

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:

Р3407

Преподаватель:

Маркина Татьяна Анатольевна

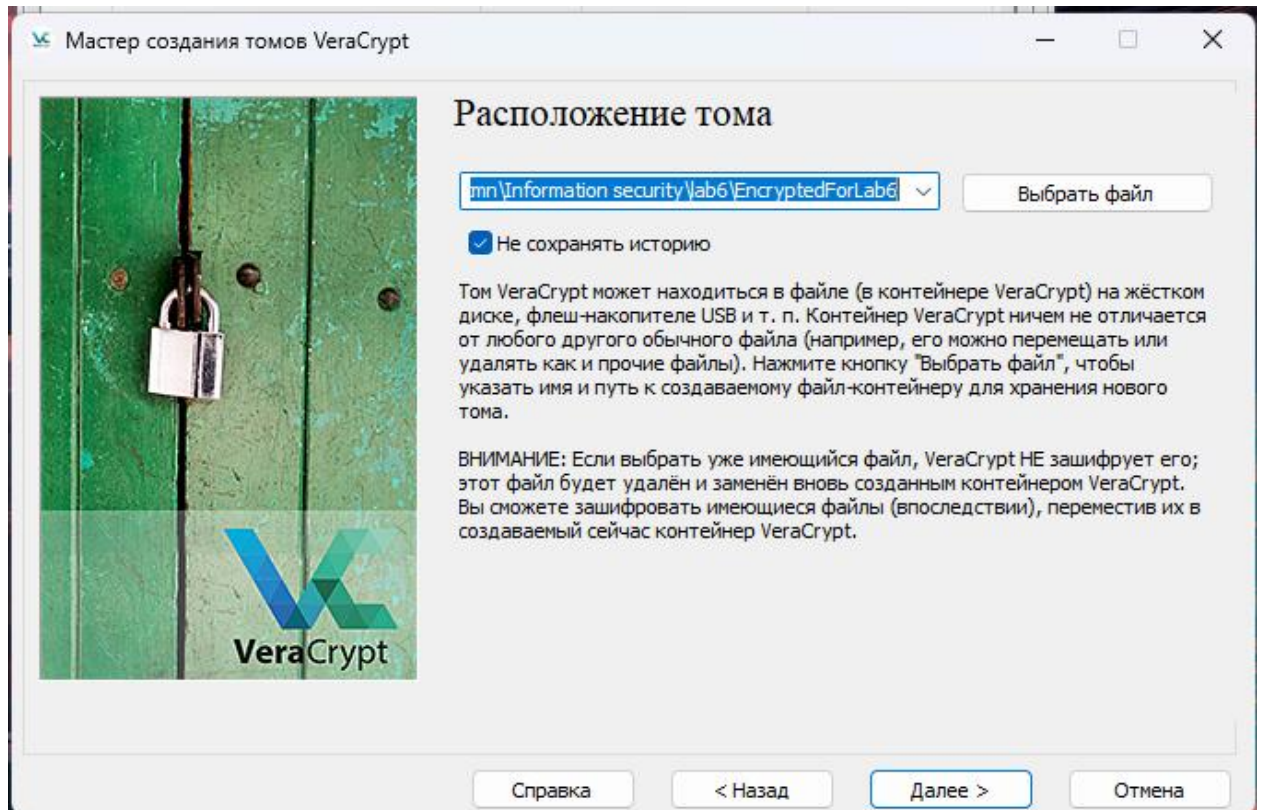
Санкт-Петербург, 2025 год

Содержание

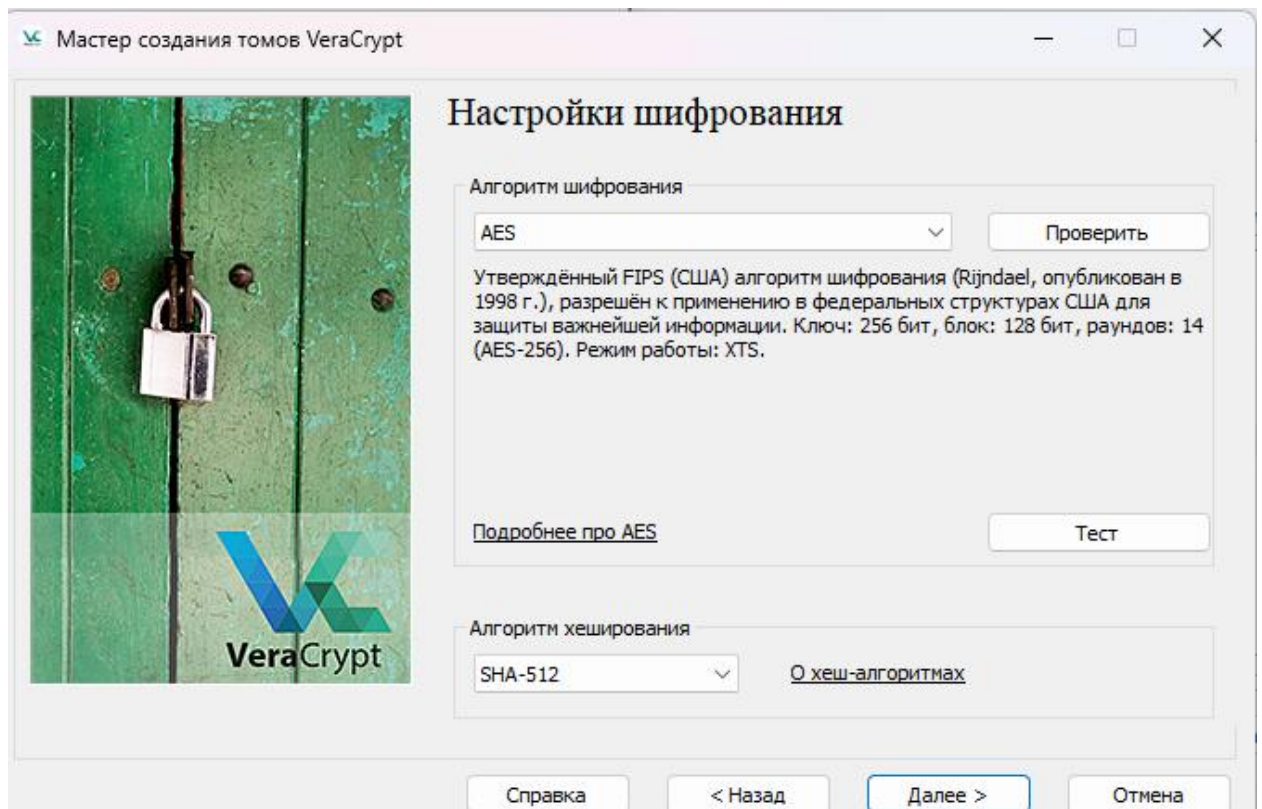
VeraCrypt	3
Создание контейнера	3
Выбор алгоритма шифрования.....	3
Определение размера тома	4
Шифрование	4
Монтирование тома для	5
Внесение файлов	6
Thunderbird	7
Генерация пары PGP ключей	8
Добавление PGP ключа	9
Разница между симметричным и асимметричным шифрованием.....	11

