Министерство образования и науки Российской Федерации  
ФГАОУ ВПО «Уральский федеральный университет имени первого  
 Президента России Б.Н. Ельцина

Научно-учебный центр «Информационная безопасность»

Отчет

По лабораторной работе №7

По дисциплине «Криптографические методы защиты информации»

Студент Родионов Леонид Владиславович

(Подпись)

Студент Ибрагимов Игорь Андреевич

(Подпись)

Преподаватель Агафонов Алексей Владимирович

(Подпись)

Дата 26.04.2022

Академическая группа РИ-481220

Екатеринбург 2022

Цели: научиться шифровать данные при передаче в сети и использовать ЭП

При выполнении лабораторной работы для отправки почты было принято решение использовать сервер по умолчанию, а не настраивать локальный. В качестве почтового клиента был использован клиент Thunderbird последней версии. Целью данной работы является настройка электронной подписи и установка закрытого канала передачи информации между двумя пользователями. Смысл работы такого канала состоит в следующем: Пользователи используют ассиметричное шифрование (В нашем примере RSA). Зная адреса электронной почты друг друга, они обмениваются сообщениями, содержащими открытые ключи. После этого между ними может быть настроен защищенный канал передачи информации. Перейдем к настройкам Thunderbird:

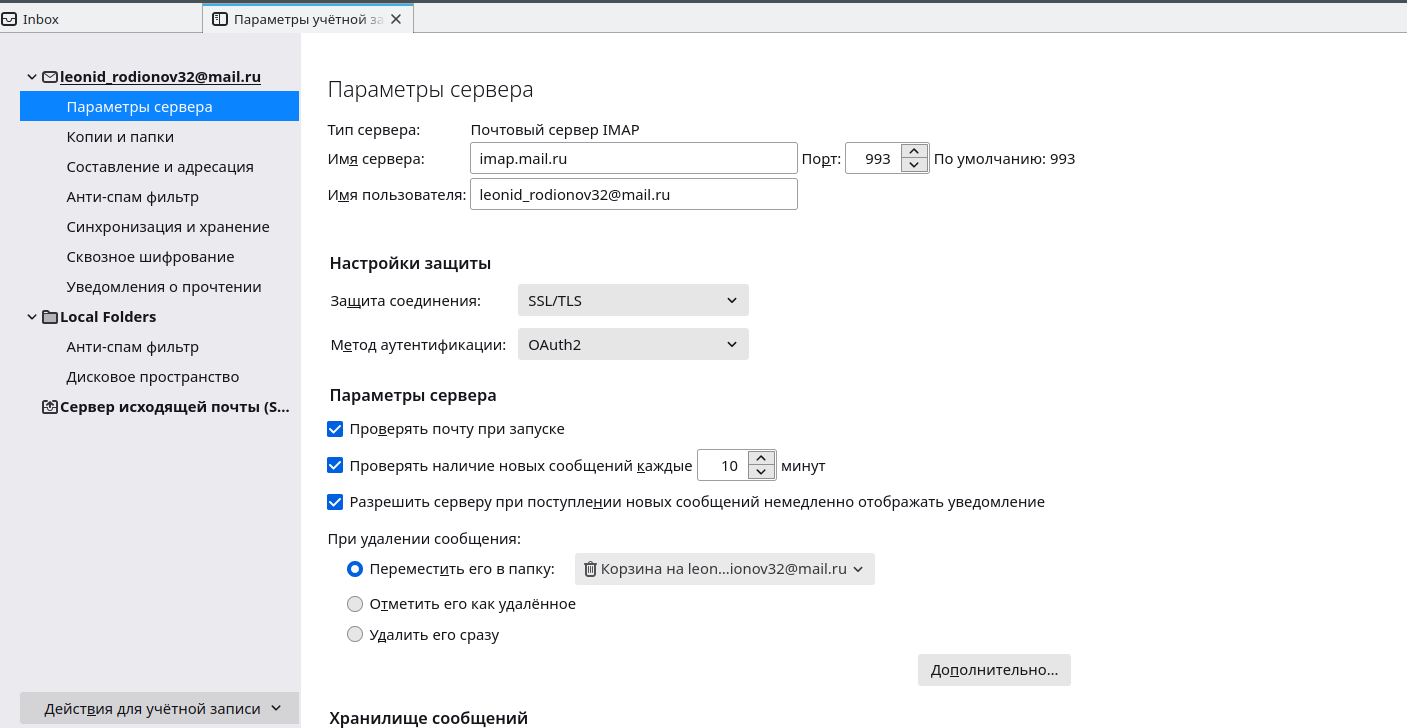


Рисунок – Настройки сервера Thunderbird

Как мы можем заметить, даже без RSA на сервере предусмотрена защита, поскольку IMAP-протокол подразумевает шифрование данных

Согласно методическим указаниям требовалось установить плагин Enigmail для Thunderbird, однако в последней версии программы функции Enigmail встроены в клиент Thunderbird. Для начала необходимо создать открытый и закрытый ключи шифрования:

Открываем параметры учетной записи выбираем слева пункт «Сквозное шифрование». В этой вкладке есть менеджер паролей, который обеспечивает связь электронной почты контактов и их открытых ключей.

