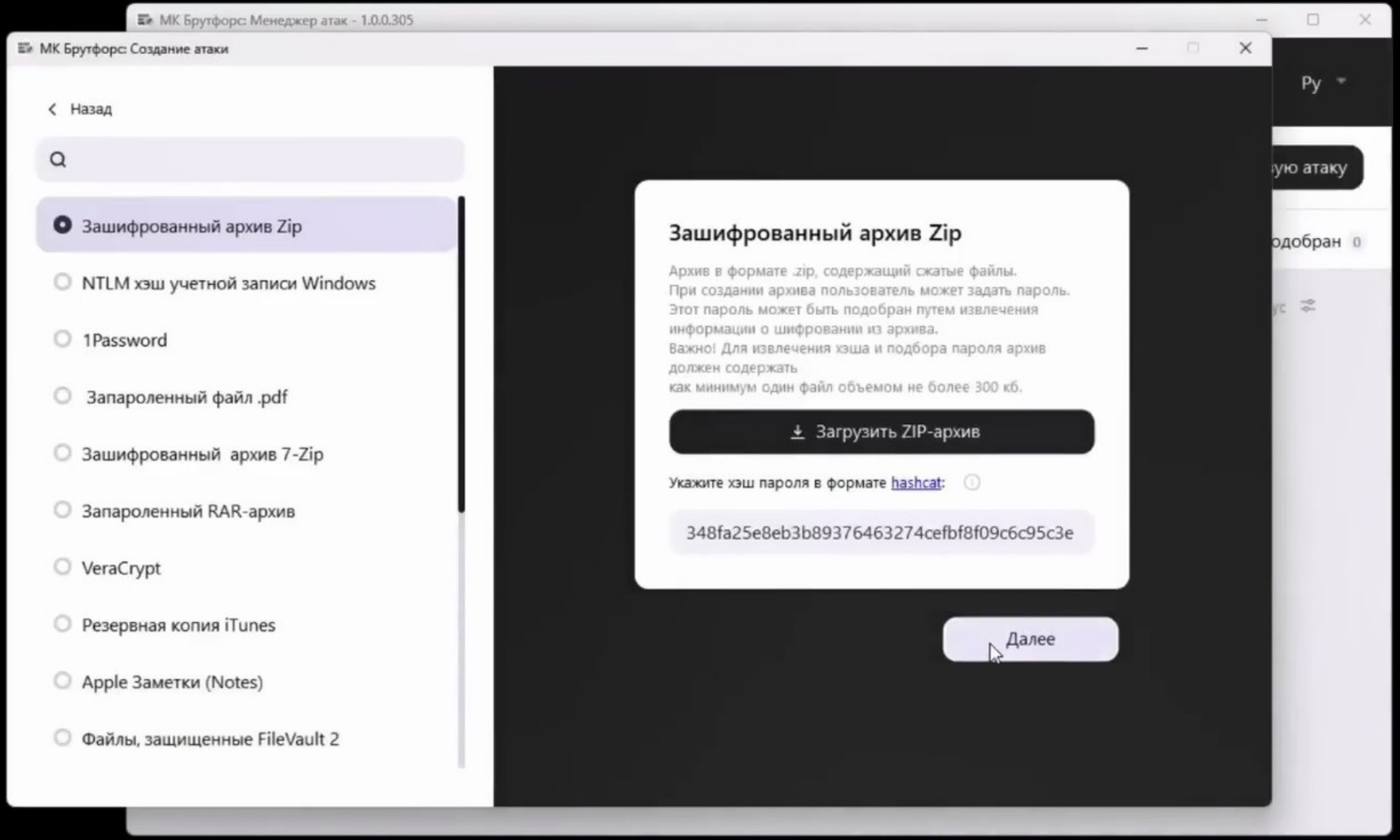
Distributed cracking

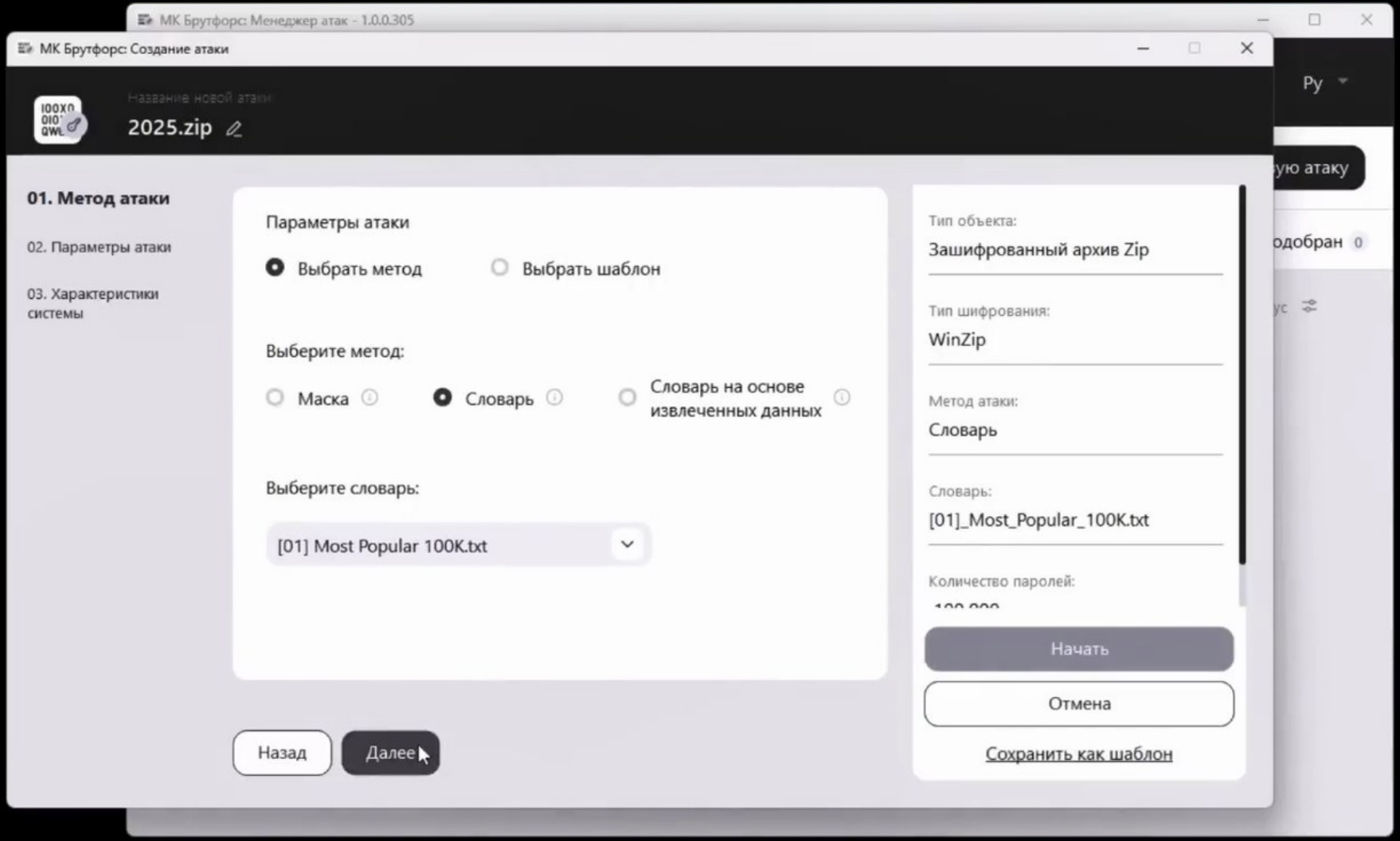
Cracking is not brute force for the sake of brute force.