VeraCrypt

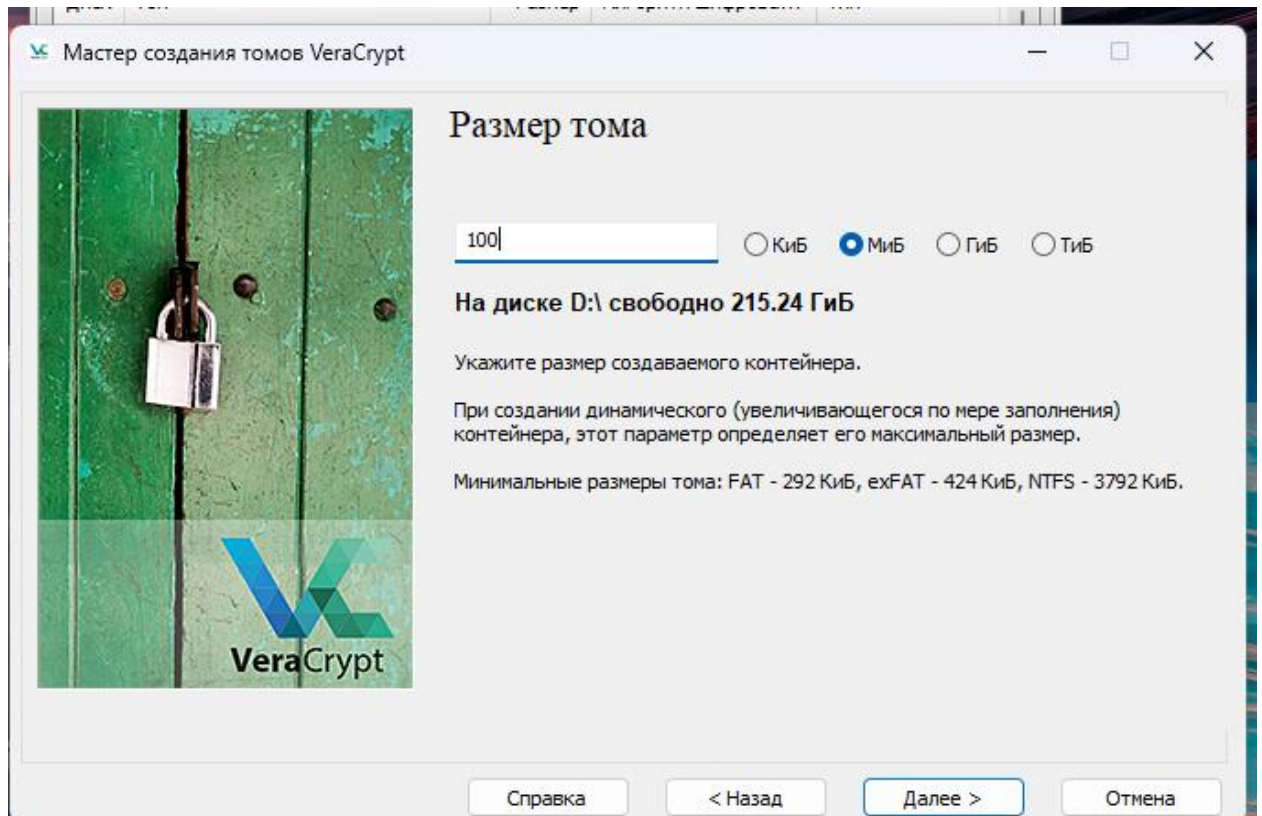
Создание контейнера