Нам нужно создать свою пару ключей. Для этого жмем «Добавить ключ»

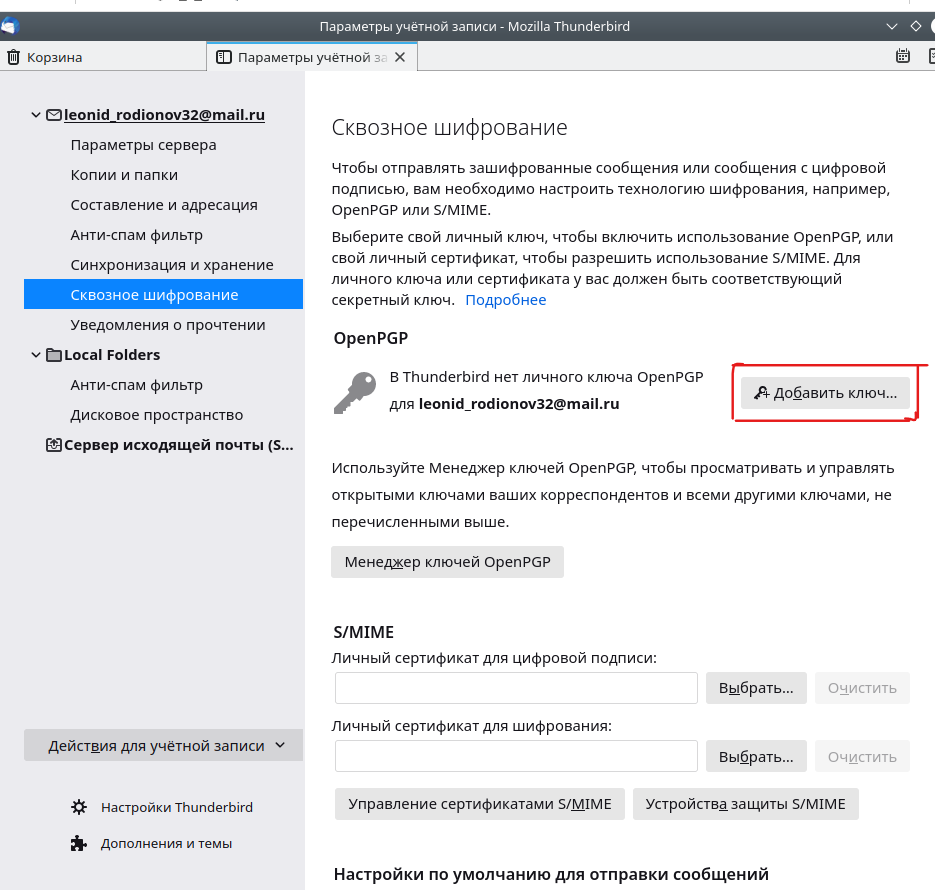


Рисунок – Вкладка «Сквозное шифрование»

Далее нам предлагают создать новый ключ или импортировать существующий

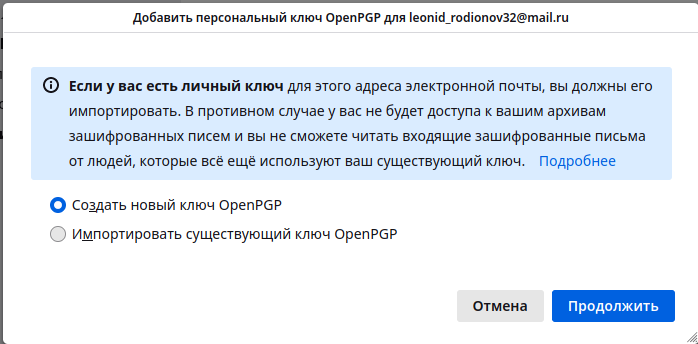


Рисунок – Создание ключа

Далее можем выбрать параметры шифрования, такие как: тип ключа, срок действия ключа, размер ключа и т.д