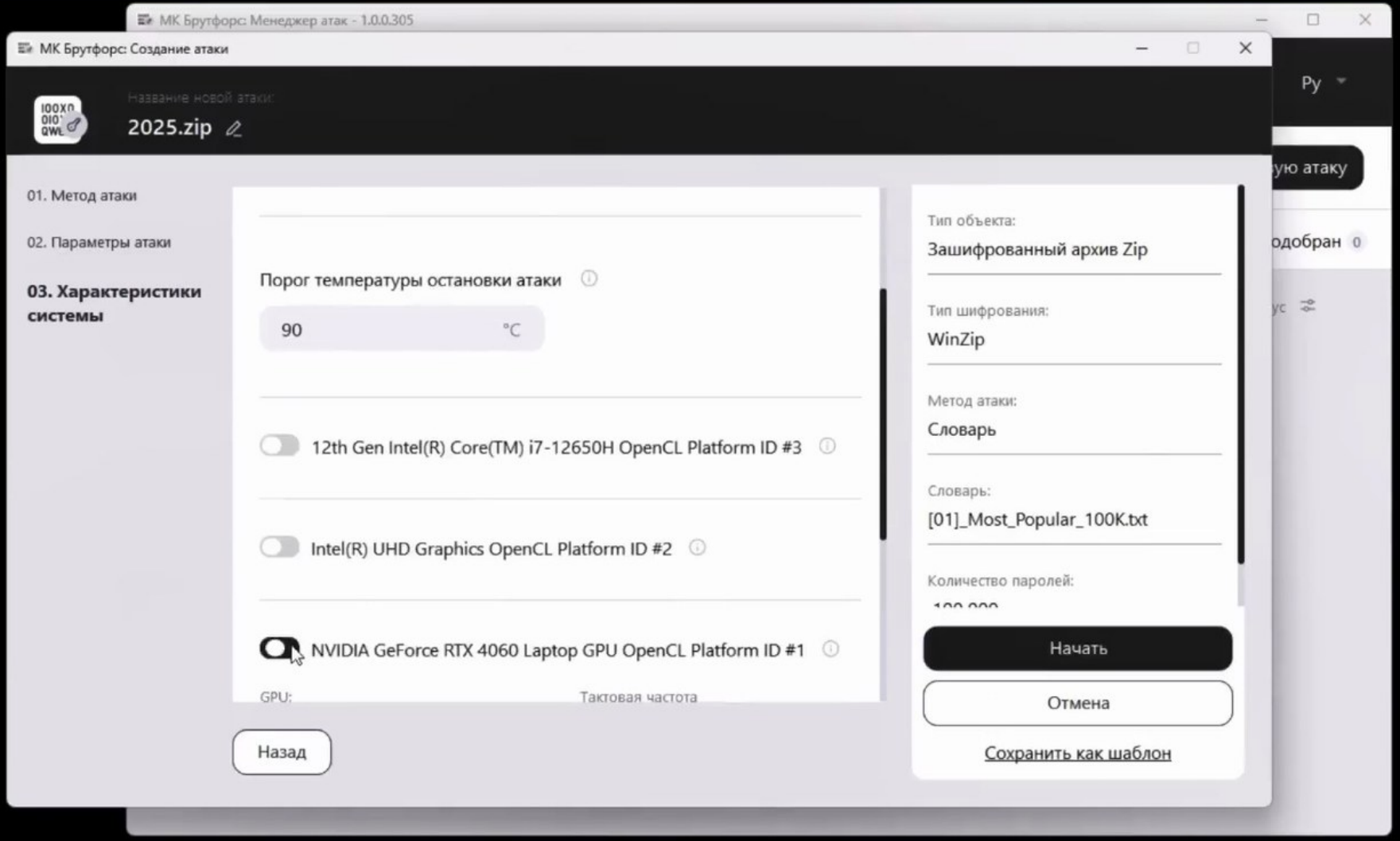
It is part of an investigation.

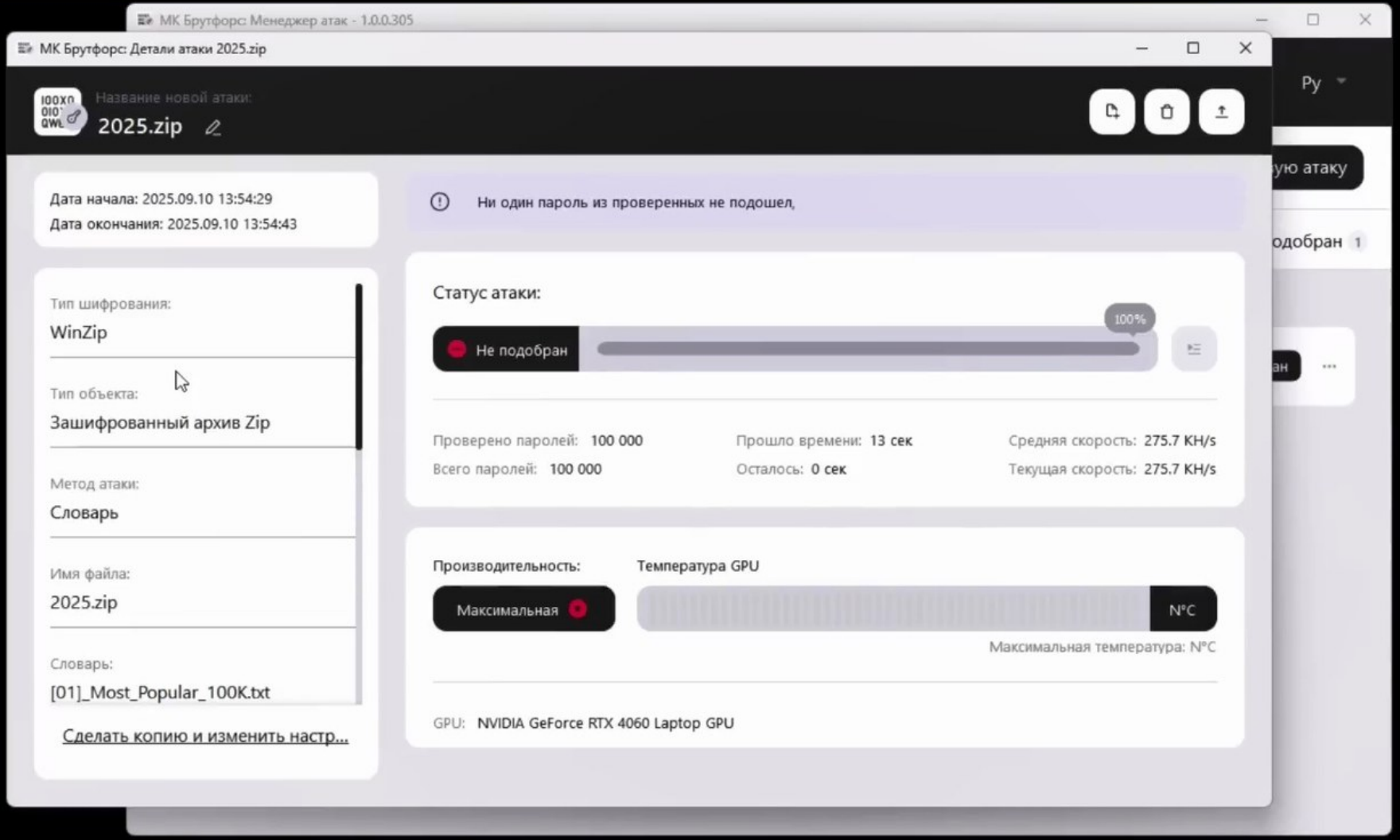
Meaningful hypotheses make it many times more effective.