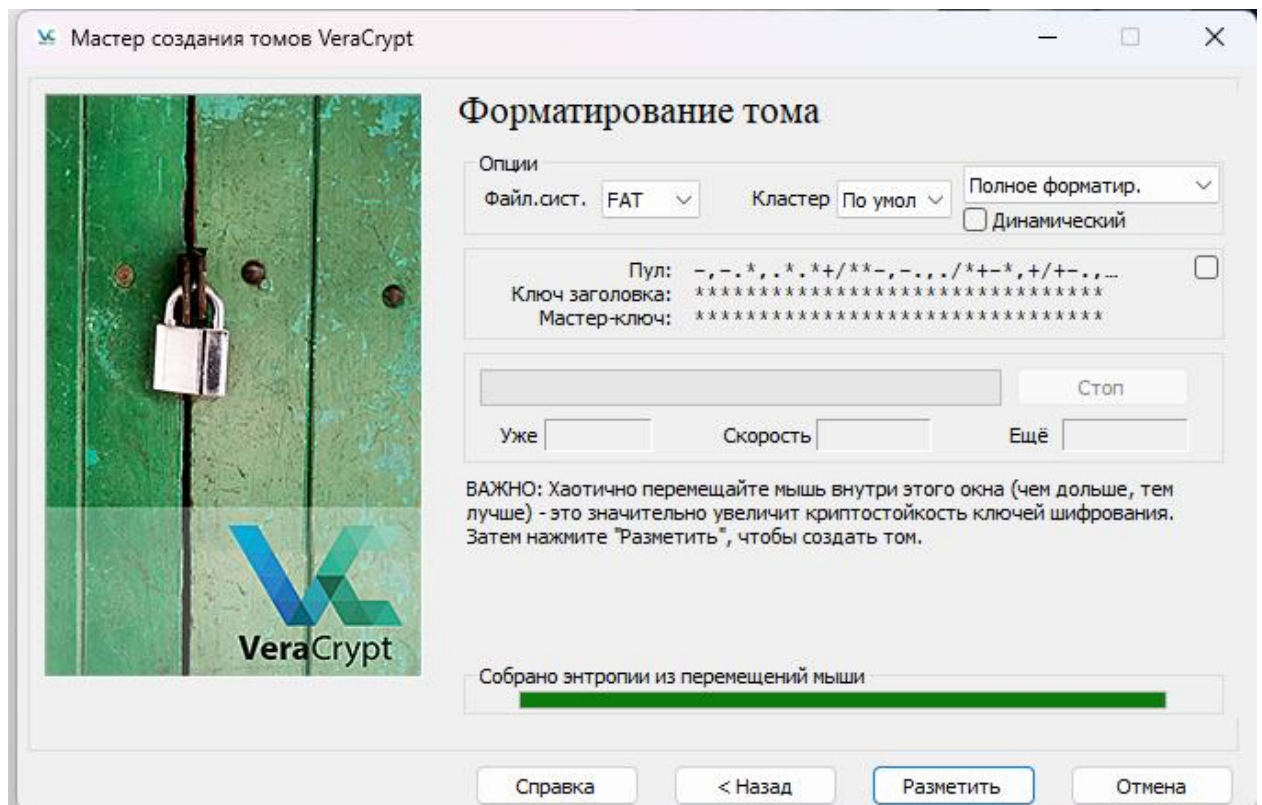
Выбор алгоритма шифрования



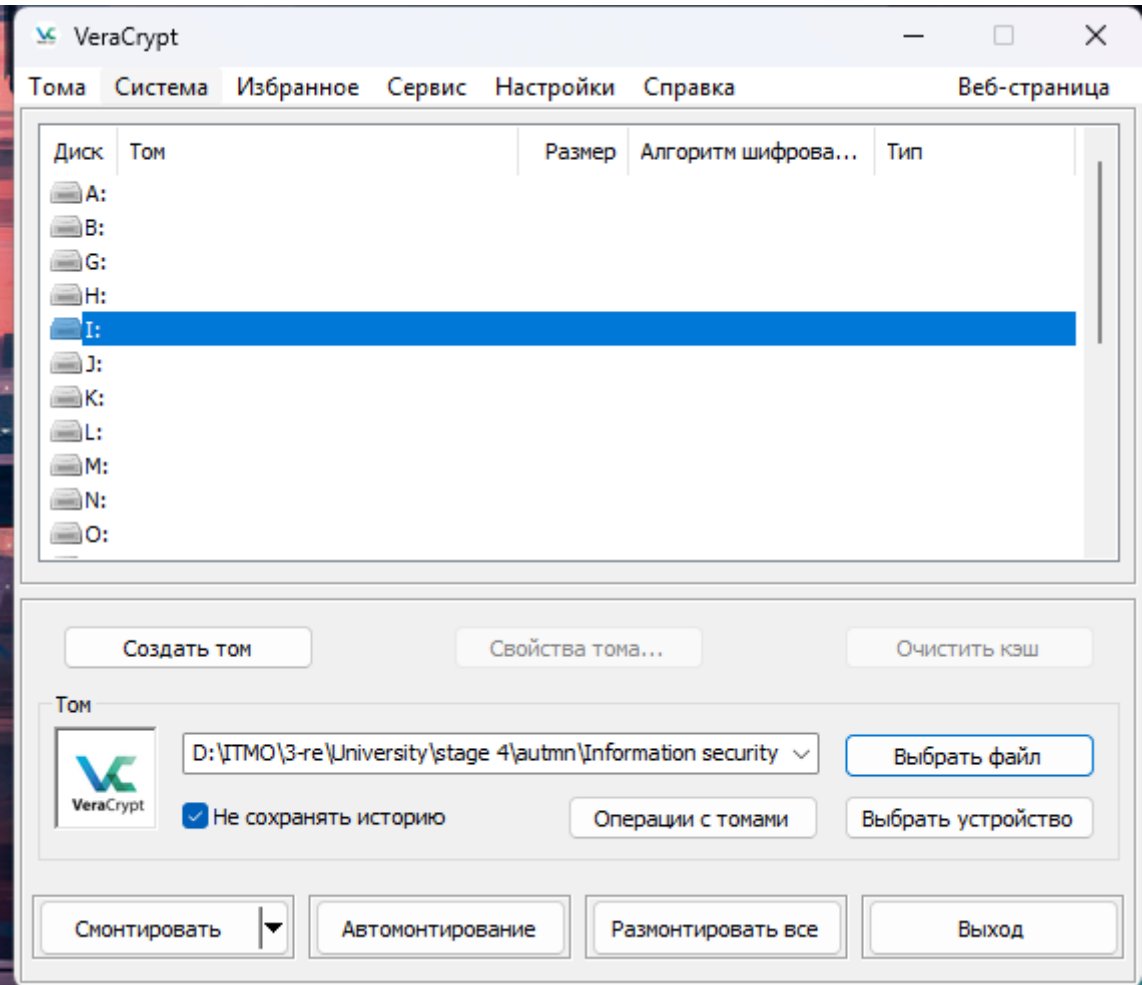