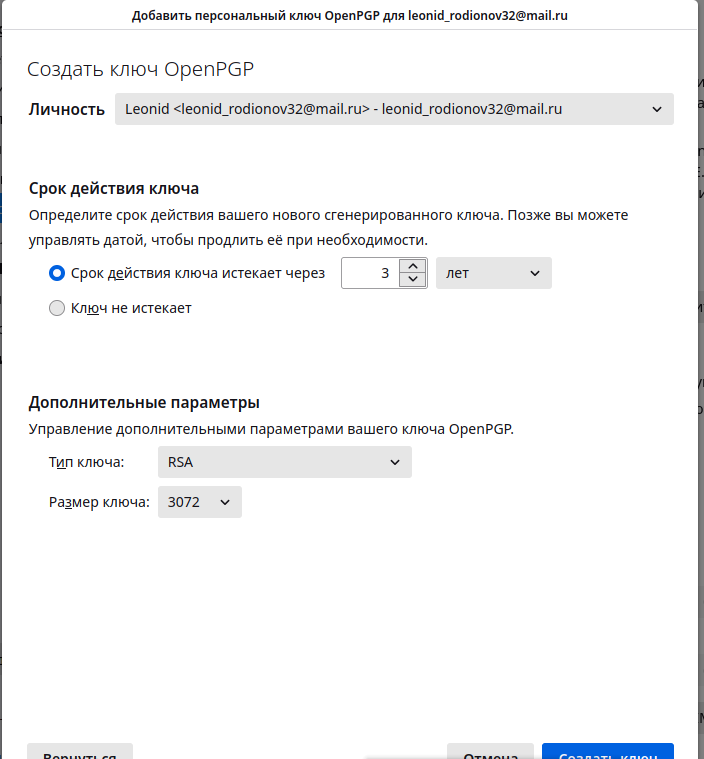


Рисунок – Параметры создаваемого ключа

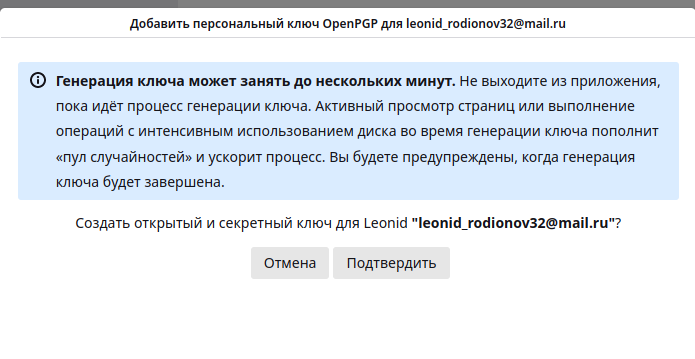


Рисунок – Подтверждение создания ключа

После создания ключа во вкладке «Сквозное шифрование» появляется следующая надпись.

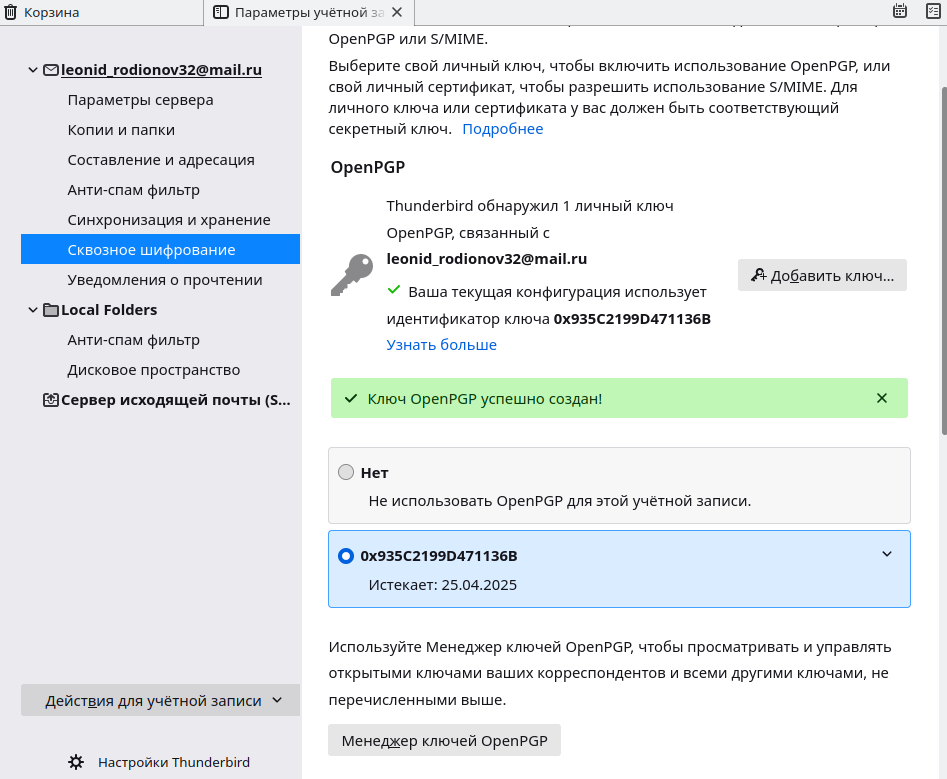


Рисунок – Изменение во вкладке «Сквозное шифрование»

