МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Информационная безопасность

Работа 6: Криптография на практике: шифрование файлов и сообщений

Выполнил:

Румский Александр Максимович

Группа:

P3407

Преподаватель:

Маркина Татьяна Анатольевна

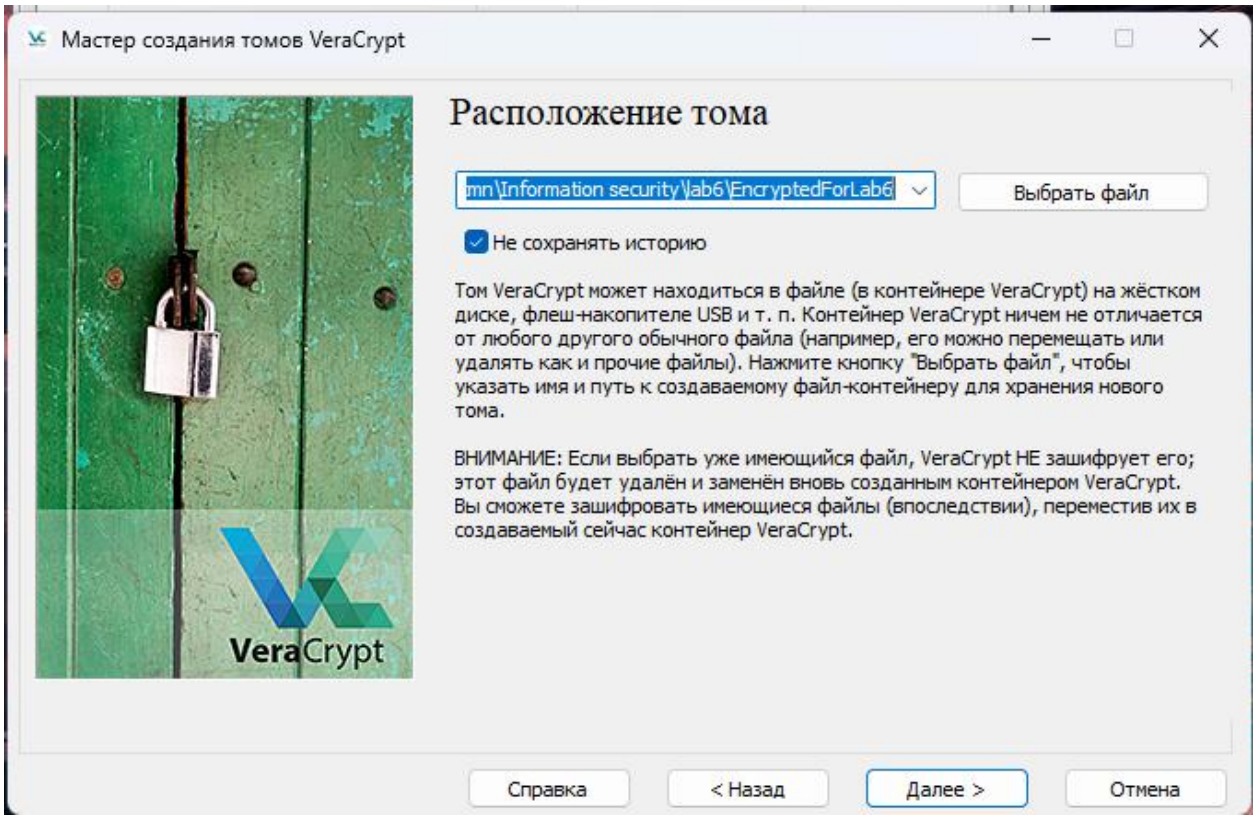
Санкт-Петербург, 2025 год

Содержание

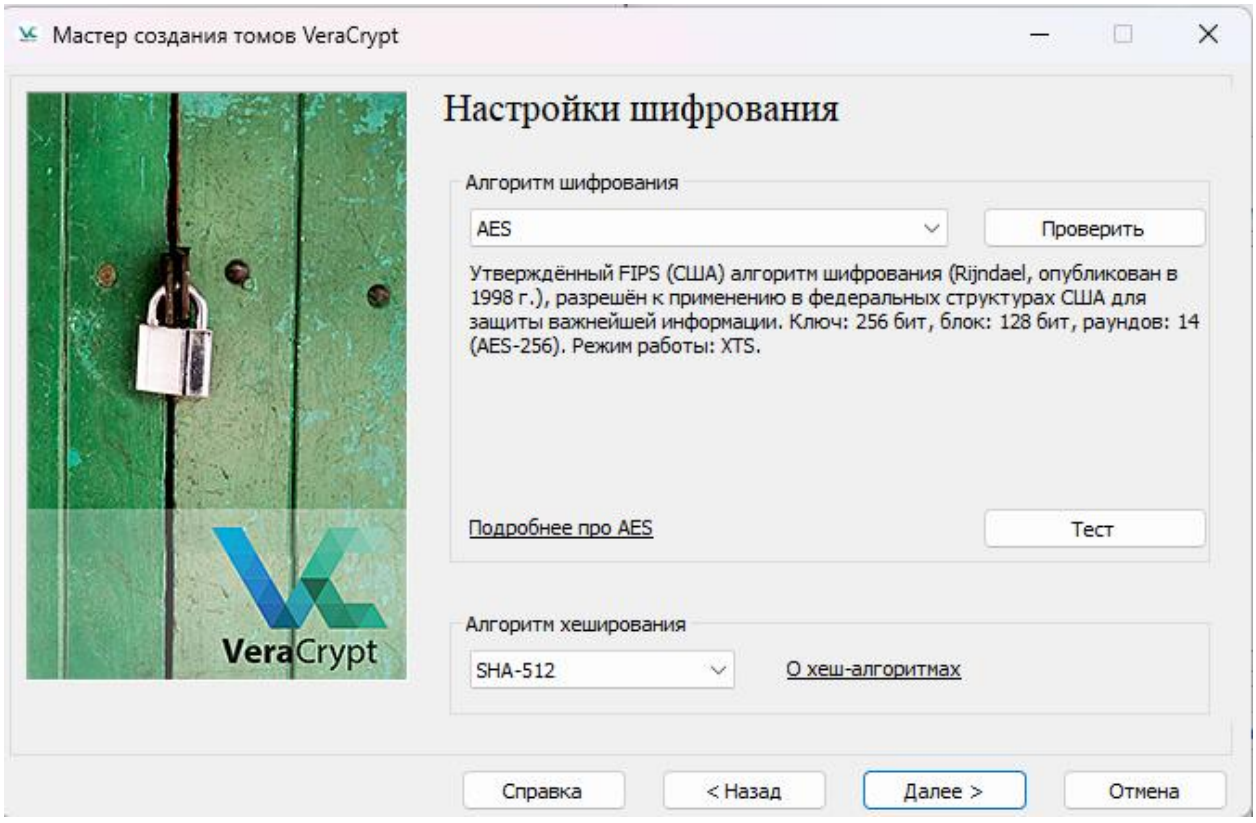
VeraCrypt 3
Создание контейнера 3
Выбор алгоритма шифрования 3
Определение размера тома 4
Шифрование 4
Монтирование тома для 5
Внесение файлов 6
Thunderbird 7
Генерация пары PGP ключей 8
Добавление PGP ключа 9
Разница между симметричным и асимметричным шифрованием 11