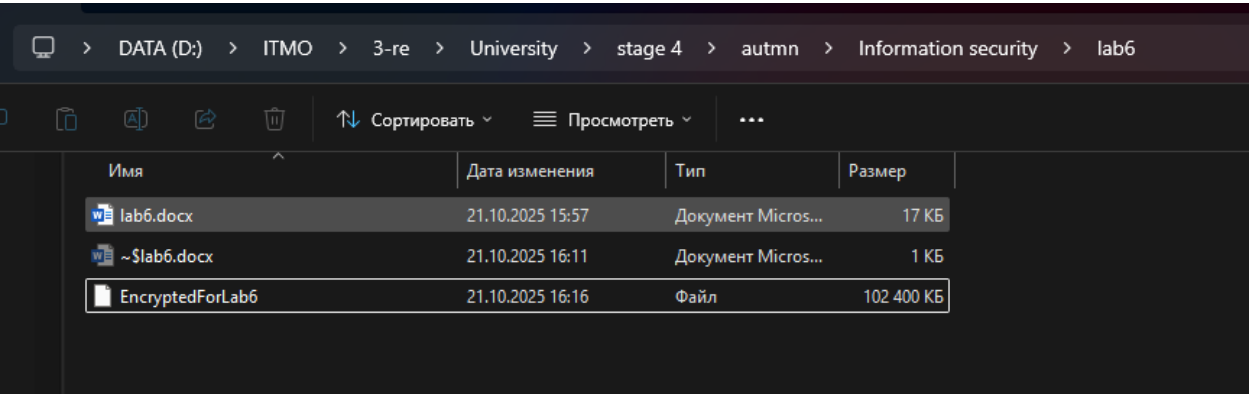
Определение размера тома