Теперь откроем менеджер ключей. Меню выглядит следующим образом:

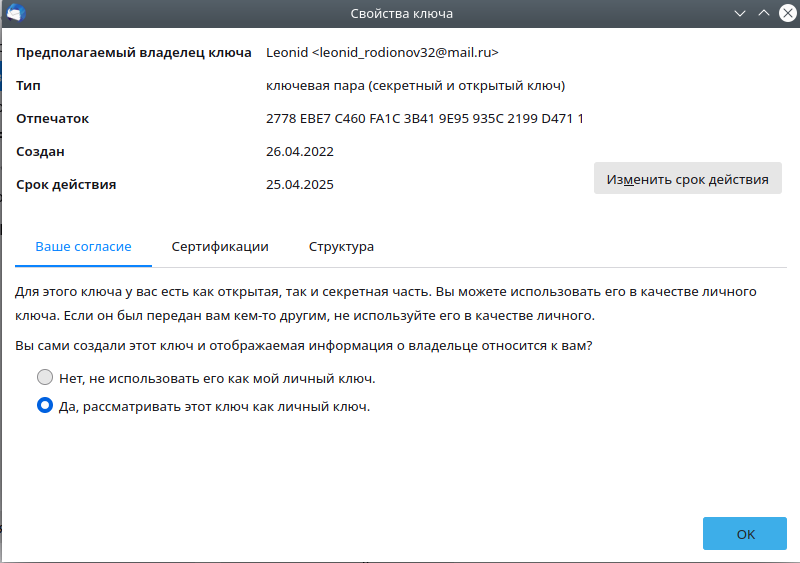


Рисунок – Окно «Менеджер ключей»

Теперь, когда мы сгенерировали ключевую пару, можно отправить наш открытый ключ собеседнику

Отправка ключа:

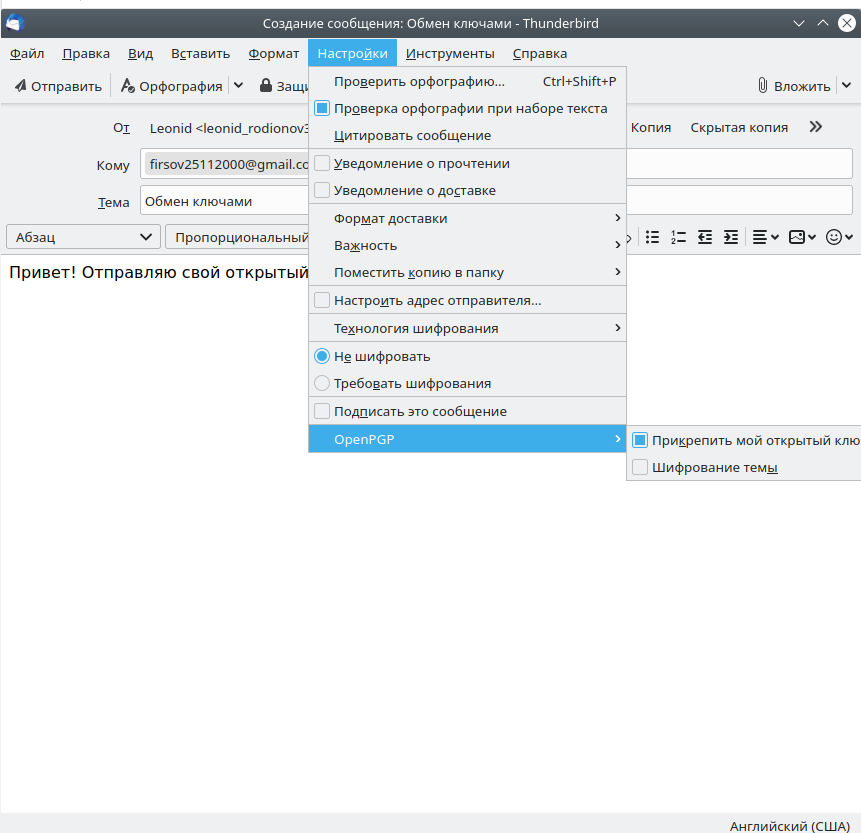


Рисунок – Отправили открытый ключ собеседнику

После этого, аналогичным образом собеседник отправляет свой открытый ключ.