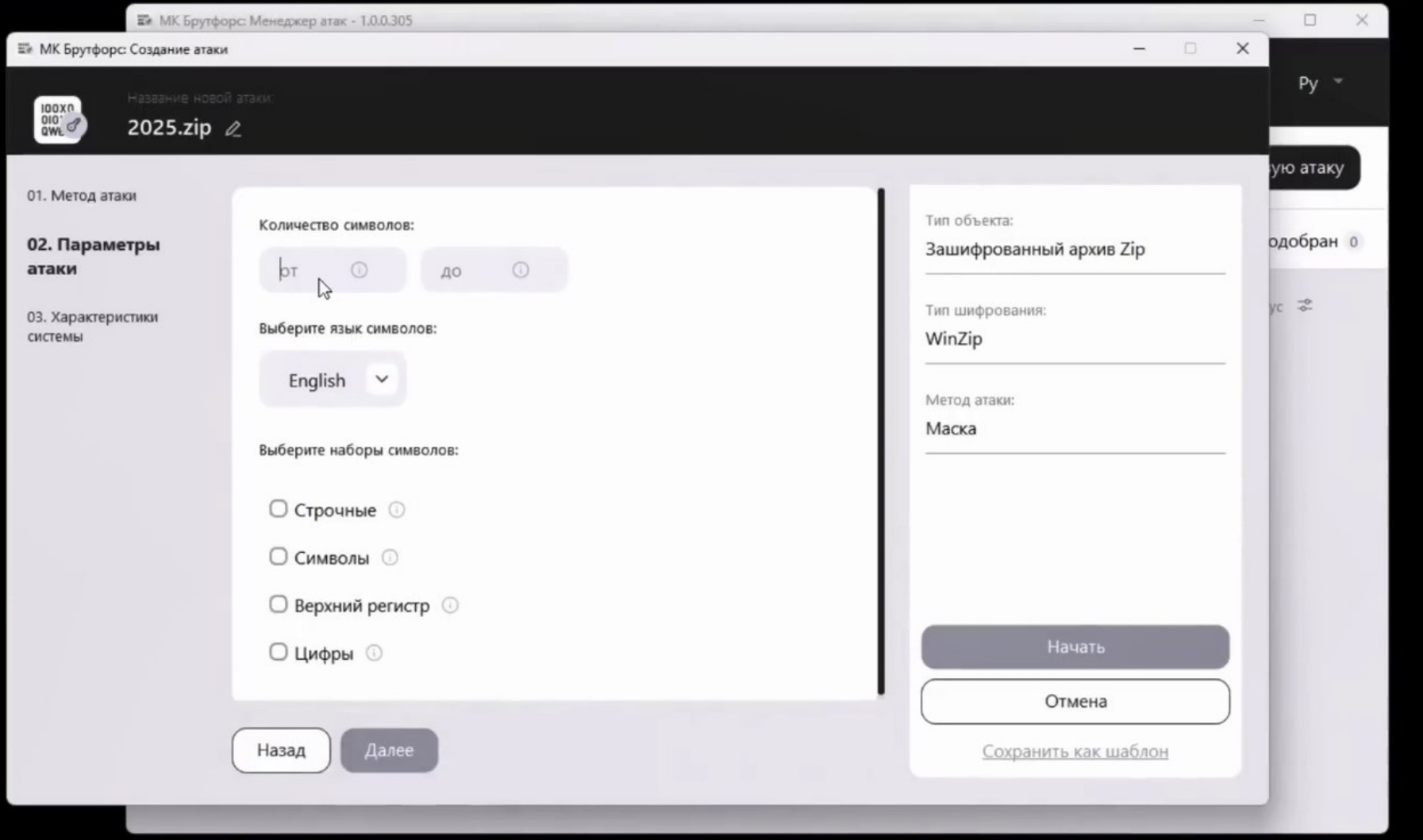

МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Выбрать ZIP-архив
« Local Disk (C:) › Program Files › MKO Systems › MK › Bruteforce ›
Search Bruteforce
Organize
New folder
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
Name
Date modified
Type
Size
FileVault2.outfiles 01.09.2025 15:26 File folder
iconengines 09.09.2025 15:22 File folder
imageformats 09.09.2025 15:22 File folder
kernels 01.09.2025 15:28 File folder
modules 09.09.2025 15:22 File folder
OpenCL 09.09.2025 15:22 File folder
platforms 09.09.2025 15:22 File folder
script 09.09.2025 15:22 File folder
sqldrivers 09.09.2025 15:22 File folder
styles 09.09.2025 15:22 File folder
D3Dcompiler_47.dll 11.03.2014 14:54 Application extens... 4 077 KB
File name:
All Files (*)
Open
Cancel
Apple Заметки (Notes)
Файлы, защищенные FileVault 2

