

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

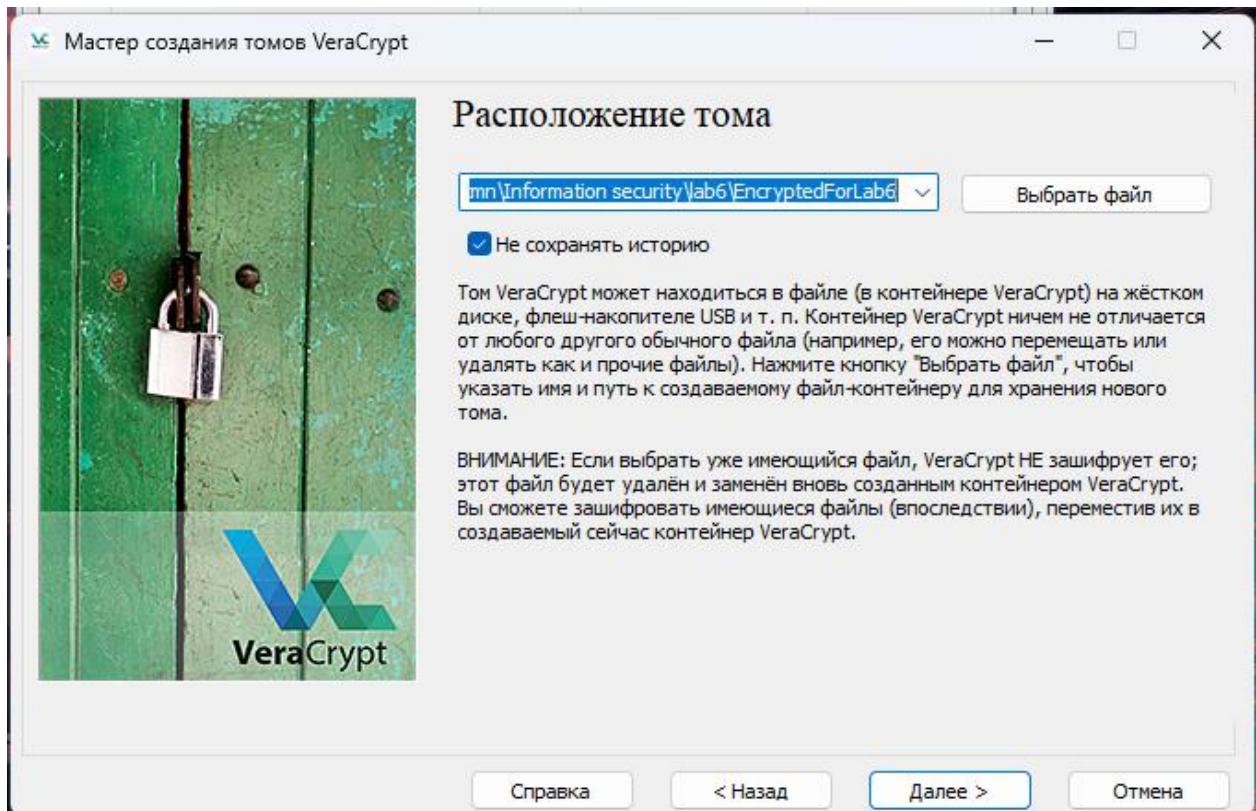
Санкт-Петербург, 2025 год

Содержание

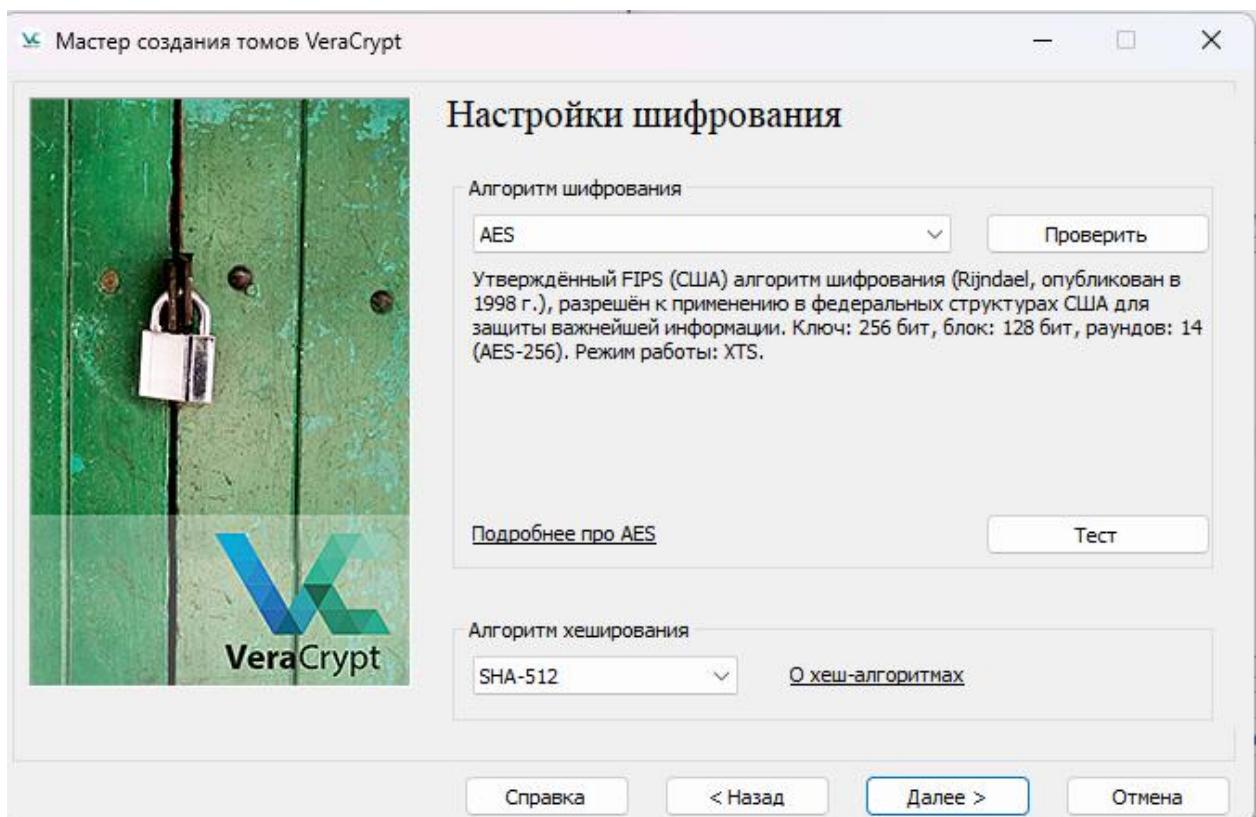
VeraCrypt	3
Создание контейнера	3
Выбор алгоритма шифрования.....	3
Определение размера тома	4
Шифрование	4
Монтирование тома для	5
Внесение файлов	6
Thunderbird	7
Генерация пары PGP ключей.....	8
Добавление PGP ключа	9
Разница между симметричным и асимметричным шифрованием.....	11