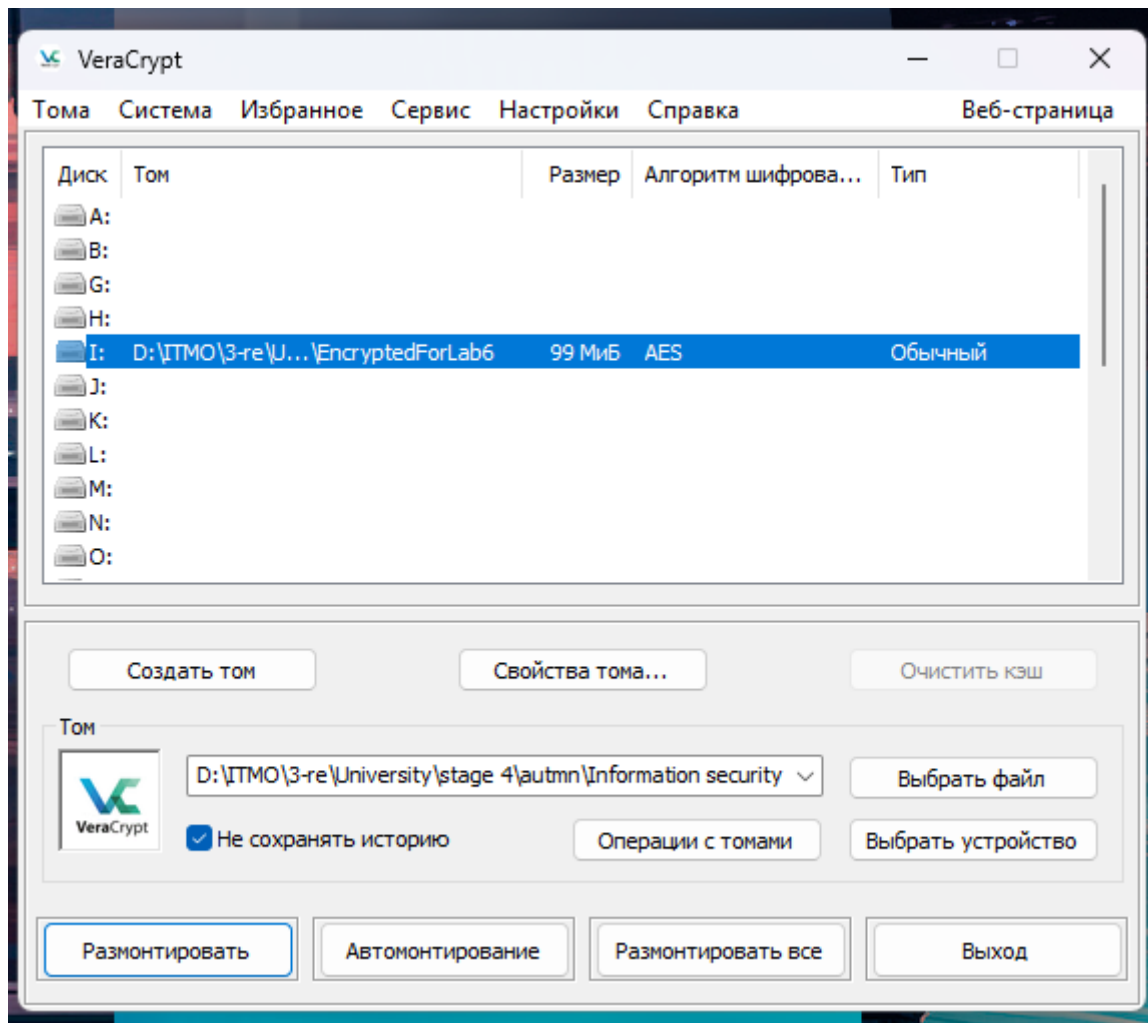


Шифрование

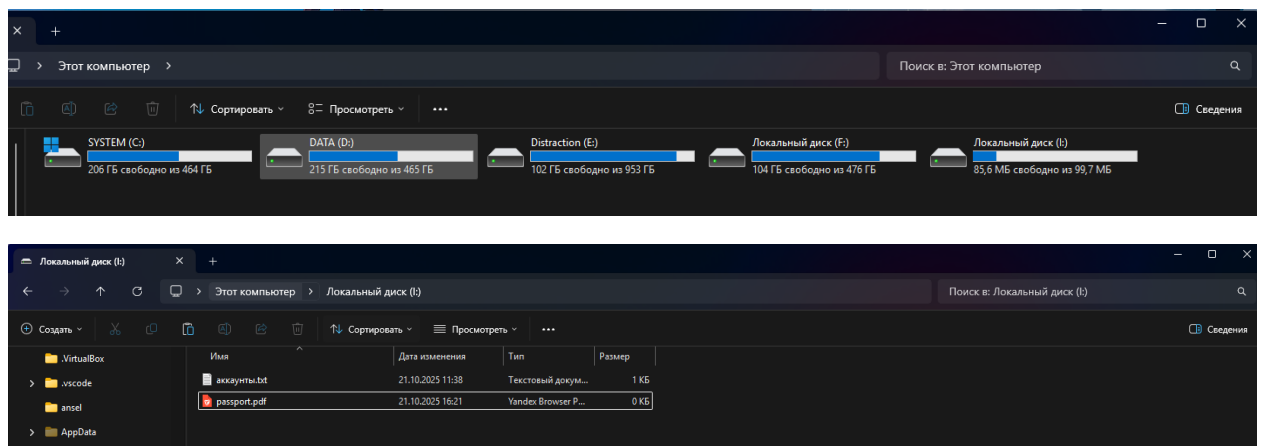


Монтирование тома для

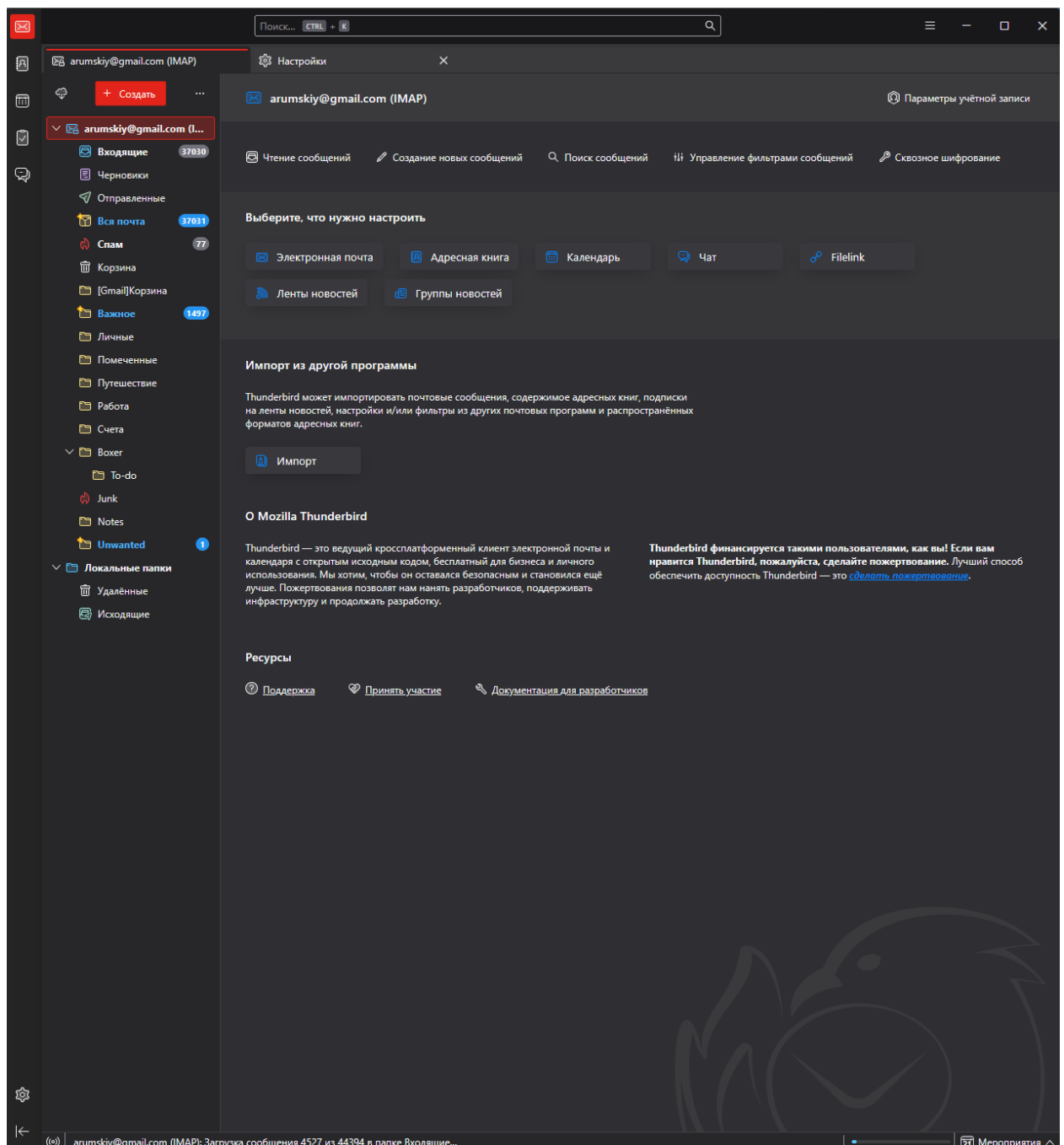




Внесение файлов



Thunderbird



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

Генерация пары PGP ключей

←

🔄

🔒

pgpkeygen.com

PGP Key Generator

🔑

📖

🔗 Спросить

PGP Key Generator

• Free & easy to use client-side PGP key generator •

🔑

📁

ℹ️

Generate a PGP key pair

Use the form below to generate a PGP key pair:

OPTIONS

👤 Александр ✓

✉️ arumskiy@gmail.com

ℹ️ Optional comments

⚙️ RSA (Recommended)

🔒 2048 bits (secure)

⌚ Never

🔑 ***** ✓

FINISHED

YOUR KEYS

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

DOWNLOAD PUBLIC KEY

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

DOWNLOAD PRIVATE KEY

Добавление PGP ключа

arumskiy@gmail.com (IMAP)

Создать учётную запись

arumskiy@gmail.com (IMAP)

Параметры сервера

Копии и папки

Составление и адресация

Анти-спам фильтр

Синхронизация и хранение

Сквозное шифрование

Уведомления о прочтении

Локальные папки

Анти-спам фильтр

Дисковое пространство

Сервер исходящей почты

Настройки Thunderbird

Дополнения и темы

Настройки

Параметры учётной записи

Сквозное шифрование

Без сквозного шифрования содержимое сообщений легко может быть прочтено 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

OpenPGP

Thunderbird не имеет личного ключа OpenPGP для arumskiy@gmail.com

Добавить ключ...

Используйте Менеджер ключей OpenPGP, чтобы просматривать и управлять открытыми ключами ваших корреспондентов и всеми другими ключами, не перечисленными выше.