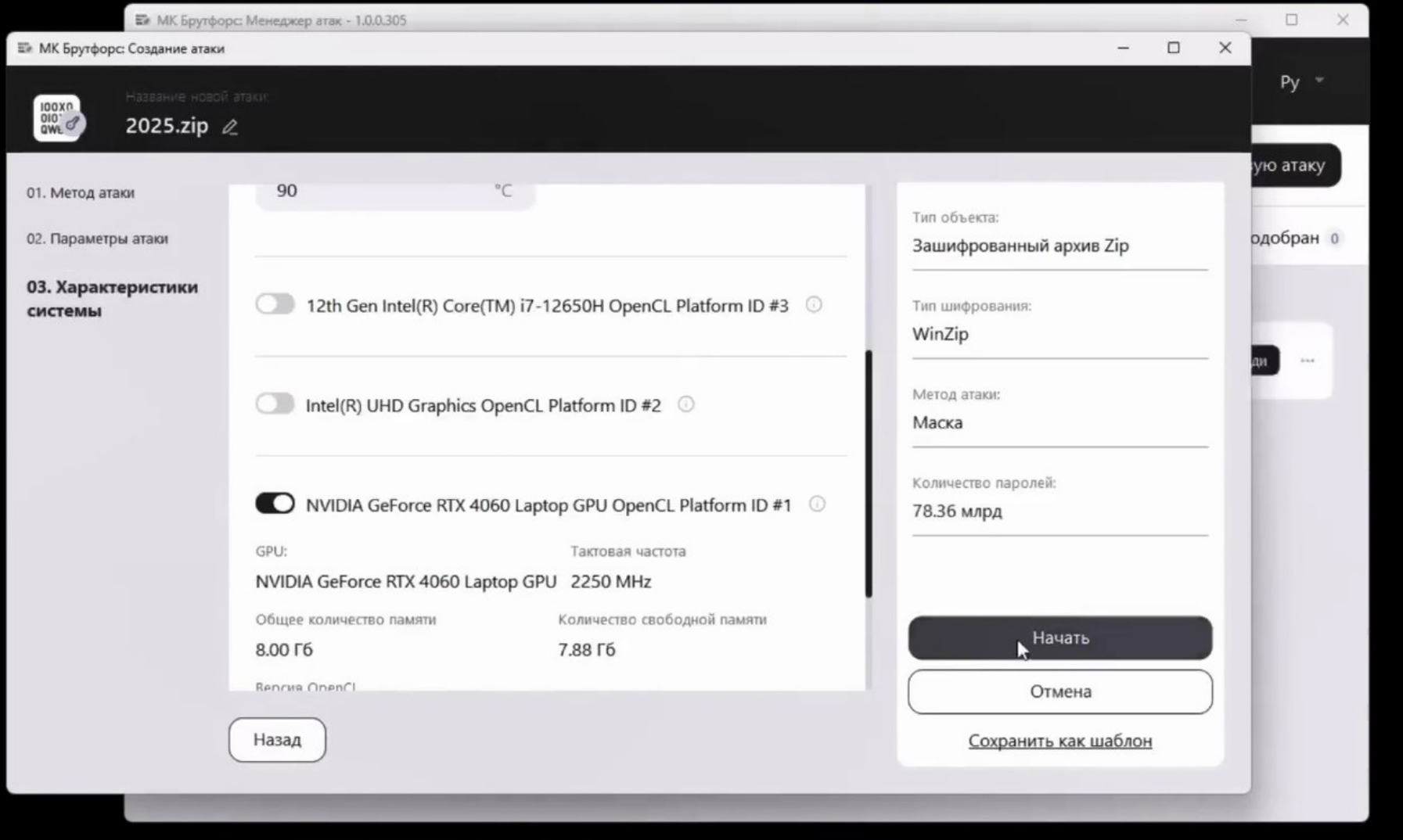

МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Назад
Зашифрованный архив Zip
NTLM хэш учетной записи Windows
1Password
Запароленный файл .pdf
Зашифрованный архив 7-Zip
Запароленный RAR-архив
VeraCrypt
Резервная копия iTunes
Apple Заметки (Notes)
Файлы, защищенные FileVault 2
Зашифрованный архив Zip
Архив в формате .zip, содержащий сжатые файлы.
При создании архива пользователь может задать пароль.
Этот пароль может быть подобран путем извлечения информации о шифровании из архива.
Важно! Для извлечения хэша и подбора пароля архив должен содержать
как минимум один файл объемом не более 300 кб.
Загрузить ZIP-архив
Укажите хэш пароля в формате hashcat:
348fa25e8eb3b89376463274cefbf8f09c6c95c3e
Далее
Ру
ую атаку
одобран 0

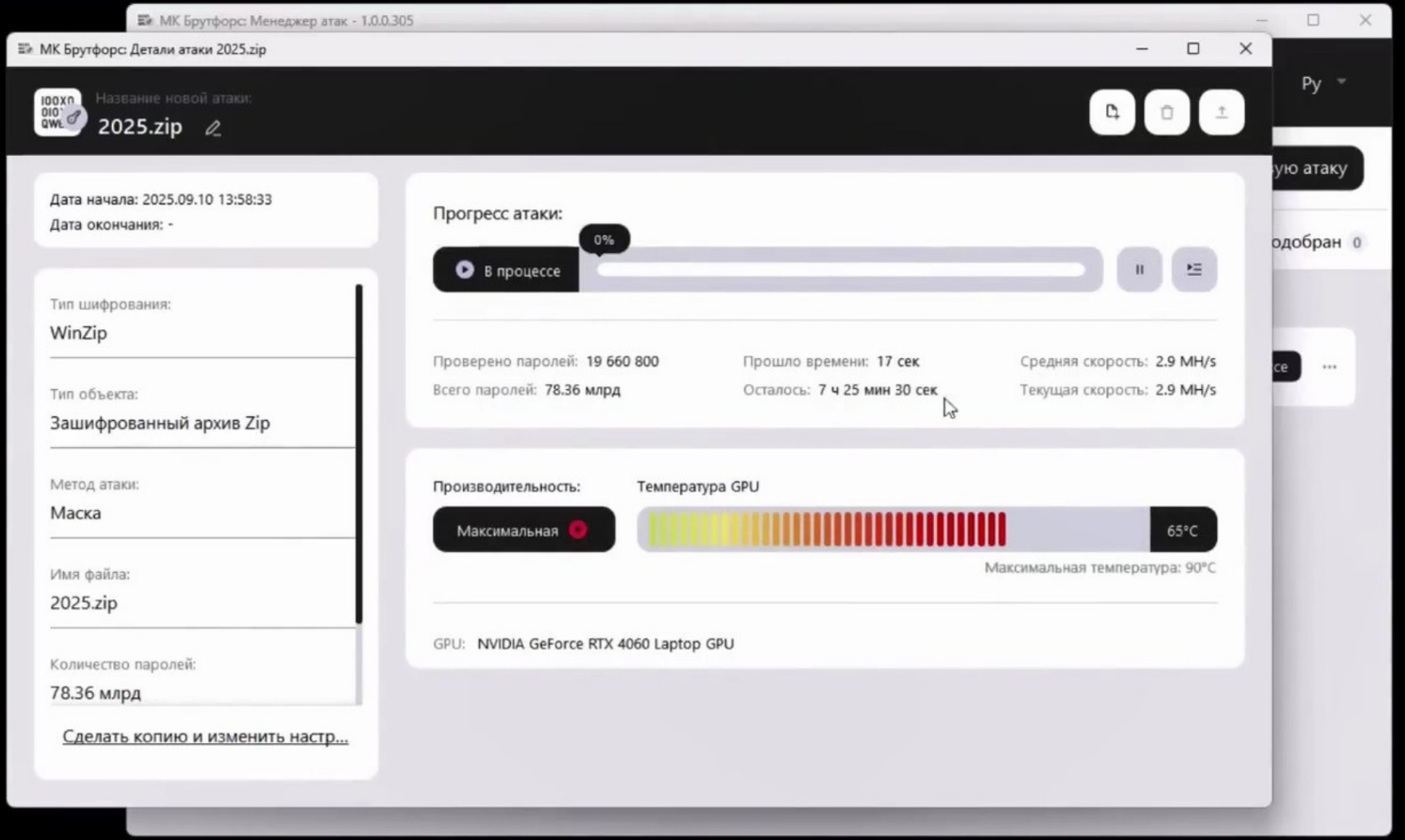

МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Название новой атаки
2025.zip
01. Метод атаки
02. Параметры атаки
03. Характеристики системы
Параметры атаки
Выбрать метод
Выбрать шаблон
Выберите метод:
Маска
Словарь
Словарь на основе извлеченных данных
Выберите словарь:
[01] Most Popular 100K.txt
Назад
Далее
Тип объекта:
Зашифрованный архив Zip
Тип шифрования:
WinZip
Метод атаки:
Словарь
Словарь:
[01]_Most_Popular_100K.txt
Количество паролей:
Начать
Отмена
Сохранить как шаблон
Ру
ую атаку
одобран 0