VeraCrypt

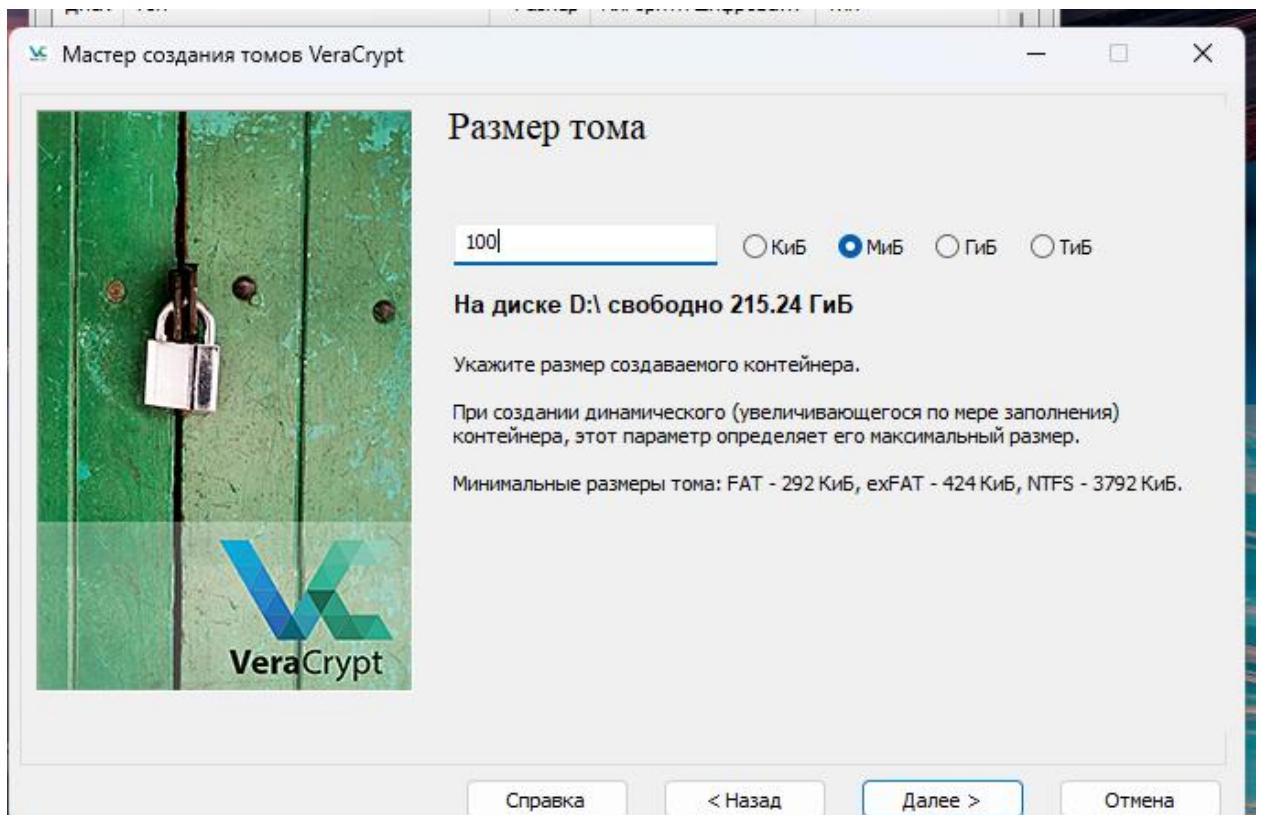
Создание контейнера