Прием открытого ключа:

На скриншоте ниже произошло недопониманием с коллегами: вместе с открытым ключом прикрепили еще и электронную подпись, которую пока невозможно проверить, ключ импортируется следующим образом:

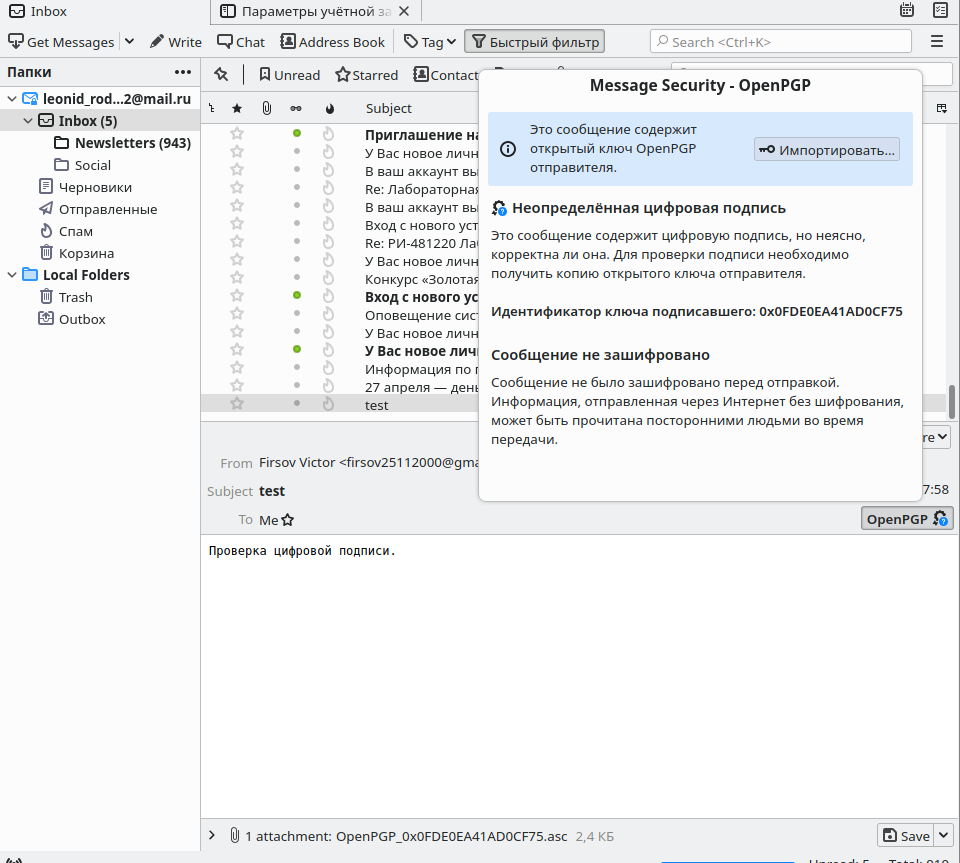


Рисунок – Импортируем ключ

Жмем импортировать и подтверждаем

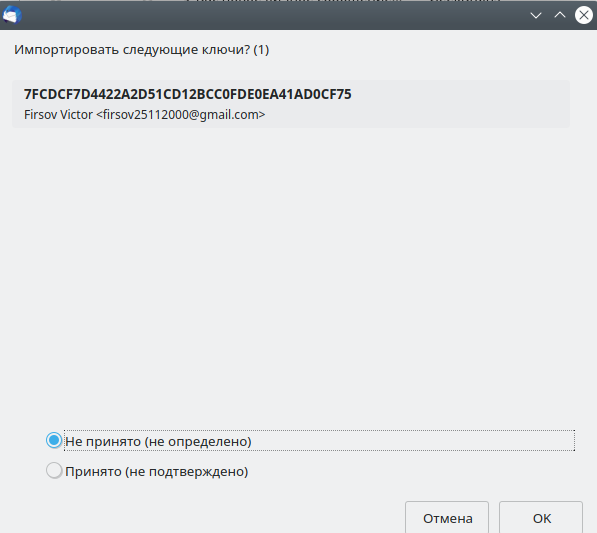


Рисунок – Подтверждение импорта ключа

Выбираем принято

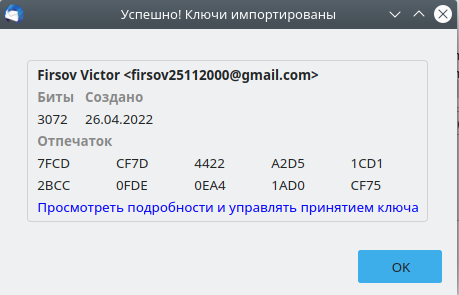


Рисунок – Уведомление об успехе импорта

Теперь отправим собеседнику свое сообщение, подписанное электронной подписью