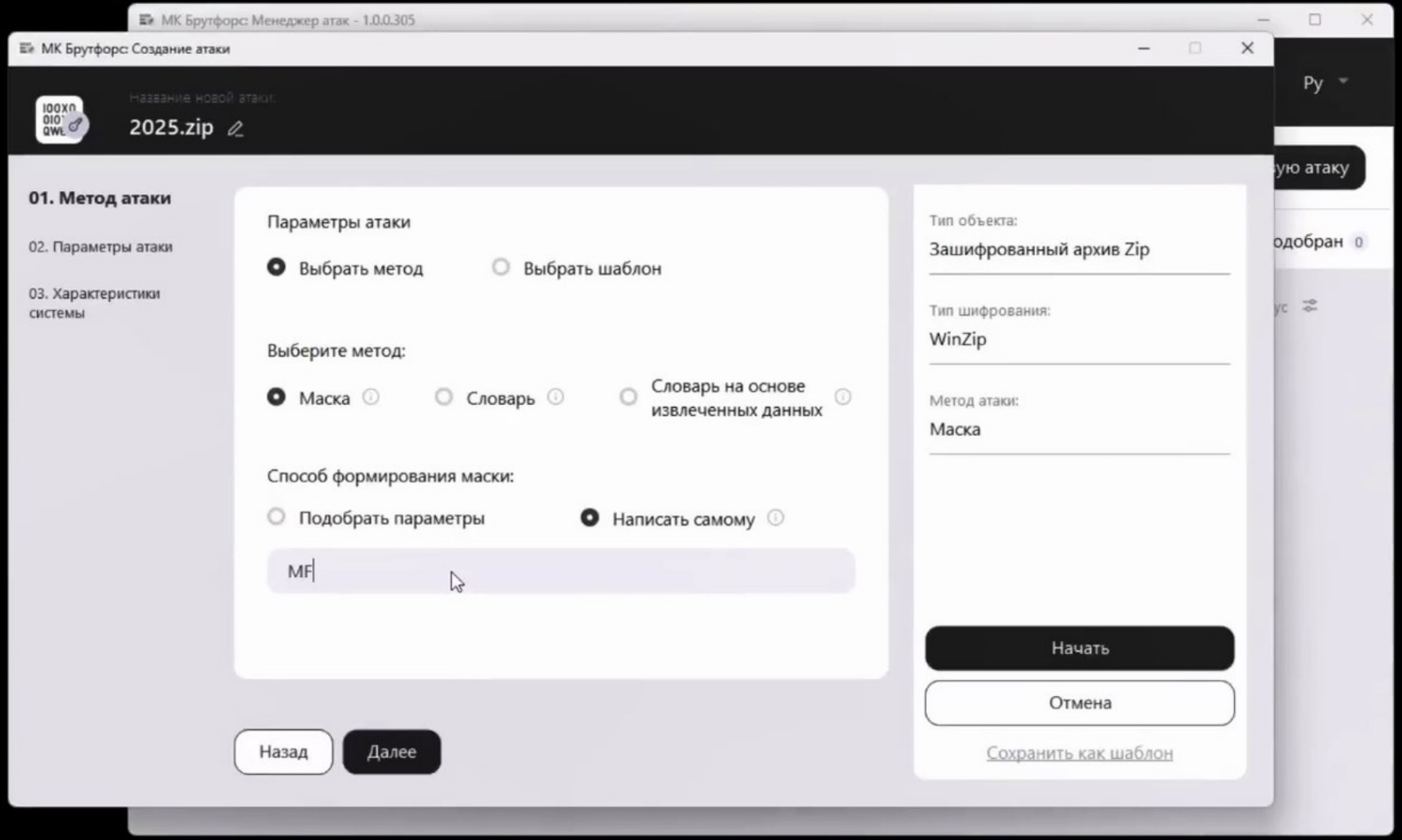

МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Название новой атаки:
2025.zip
01. Метод атаки
02. Параметры атаки
03. Характеристики системы
Порог температуры остановки атаки
90
°C
12th Gen Intel(R) Core(TM) i7-12650H OpenCL Platform ID #3
Intel(R) UHD Graphics OpenCL Platform ID #2
NVIDIA GeForce RTX 4060 Laptop GPU OpenCL Platform ID #1
GPU:
Тактовая частота
Назад
Тип объекта:
Зашифрованный архив Zip
Тип шифрования:
WinZip
Метод атаки:
Словарь
Словарь:
[01]_Most_Popular_100K.txt
Количество паролей:
Начать
Отмена
Сохранить как шаблон
Ру
ую атаку
одобран 0

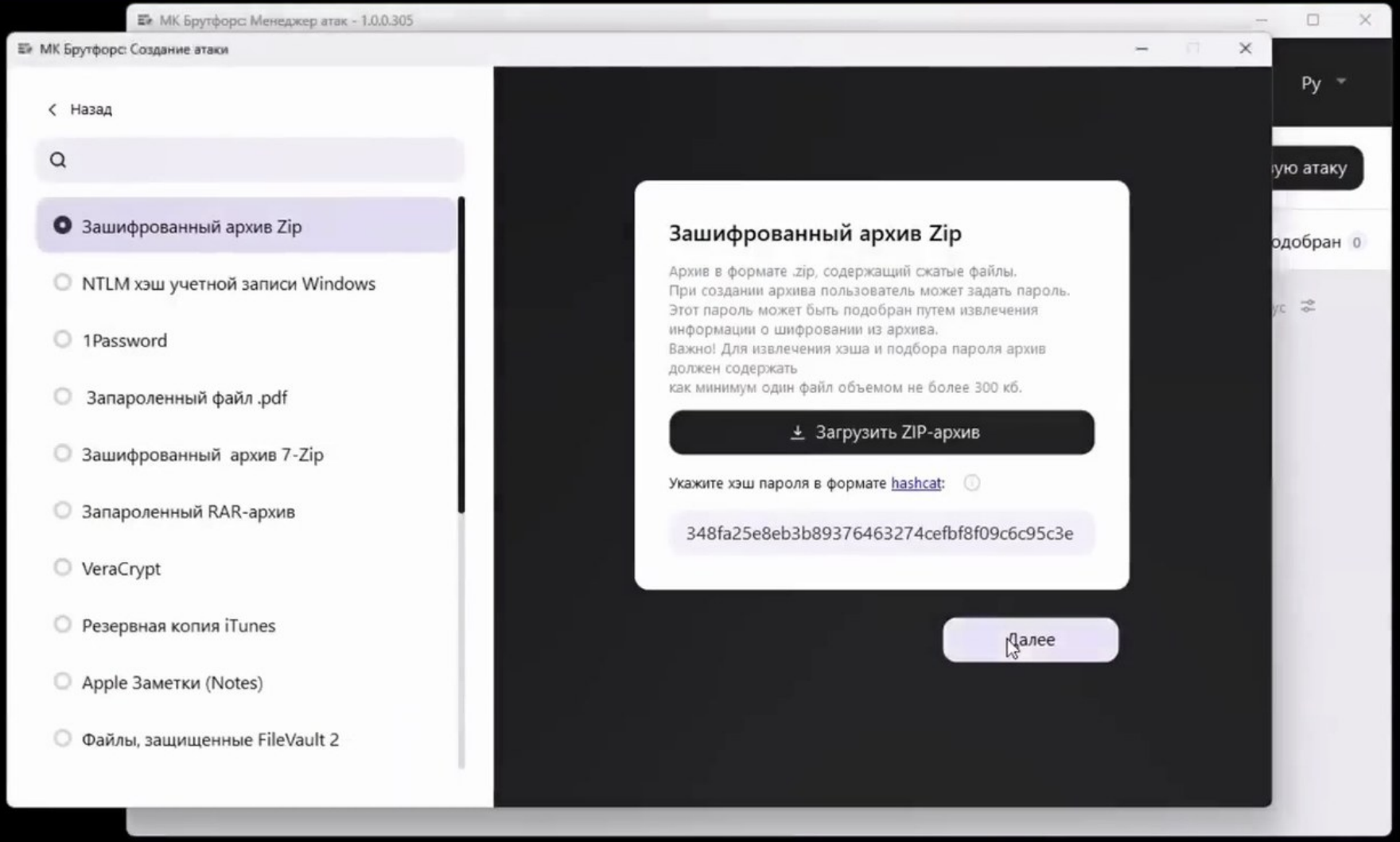

МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Детали атаки 2025.zip
Название новой атаки:
2025.zip
Дата начала: 2025.09.10 13:54:29
Дата окончания: 2025.09.10 13:54:43
Ни один пароль из проверенных не подошел,
Тип шифрования:
WinZip
Тип объекта:
Зашифрованный архив Zip
Метод атаки:
Словарь
Имя файла:
2025.zip
Словарь:
[01]_Most_Popular_100K.txt
Сделать копию и изменить настр...
Статус атаки:
Не подобран
100%
Проверено паролей: 100 000
Всего паролей: 100 000
Прошло времени: 13 сек
Осталось: 0 сек
Средняя скорость: 275.7 KH/s
Текущая скорость: 275.7 KH/s
Производительность:
Максимальная
Температура GPU
N°C
Максимальная температура: N°C
GPU: NVIDIA GeForce RTX 4060 Laptop GPU
Ру
ую атаку
одобран 1