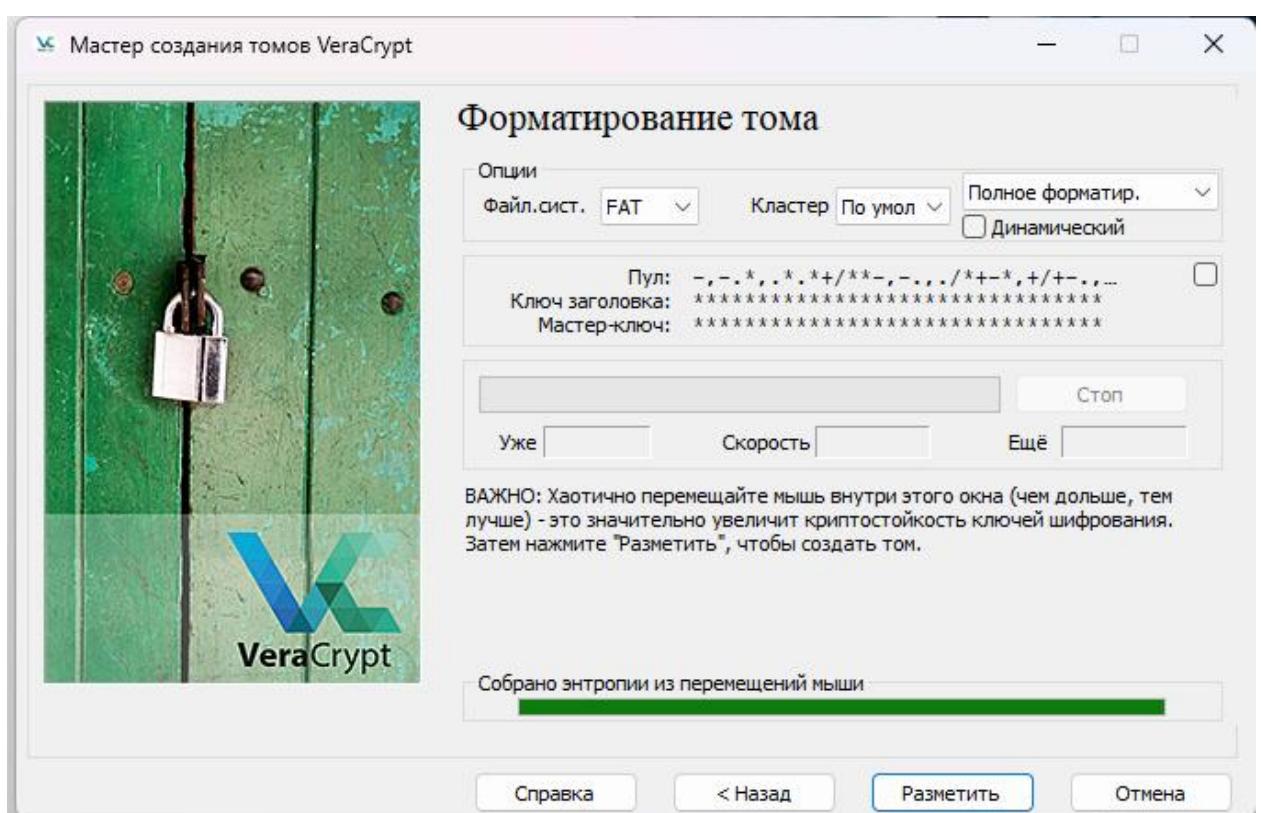
Выбор алгоритма шифрования



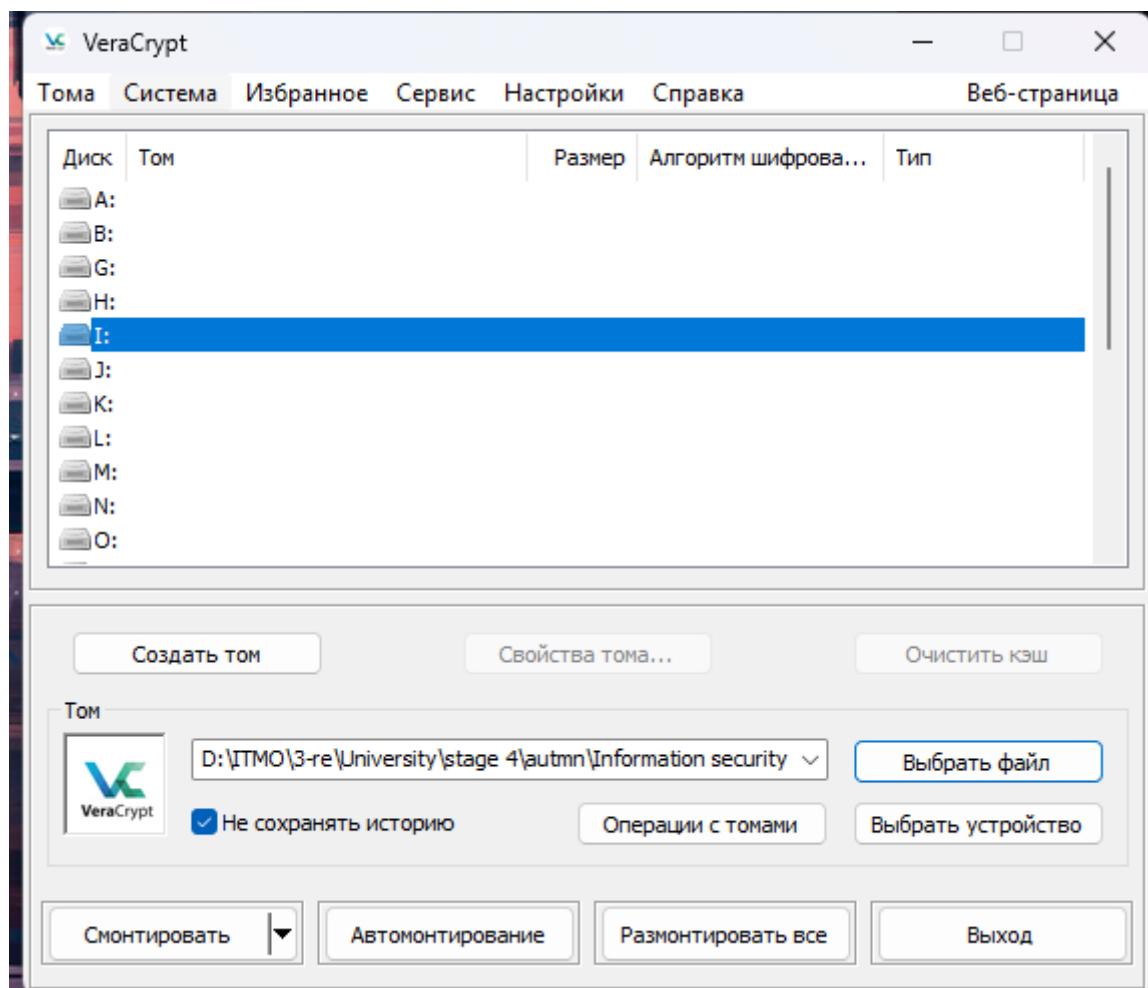