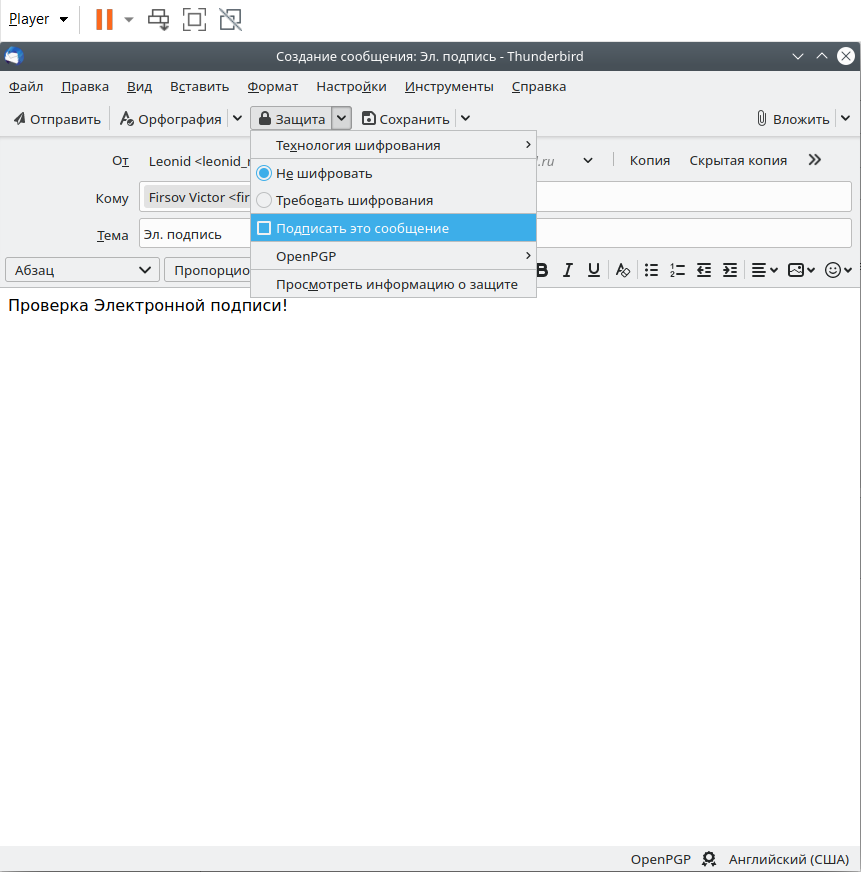


Рисунок – Подписываем сообщение электронной подписью

Теперь вместе с нашим сообщением отправляется зашифрованная открытым ключом контрольная сумма сообщения. Если сообщение будет изменено в процессе передачи, наш собеседник увидит предупреждение от PGP об искажении содержимого.

Прием письма с электронной подписью:

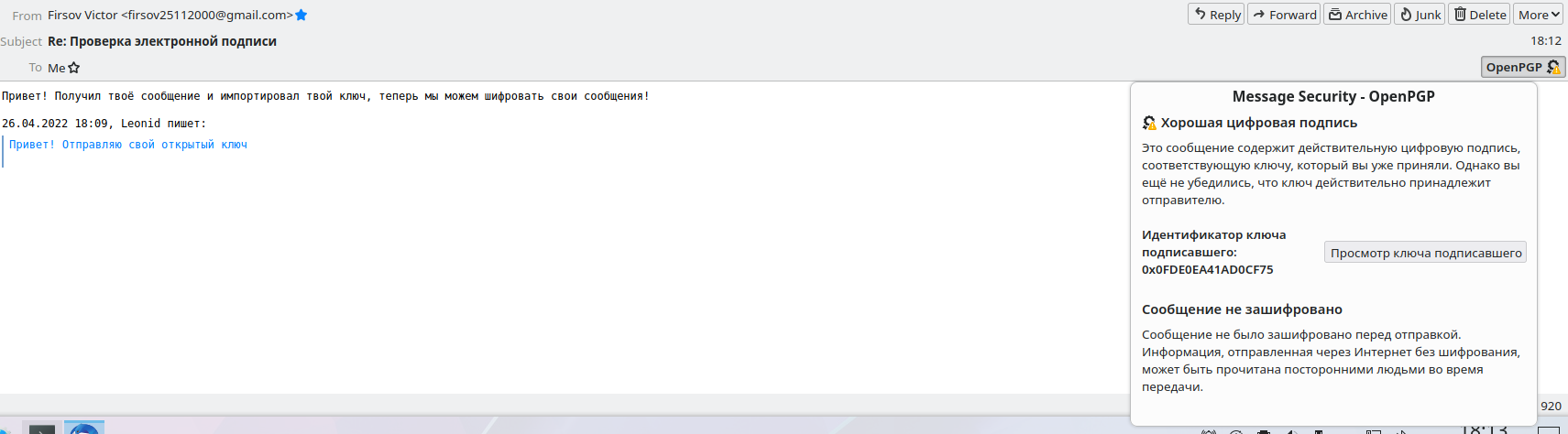


Рисунок – Параметры OpenPGP полученного подписанного письма

Теперь, когда мы убедились, что ключи шифрования корректно установлены и работают, отправим и примем зашифрованные методом RSA сообщения