VeraCrypt

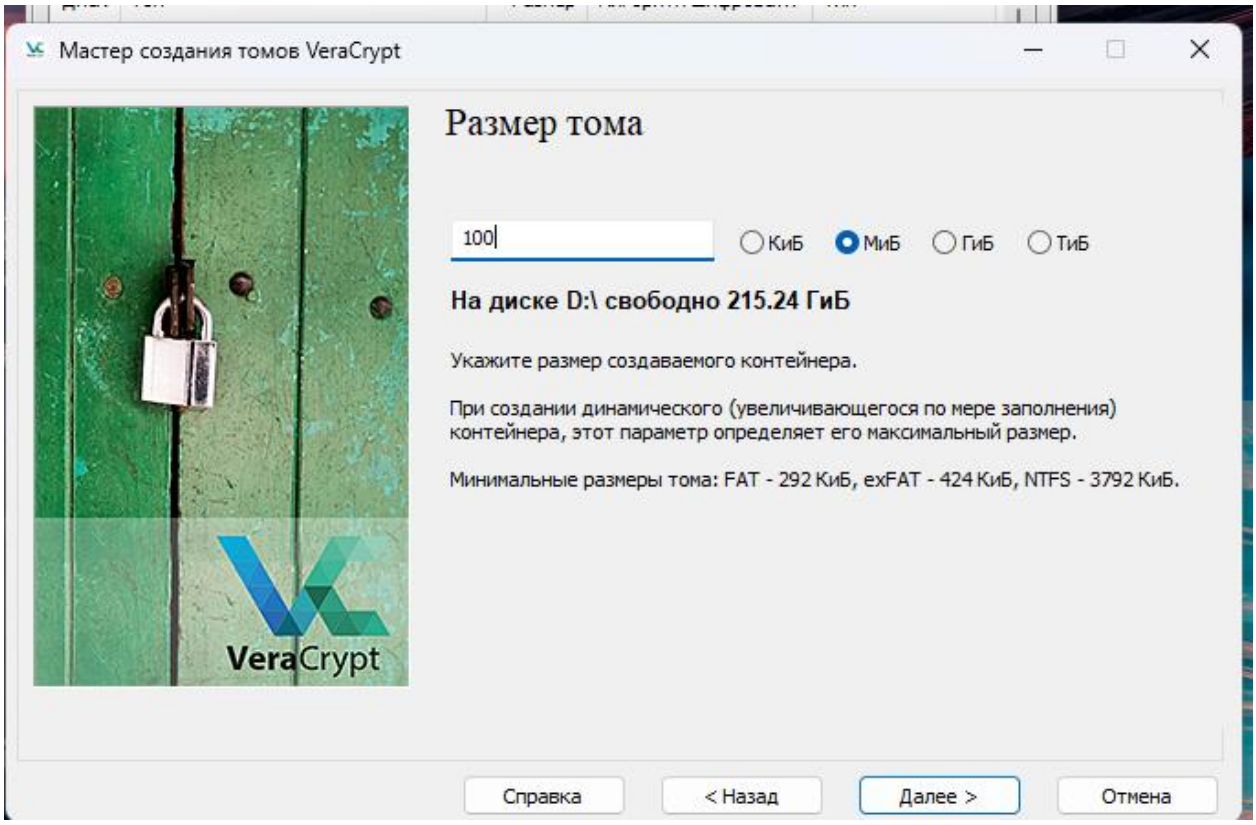
Создание контейнера



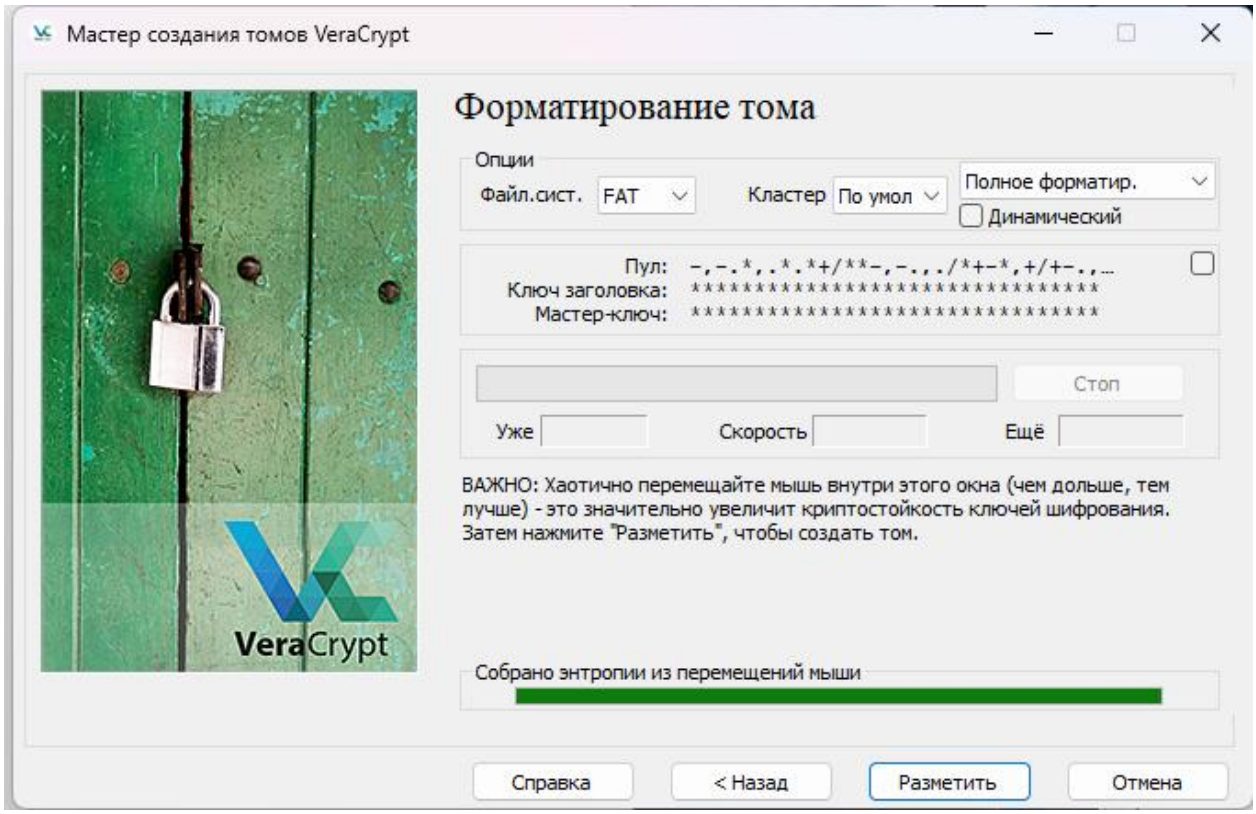
Выбор алгоритма шифрования



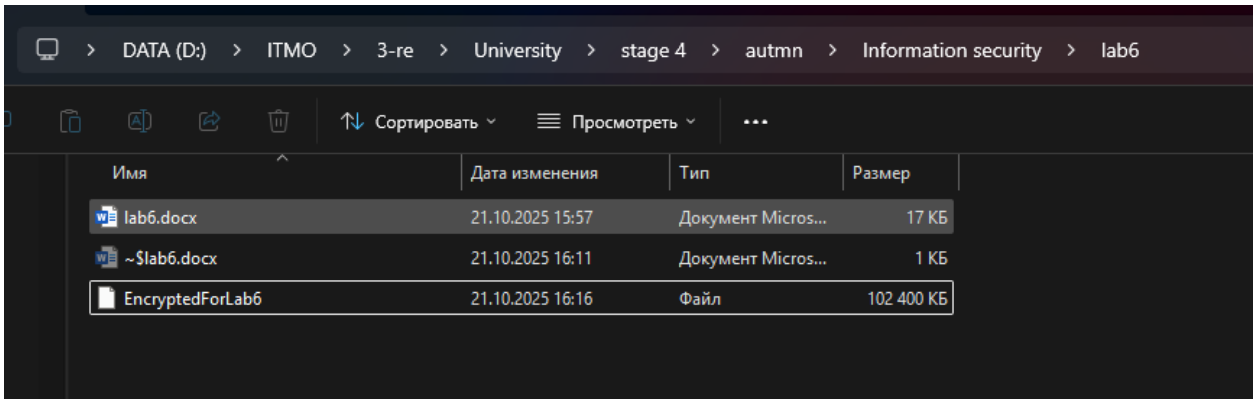
Определение размера тома