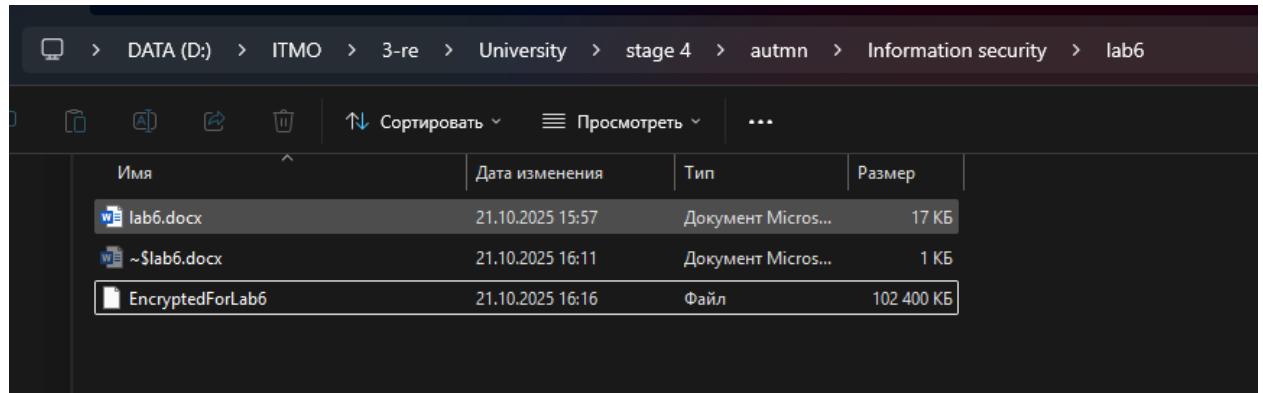
Определение размера тома