Прием зашифрованного письма:

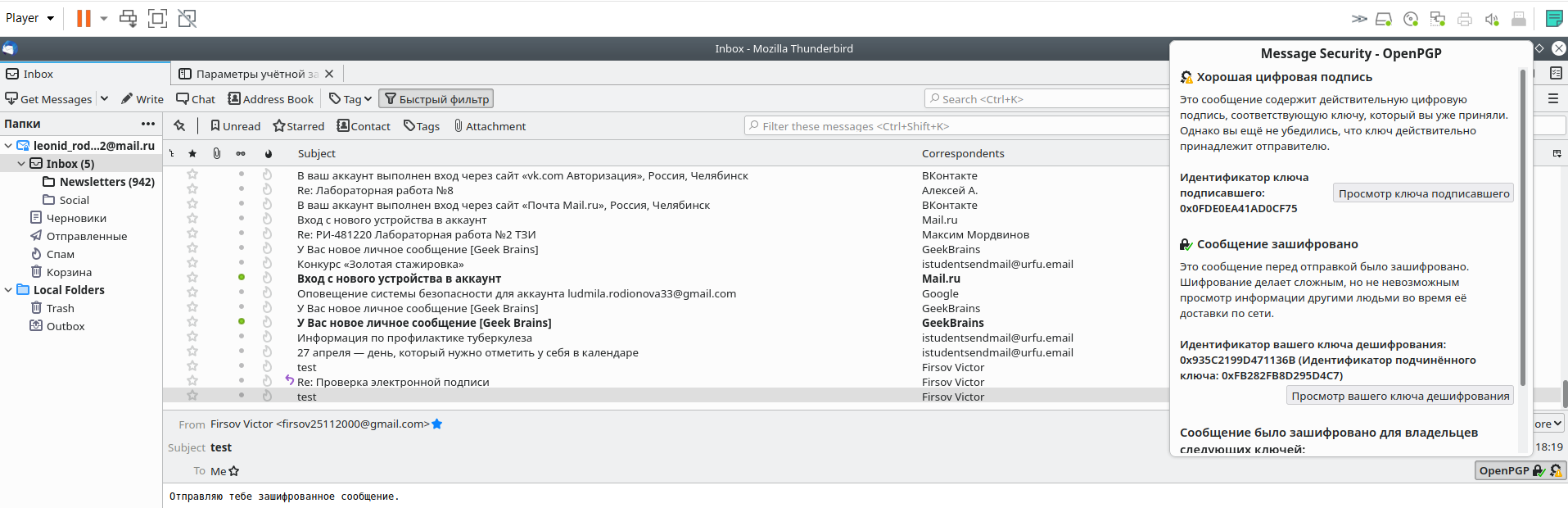


Рисунок – Параметры зашифрованного сообщения

Отправка зашифрованного письма:

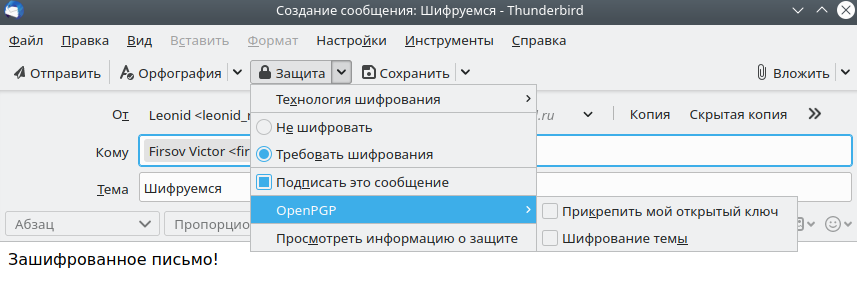


Рисунок – Отправка зашифрованного письма

Посмотрим, какой трафик отправляется при передаче зашифрованного сообщения, создадим письмо, запустим захват трафика в Wireshark и попробуем перехватить содержимое