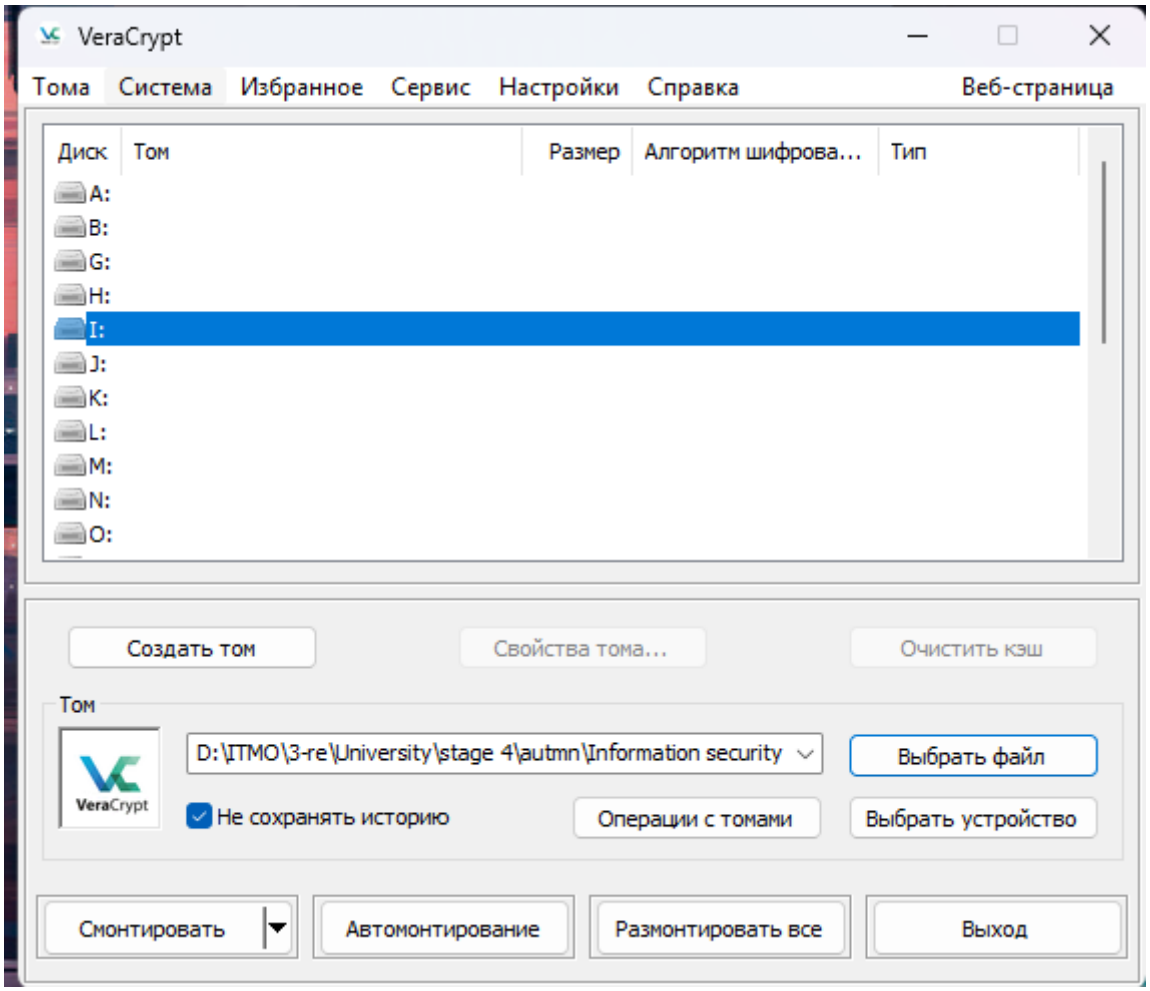


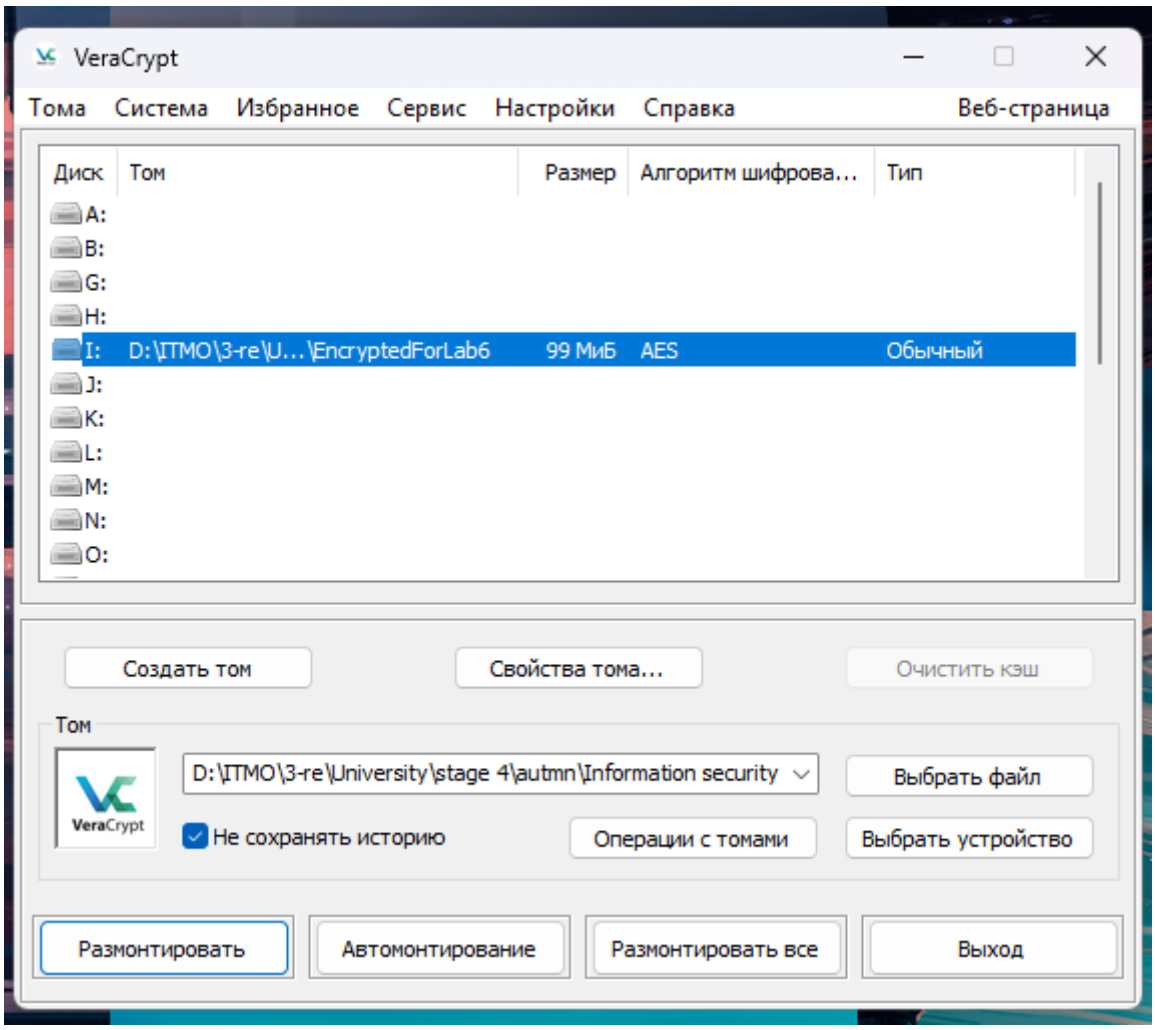
Шифрование



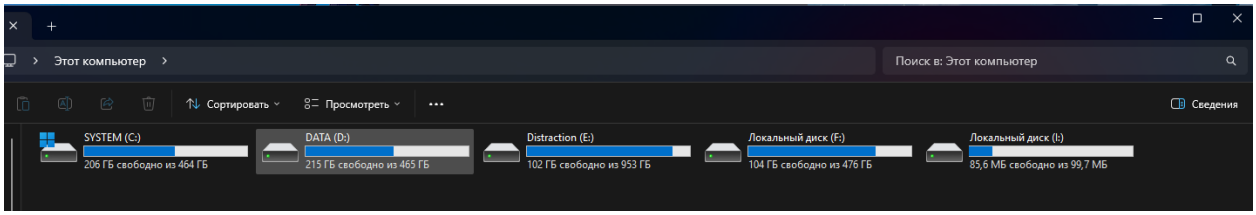
Монтирование тома для

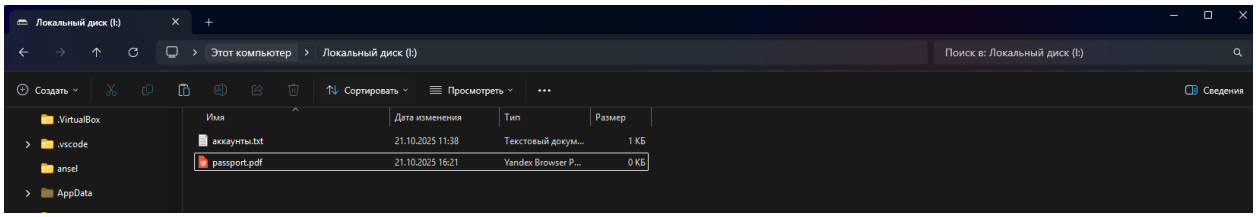




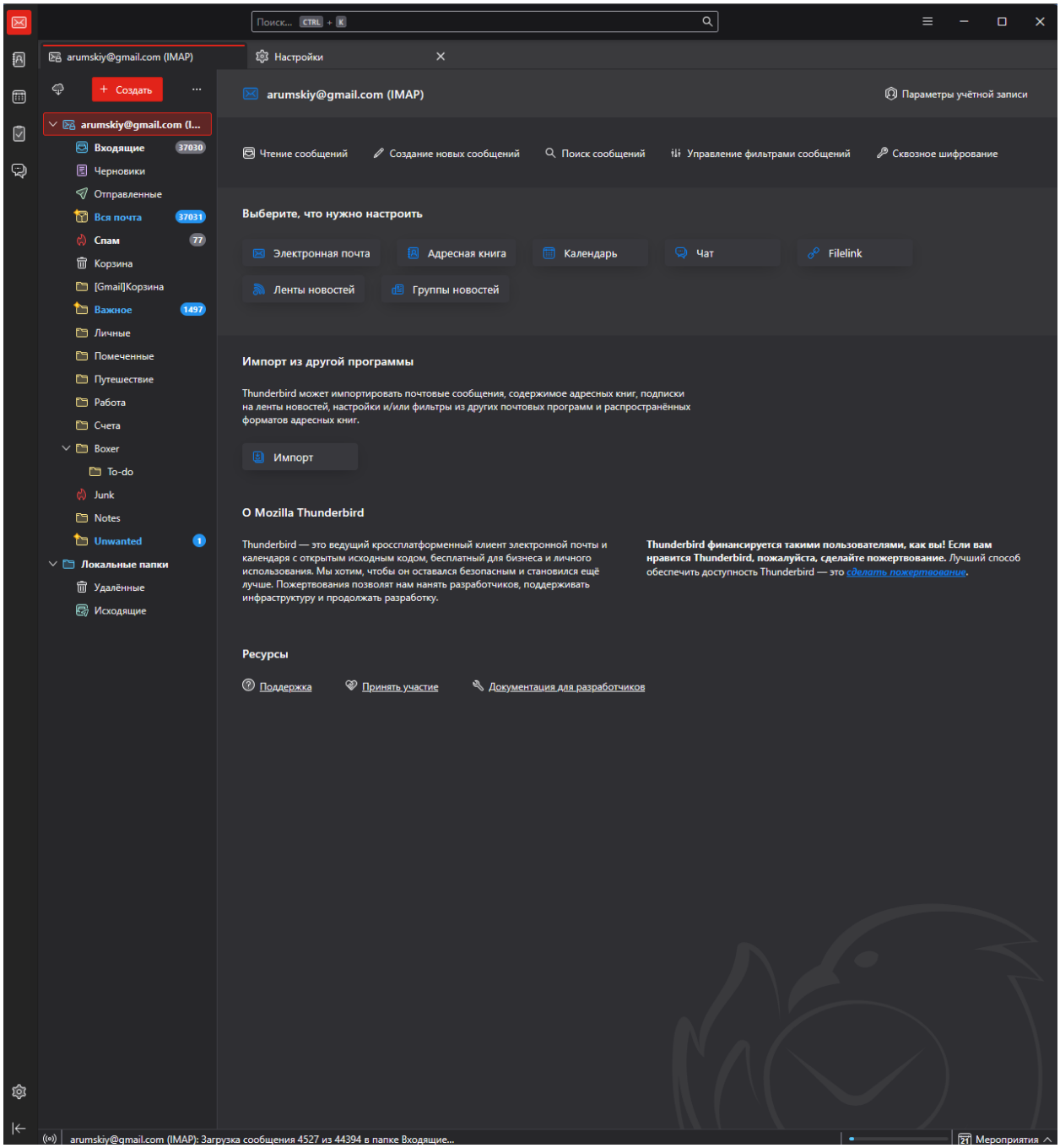