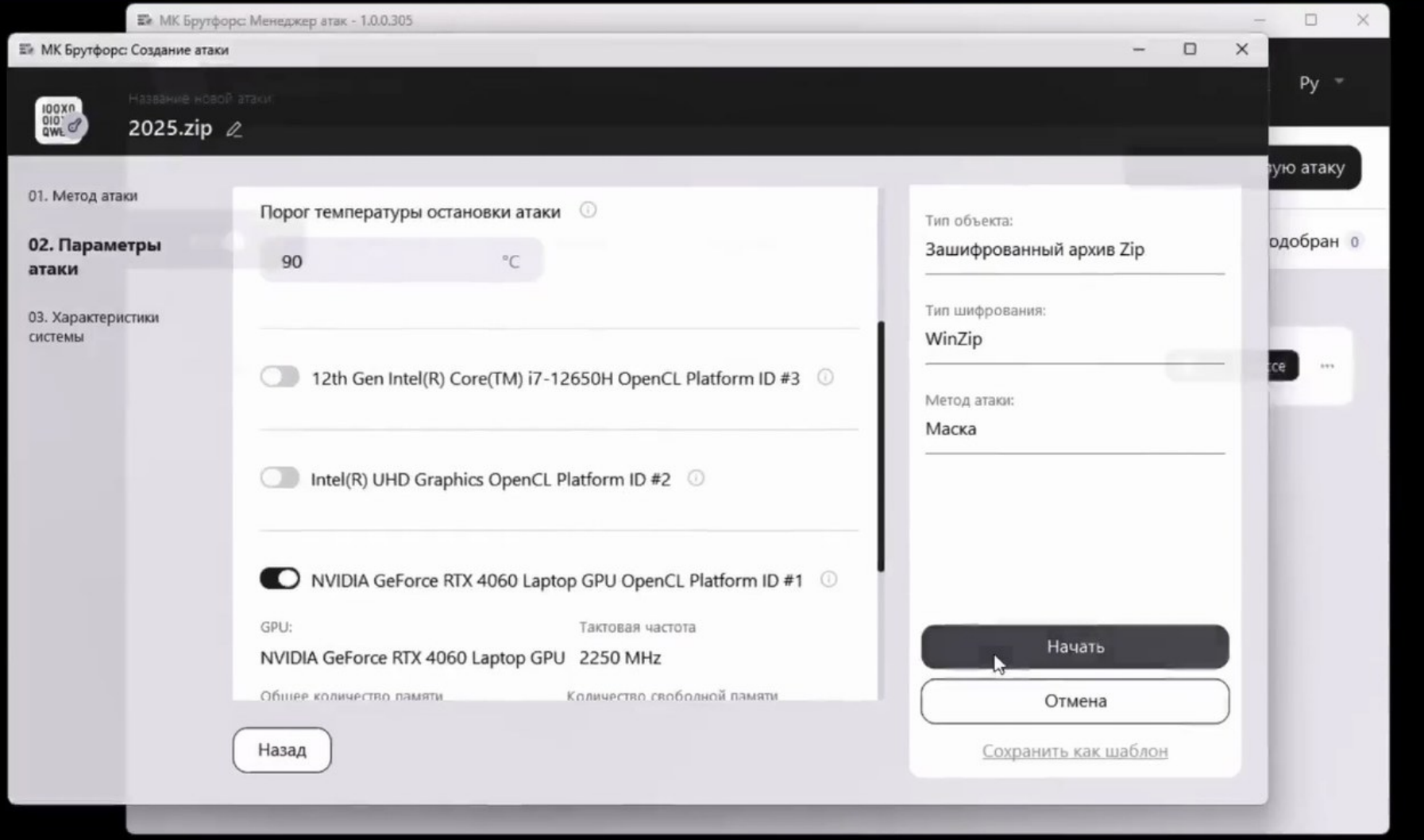

МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Название новой атаки:
2025.zip
01. Метод атаки
02. Параметры атаки
03. Характеристики системы
Количество символов:
от
до
Выберите язык символов:
English
Выберите наборы символов:
Строчные
Символы
Верхний регистр
Цифры
Назад
Далее
Тип объекта:
Зашифрованный архив Zip
Тип шифрования:
WinZip
Метод атаки:
Маска
Начать
Отмена
Сохранить как шаблон
Ру
ую атаку
одобран 0


МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Название новой атаки:
2025.zip
01. Метод атаки
02. Параметры атаки
03. Характеристики системы
90 °C
12th Gen Intel(R) Core(TM) i7-12650H OpenCL Platform ID #3
Intel(R) UHD Graphics OpenCL Platform ID #2
NVIDIA GeForce RTX 4060 Laptop GPU OpenCL Platform ID #1
GPU:
NVIDIA GeForce RTX 4060 Laptop GPU
Тактовая частота
2250 MHz
Общее количество памяти
8.00 Гб
Количество свободной памяти
7.88 Гб
Версия OpenCL
Назад
Тип объекта:
Зашифрованный архив Zip
Тип шифрования:
WinZip
Метод атаки:
Маска
Количество паролей:
78.36 млрд
Начать
Отмена
Сохранить как шаблон


МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Детали атаки 2025.zip
Название новой атаки:
2025.zip
Дата начала: 2025.09.10 13:58:33
Дата окончания: -
Тип шифрования:
WinZip
Тип объекта:
Зашифрованный архив Zip
Метод атаки:
Маска
Имя файла:
2025.zip
Количество паролей:
78.36 млрд
Сделать копию и изменить настр...
Прогресс атаки:
0%
В процессе
Проверено паролей: 19 660 800
Всего паролей: 78.36 млрд
Прошло времени: 17 сек
Осталось: 7 ч 25 мин 30 сек
Средняя скорость: 2.9 MH/s
Текущая скорость: 2.9 MH/s
Производительность:
Максимальная
Температура GPU
65°C
Максимальная температура: 90°C
GPU: NVIDIA GeForce RTX 4060 Laptop GPU
Ру
ую атаку
одобран 0


МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Название новой атаки:
2025.zip
01. Метод атаки
02. Параметры атаки
03. Характеристики системы
Параметры атаки
Выбрать метод
Выбрать шаблон
Выберите метод:
Маска
Словарь
Словарь на основе извлеченных данных
Способ формирования маски:
Подобрать параметры
Написать самому
MF
Назад
Далее
Тип объекта:
Зашифрованный архив Zip
Тип шифрования:
WinZip
Метод атаки:
Маска
Начать
Отмена
Сохранить как шаблон
Ру
ую атаку
одобран 0


МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Назад
Зашифрованный архив Zip
NTLM хэш учетной записи Windows
1Password
Запароленный файл .pdf
Зашифрованный архив 7-Zip
Запароленный RAR-архив
VeraCrypt
Резервная копия iTunes
Apple Заметки (Notes)
Файлы, защищенные FileVault 2
Зашифрованный архив Zip
Архив в формате .zip, содержащий сжатые файлы.
При создании архива пользователь может задать пароль.
Этот пароль может быть подобран путем извлечения информации о шифровании из архива.
Важно! Для извлечения хэша и подбора пароля архив должен содержать
как минимум один файл объемом не более 300 кб.
Загрузить ZIP-архив
Укажите хэш пароля в формате hashcat:
348fa25e8eb3b89376463274cefbf8f09c6c95c3e
Далее
Ру
ую атаку
одобран 0


МК Брутфорс: Менеджер атак - 1.0.0.305
МК Брутфорс: Создание атаки
Название новой атаки
2025.zip
01. Метод атаки
02. Параметры атаки
03. Характеристики системы
Порог температуры остановки атаки
90
°C
12th Gen Intel(R) Core(TM) i7-12650H OpenCL Platform ID #3
Intel(R) UHD Graphics OpenCL Platform ID #2
NVIDIA GeForce RTX 4060 Laptop GPU OpenCL Platform ID #1
GPU:
NVIDIA GeForce RTX 4060 Laptop GPU
Тактовая частота
2250 MHz
Общее количество памяти
Количество свободной памяти
Назад
Тип объекта:
Зашифрованный архив Zip
Тип шифрования:
WinZip
Метод атаки:
Маска
Начать
Отмена
Сохранить как шаблон
Ру
ую атаку
одобран 0

FEATURES

The module makes it possible not only to crack the password to encrypted data, but also to extract the hash from some file types automatically, and it needs no special technical skills.

- Efficient password cracking for various kinds of encrypted data.
- Running attacks one after another until the password is found.
- Creating attacks that crack the password with various dictionaries and masks.
- An easy-to-use interface that lets you start quickly with no complex setup.

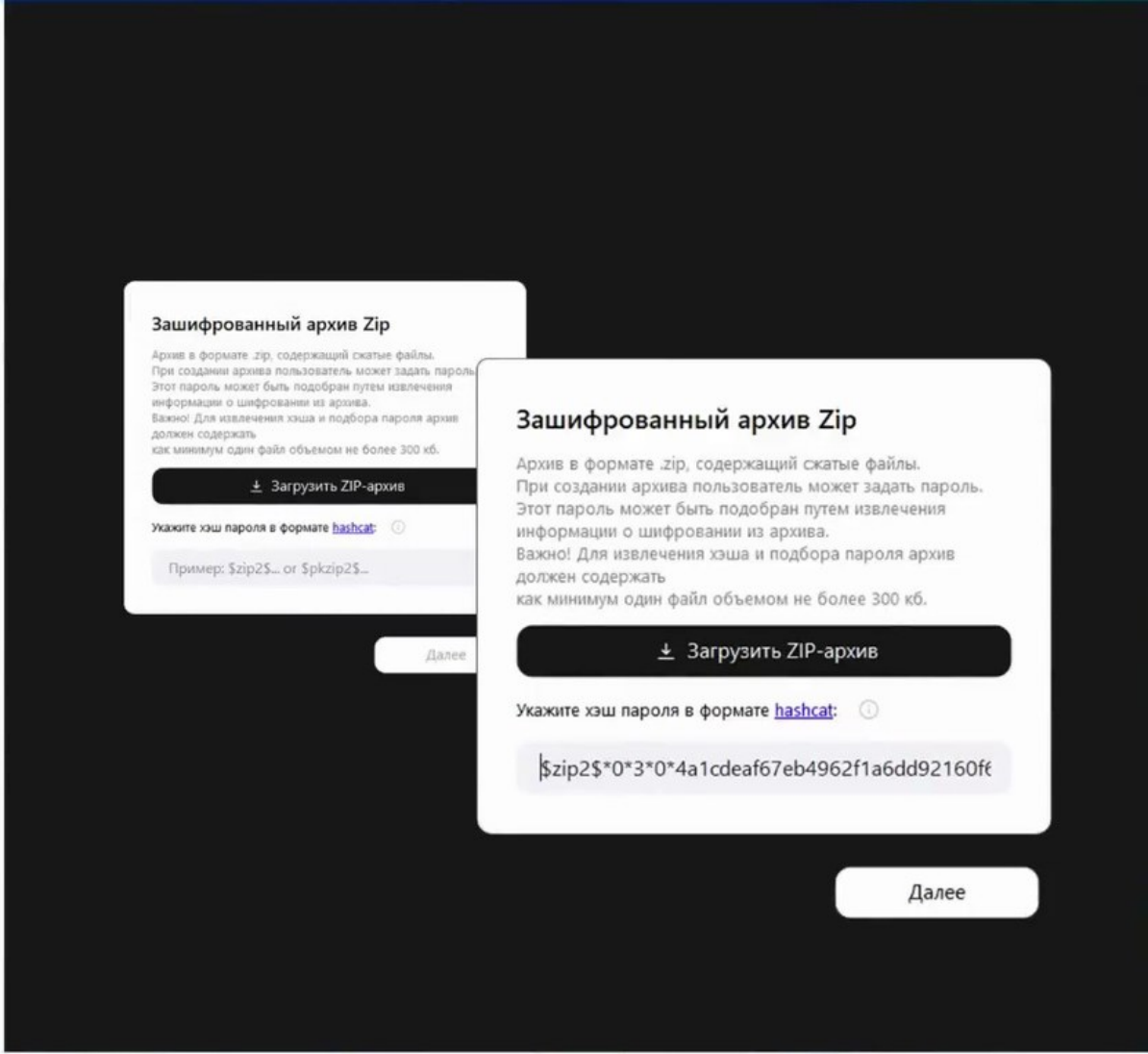
IT CAN CRACK

- Telegram Desktop passcode
- Android physical image
- 7 ZIP-архив
- RAR-архив
- VeraCrypt
- Apple Notes
- NTLM
- ZIP-архив
- Android backup
- Word, Excel, PowerPoint
- BitLocker
- iTunes backup
- Huawei HiSuite backup