Менеджер ключей OpenPGP

Менеджер ключей OpenPGP

Файл Правка Вид Сервер ключей Создание

Поиск ключей

Имя	Идентификат...	Создан	Срок д...	
-----	----------------	--------	-----------	--

Очистить

Очистить

равьте его

Закреть

Цифровая подпись позволяет получателям удостовериться, что сообщение было отправлено именно вами, и что его содержимое не было изменено. Зашифрованные сообщения всегда подписаны по умолчанию.

☐ Подписывать незашифрованные сообщения

Дополнительные параметры

☒ Прикреплять мой открытый ключ при добавлении цифровой подписи OpenPGP

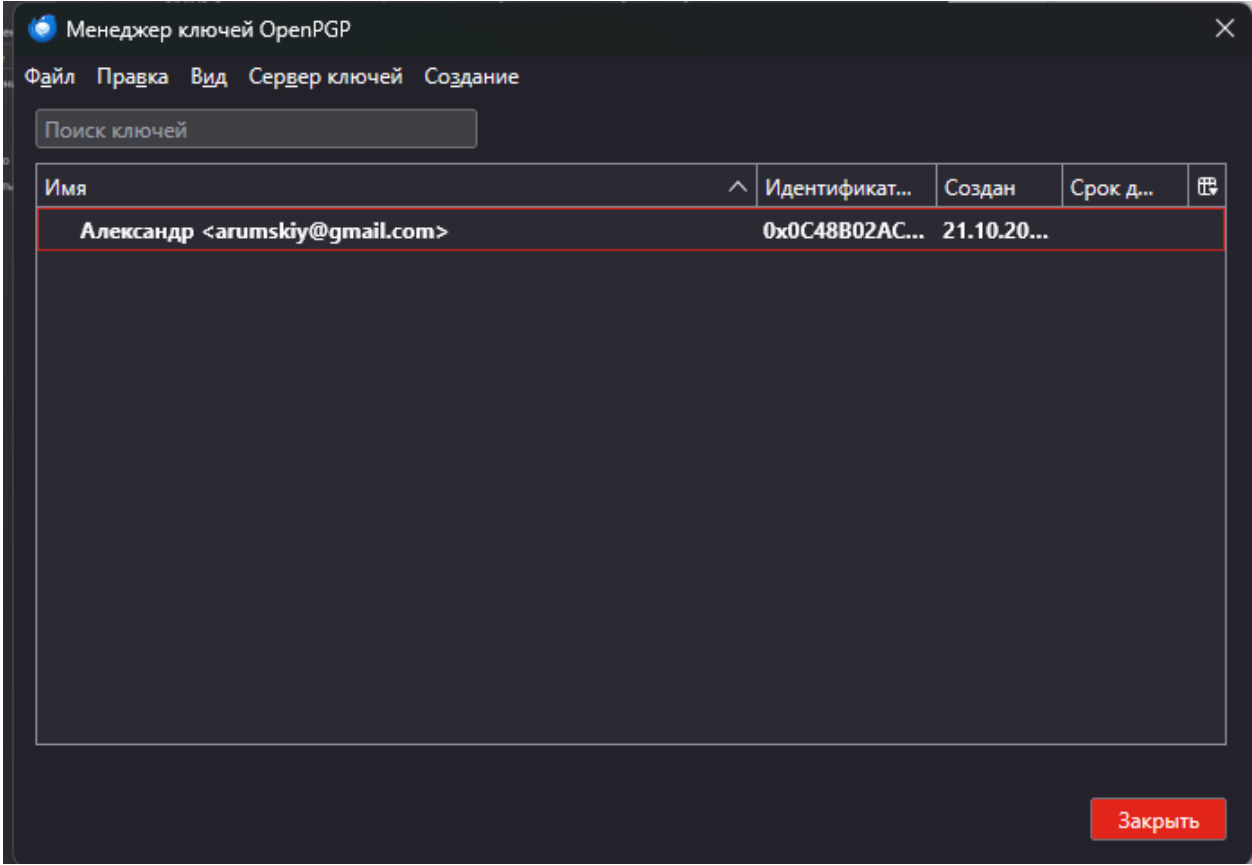
☒ Отправлять открытый(е) ключ(и) OpenPGP в заголовках электронной почты для совместимости с Autocrypt.

☒ Шифровать тему сообщений OpenPGP

☒ Хранить черновики сообщений в зашифрованном формате

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.