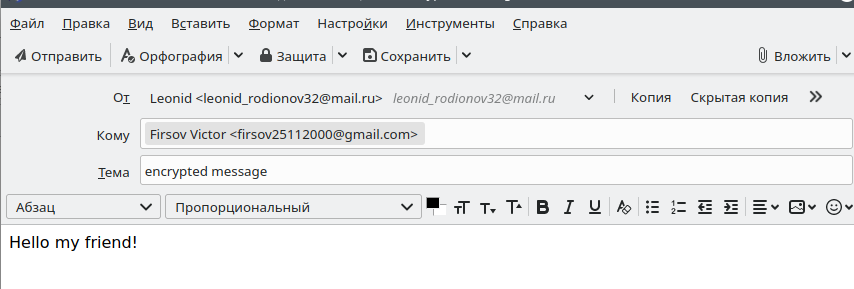


Рисунок – Создаем шифрованное письмо

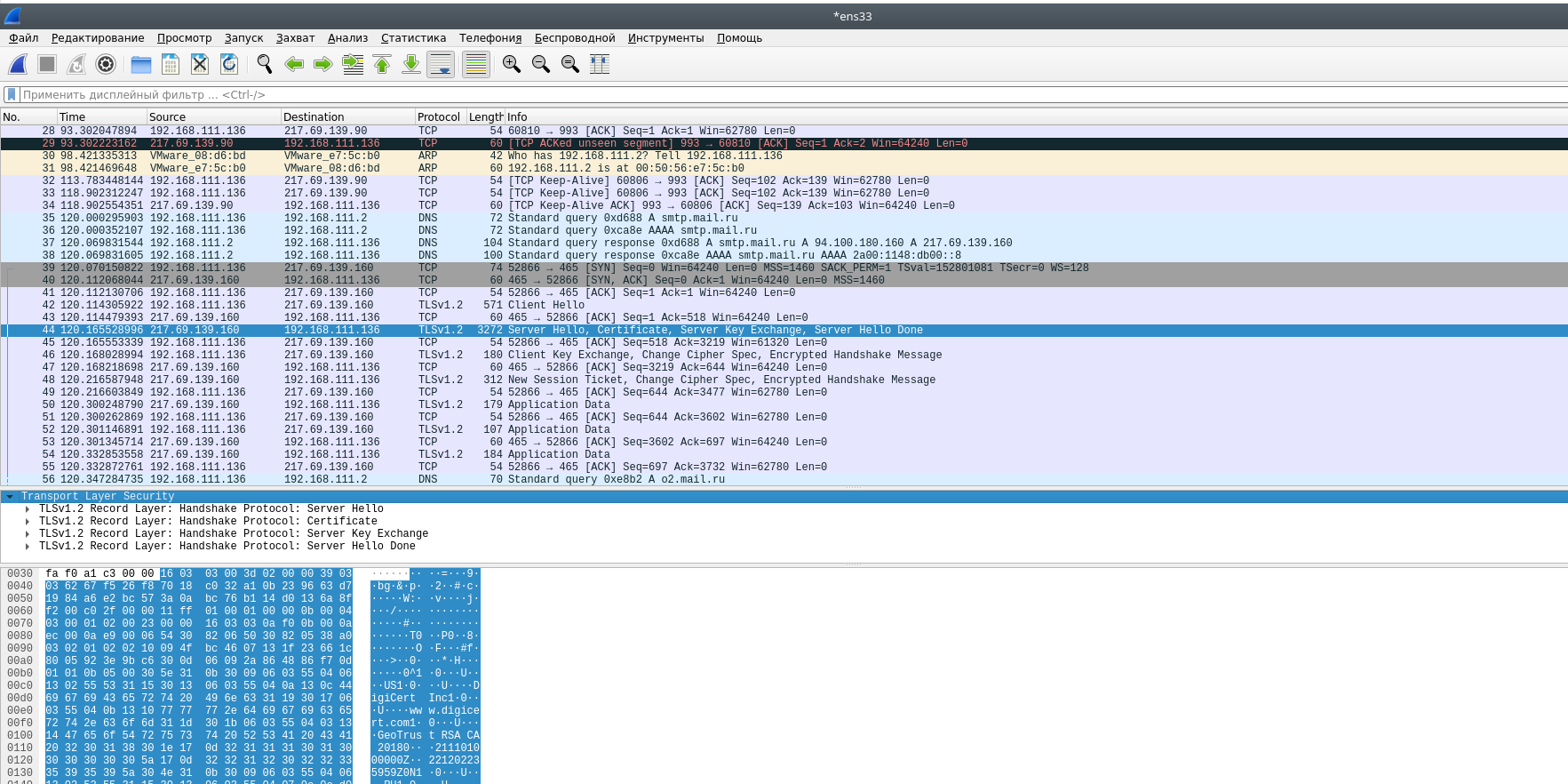


Рисунок -Захваченные при передаче письма пакеты

Ни в одном из пакетов мы не можем увидеть содержимого письма, так как трафик зашифрован

**Выводы:**

В результате выполнения данной лабораторной работы мы на примере почтового клиента Thunderbird научились настраивать защищенный канал передачи информации. Благодаря протоколу IMAP и асинхронному шифрованию содержимое писем будет практически невозможно расшифровать. Если же такие меры защиты не принимаются или злоумышленник, перехватив письмо на одном из промежуточных узлов связи (например атака MITM), изменил содержимое, то на приемном конце получатель увидит изменения благодаря электронной подписи.