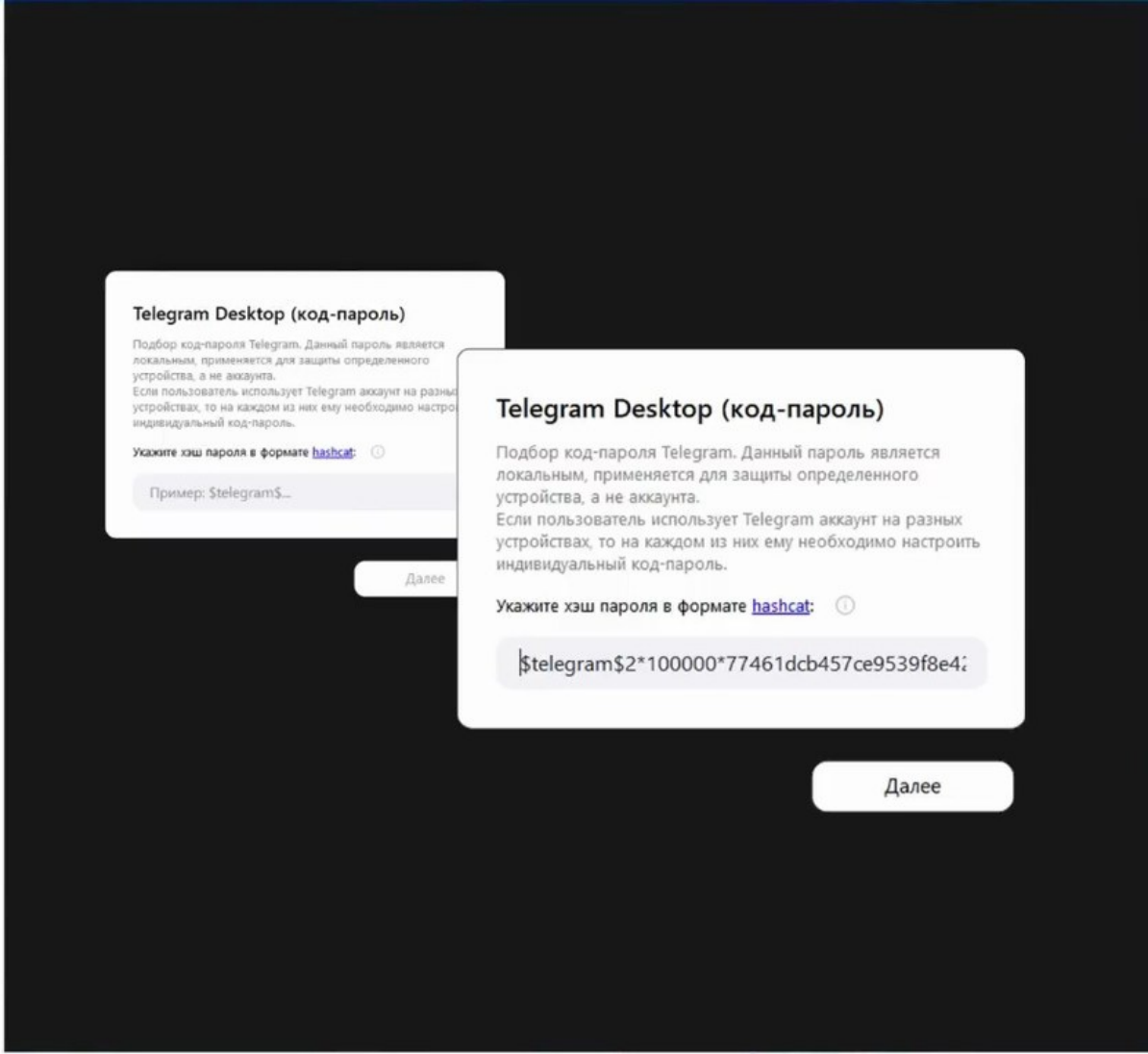
WHERE DO YOU GET THE HASH?

- (•) ZIP-архив
- ( ) 7 ZIP-архив
- ( ) RAR-архив
- ( ) Word, Excel, PowerPoint



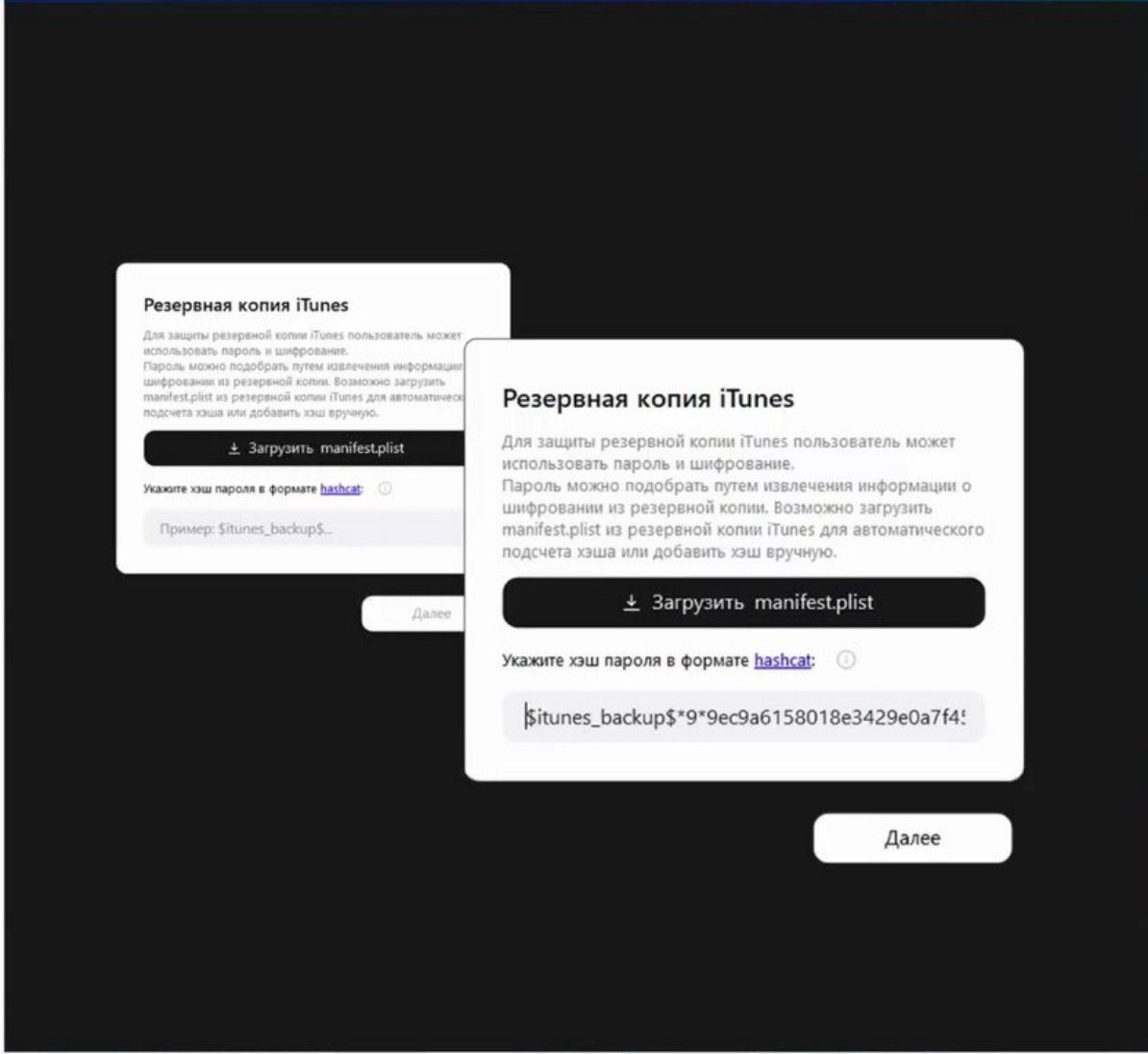
WHERE DO YOU GET THE HASH?

- Telegram Desktop passcode
- BitLocker
- NTLM



WHERE DO YOU GET THE HASH?

- iTunes backup
- Android backup
- Huawei HiSuite backup
- Android physical image
- Apple Notes



MK BRUTE FORCE

A product by MKO Systems for cracking passwords or hashed values of encrypted data.

To speed the cracking up, one or several GPUs/CPUs of the workstation can be put to work.



The module is built on hashcat, recognised as one of the best available password-cracking tools, with support for hundreds of hash types.

QUESTIONS?