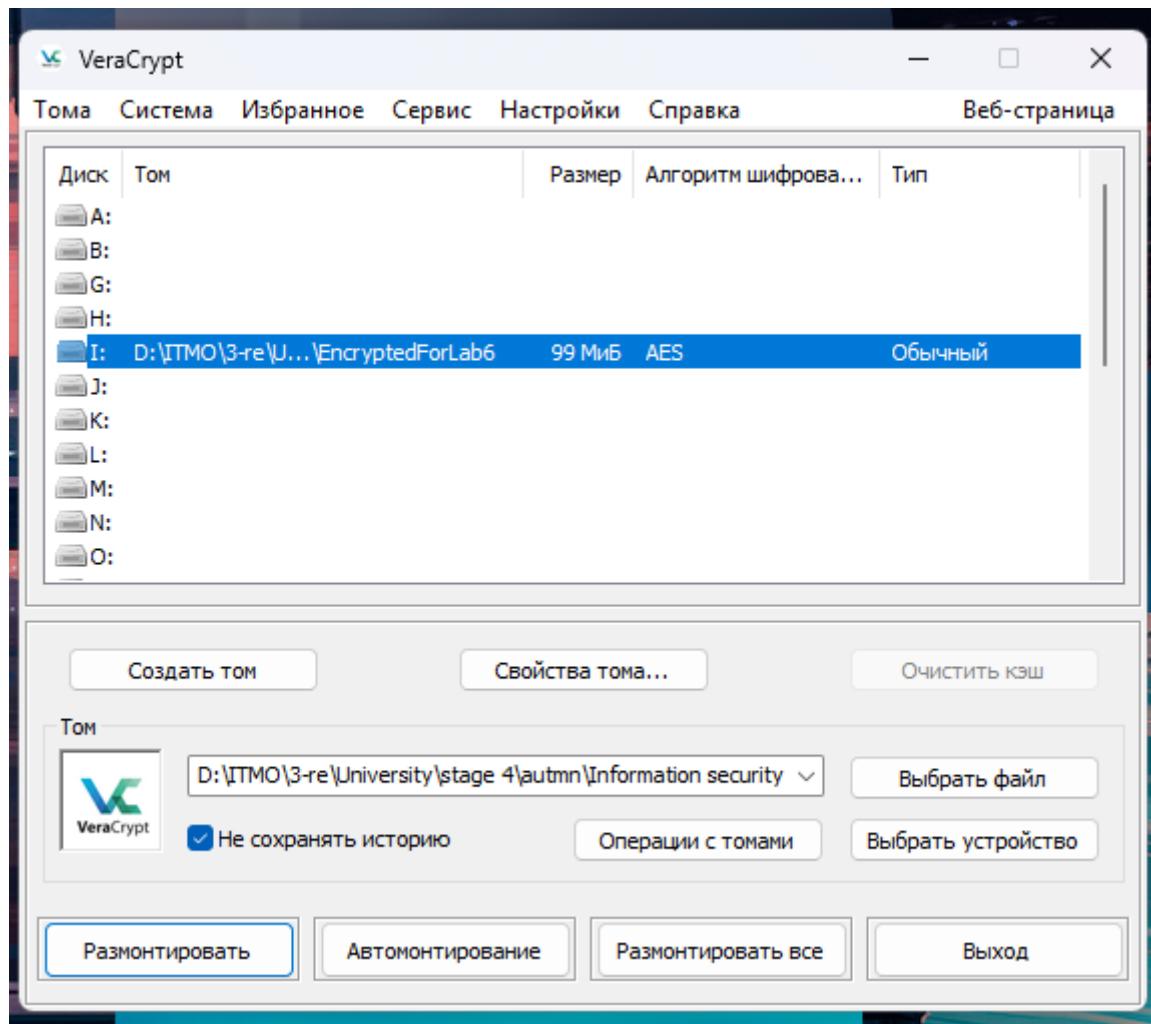


Шифрование

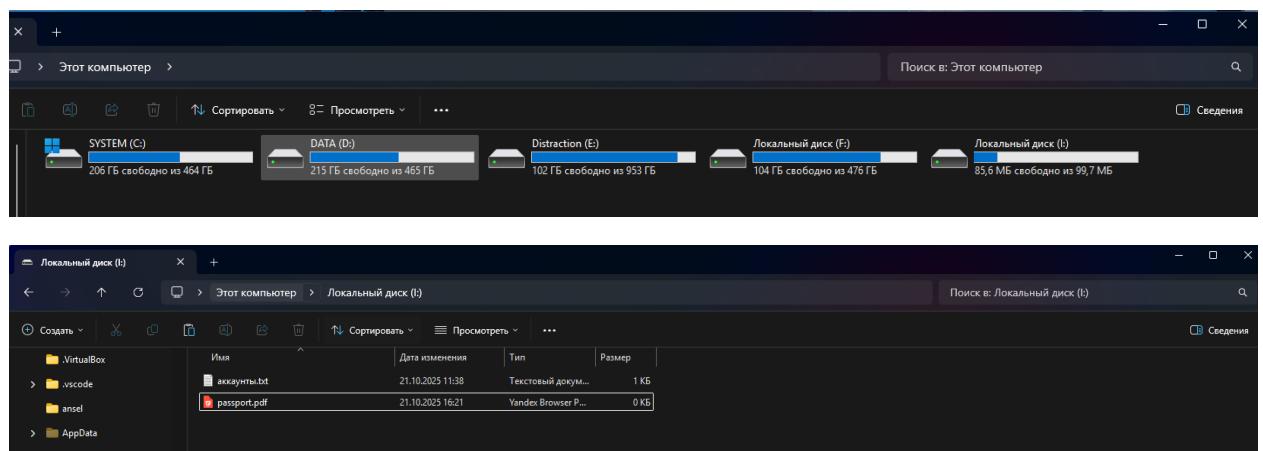


Монтирование тома для

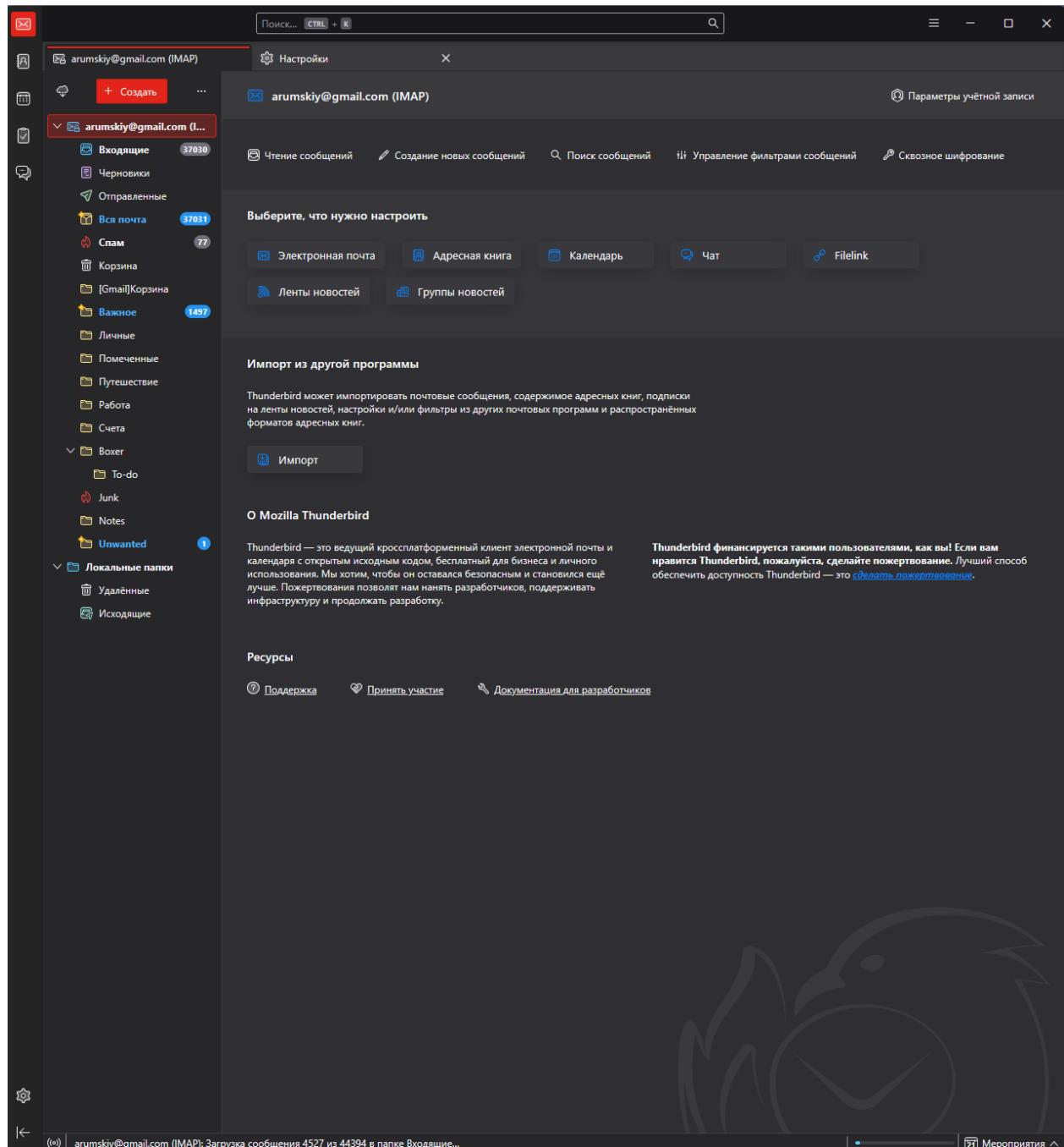




Внесение файлов



Thunderbird



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

Генерация пары PGP ключей

The screenshot shows the PGP Key Generator interface on pgpkeygen.com. At the top, there's a navigation bar with icons for back, forward, search, and a user profile. The main title "PGP Key Generator" is centered above a sub-header "Free & easy to use client-side PGP key generator". Below this, there are three tabs: a red "Generate" tab (which is active), a grey "Import" tab, and a blue "Export" tab.

The main content area is titled "Generate a PGP key pair". It includes a sub-instruction "Use the form below to generate a PGP key pair." Below this, there are two sections: "OPTIONS" on the left and "YOUR KEYS" on the right.

OPTIONS:

- Name: Александр (with a checkmark)
- Email: arumskiy@gmail.com
- Comments: Optional comments (empty)
- Algorithm: RSA (Recommended)
- Key Size: 2048 bits (secure)
- Expire In: Never
- Passphrase: (empty)

YOUR KEYS:

PGP PUBLIC KEY:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: Keybase OpenPGP v1.0.0  
Comment: https://keybase.io/crypto  
[REDACTED]
```

DOWNLOAD PUBLIC KEY

PGP PRIVATE KEY:

```
-----BEGIN PGP PRIVATE KEY BLOCK-----  
Version: Keybase OpenPGP v1.0.0  
Comment: https://keybase.io/crypto  
[REDACTED]
```

DOWNLOAD PRIVATE KEY

At the bottom center is a "FINISHED" button.

Добавление PGP ключа

The screenshot shows the Thunderbird application window with the following details:

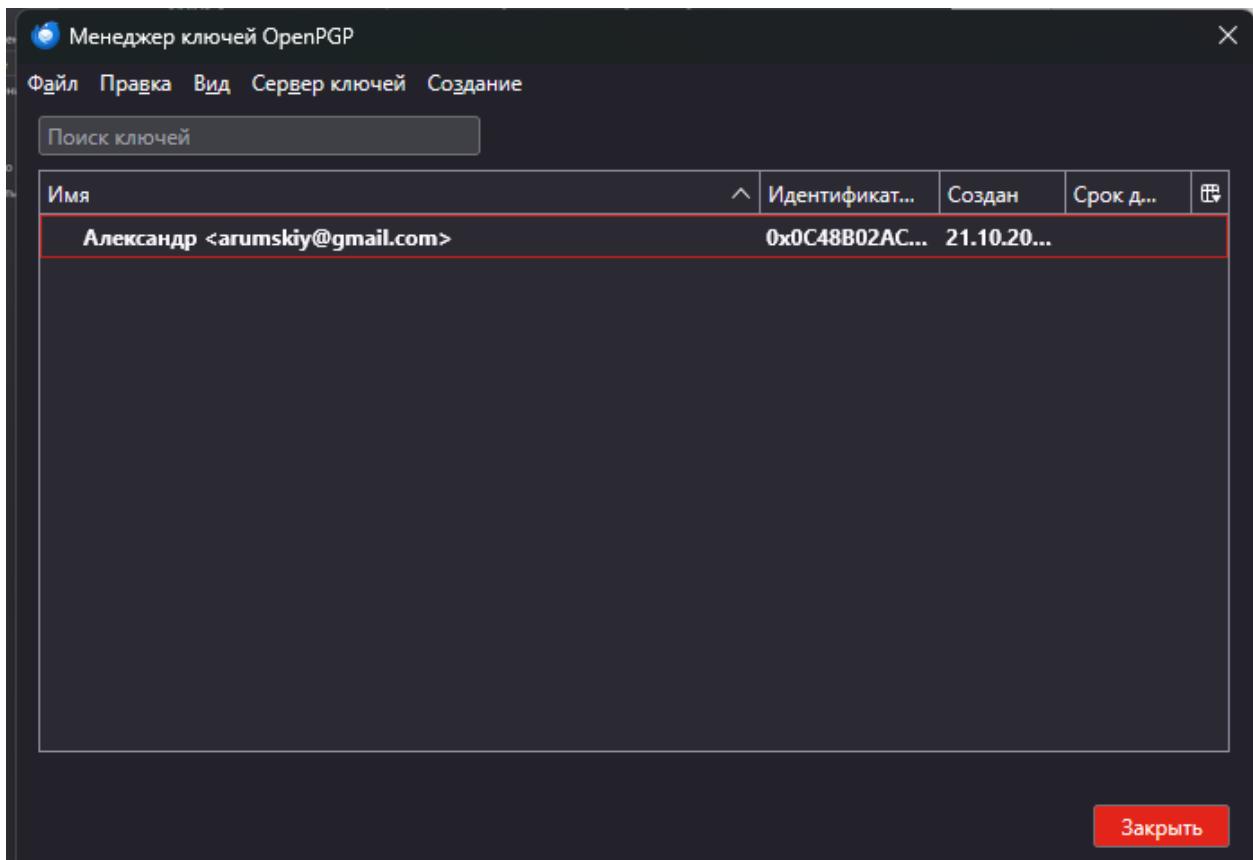
- Account Selection:** arumskiy@gmail.com (IMAP)
- Tab:** Параметры учётной записи (Account Settings)
- Left Sidebar:** Contains links like Создать учётную запись, Параметры сервера, Копии и папки, Составление и адресация, Анти-спам фильтр, Синхронизация и хранение, Сквозное шифрование (selected), Уведомления о прочтении, Локальные папки, Анти-спам фильтр, Дисковое пространство, and Сервер исходящей почты.
- Main Content Area:**
 - Section:** Сквозное шифрование (End-to-end encryption)

Без сквозного шифрования содержимое сообщений легко может быть прочито вашим провайдером электронной почты или системой прослушивания.

Чтобы отправлять зашифрованные сообщения или сообщения с цифровой подписью, вам необходимо настроить технологию шифрования, например, OpenPGP или S/MIME.

Выберите свой личный ключ, чтобы включить использование OpenPGP, или свой личный сертификат, чтобы разрешить использование S/MIME. Для личного ключа или сертификата у вас должен быть соответствующий секретный ключ.

[Подробнее](#)
 - Section:** OpenPGP
 - Key Status:** Thunderbird не имеет личного ключа OpenPGP для arumskiy@gmail.com
 - Action Button:** Добавить ключ...
 - Text:** Используйте Менеджер ключей OpenPGP, чтобы просматривать и управлять открытыми ключами ваших корреспондентов и всеми другими ключами, не перечисленными выше.
 - Sub-Window:** Менеджер ключей OpenPGP
 - Title:** Менеджер ключей OpenPGP
 - Toolbar:** Файл, Правка, Вид, Сервер ключей, Создание
 - Search Bar:** Поиск ключей
 - Table:** Имя, Идентификат..., Создан, Срок д...
 - Buttons:** Закрыть
 - Text:** Цифровая подпись позволяет получателям удостовериться, что сообщение было отправлено именно вами, и что его содержимое не было изменено. Зашифрованные сообщения всегда подписыны по умолчанию.
 Подписывать незашифрованные сообщения
 - Section:** Дополнительные параметры
 - Прикреплять мой открытый ключ при добавлении цифровой подписи OpenPGP
 - Отправлять открытый(е) ключ(и) OpenPGP в заголовках электронной почты для совместимости с Autocrypt.
 - Шифровать тему сообщений OpenPGP
 - Хранить черновики сообщений в зашифрованном формате
 - Section:** Предпочитаемая технология шифрования:
 - Автовыбор на основе доступных ключей или сертификатов



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.