Внесение файлов



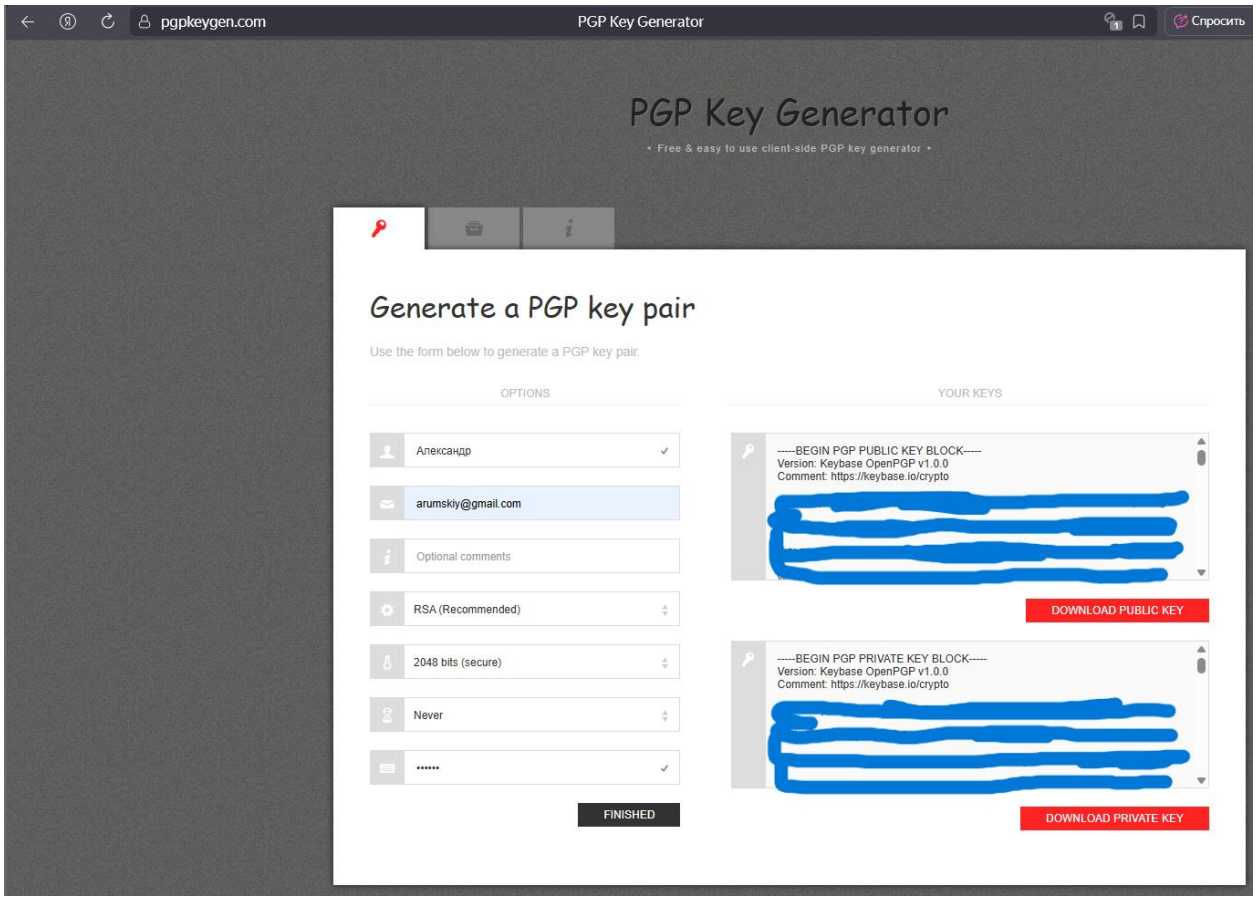


Thunderbird

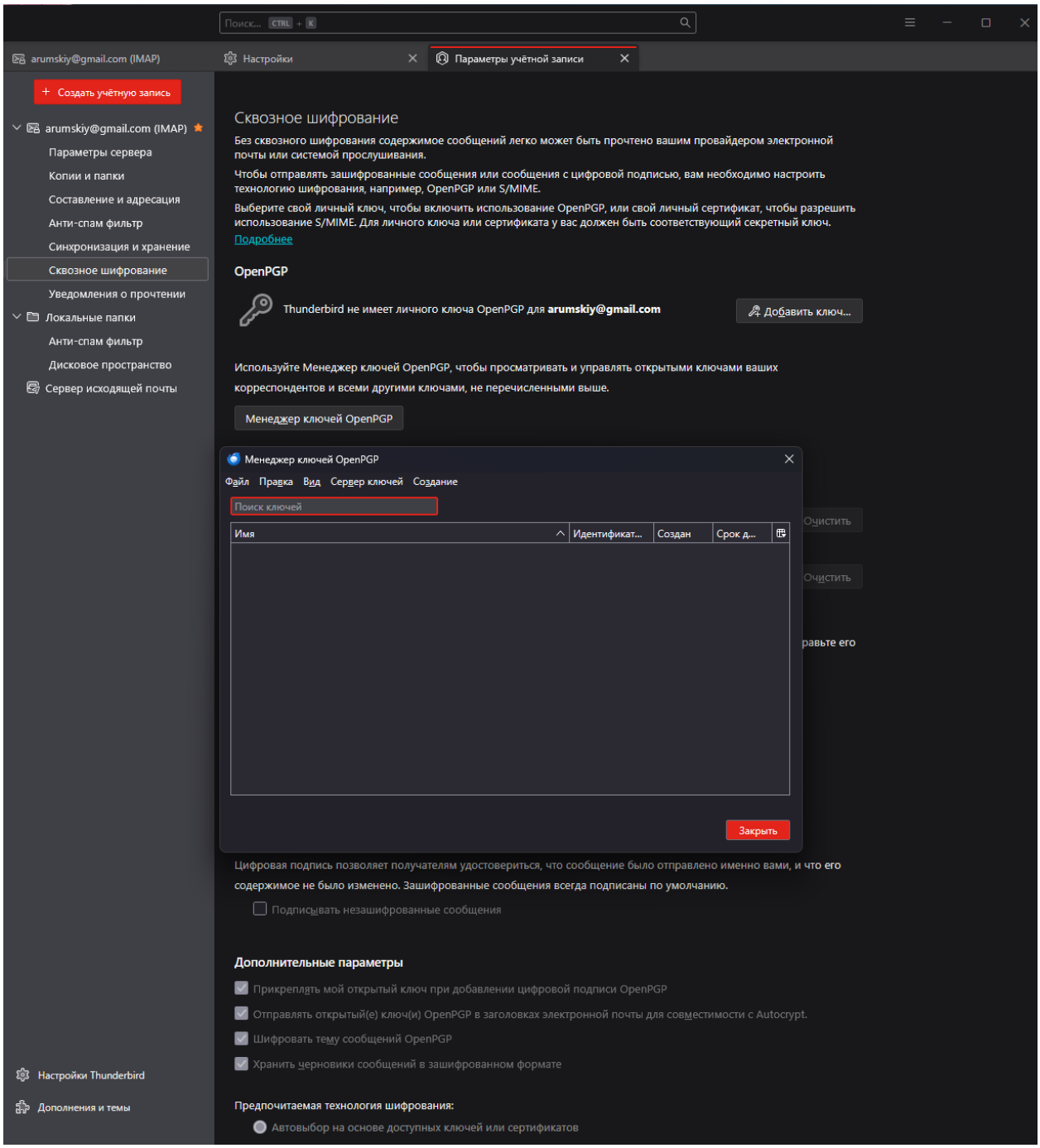


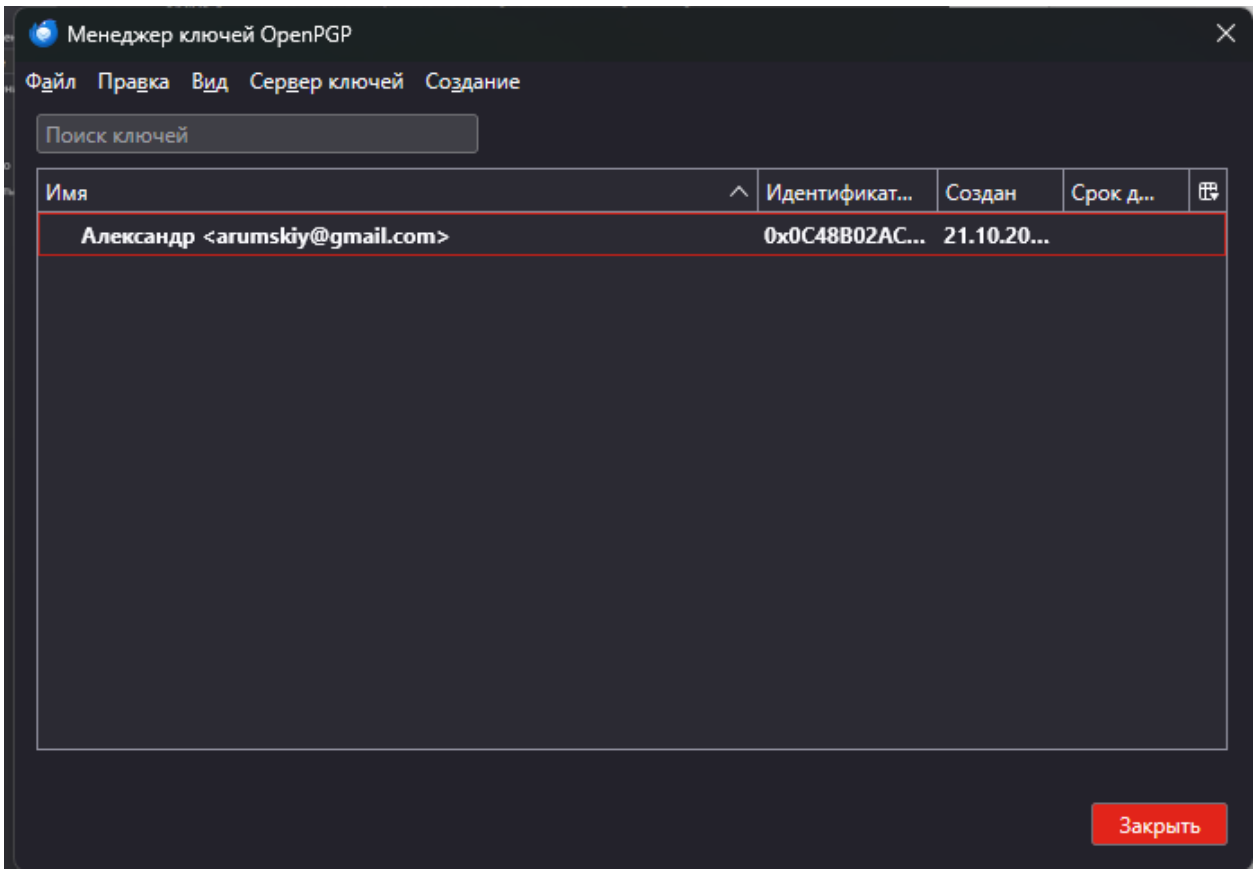
На момент выполнения дополнение Enigmail больше не поддерживается, вместо него используются встроенные инструменты работы с PGP

Генерация пары PGP ключей



Добавление PGP ключа




Менеджер ключей OpenPGP
Файл Правка Вид Сервер ключей Создание
Поиск ключей
Имя
Идентификат...
Создан
Срок д...
Александр <arumskiy@gmail.com>
0x0C48B02AC...
21.10.20...
Закрыть

Разница между симметричным и асимметричным шифрованием

Разница заключается в количестве ключей и алгоритмах. При симметричном шифровании для шифровки и расшифровки используется один и тот же ключ – проще но выше риск кражи данных, так как при утечке ключа можно расшифровать данные. При асинхронном шифровании используется пара ключей: приватный и публичный. Данные шифруются публичным ключом, расшифровываются приватным и подписываются приватным ключом, проверяются публичным – то есть можно не боясь передавать публичный ключ, так как он используется только при проверках и расшифровке.