**Лекция 16**

**Шибко Татьяна**

**Задание 3а**

**4 курс 12 группа**

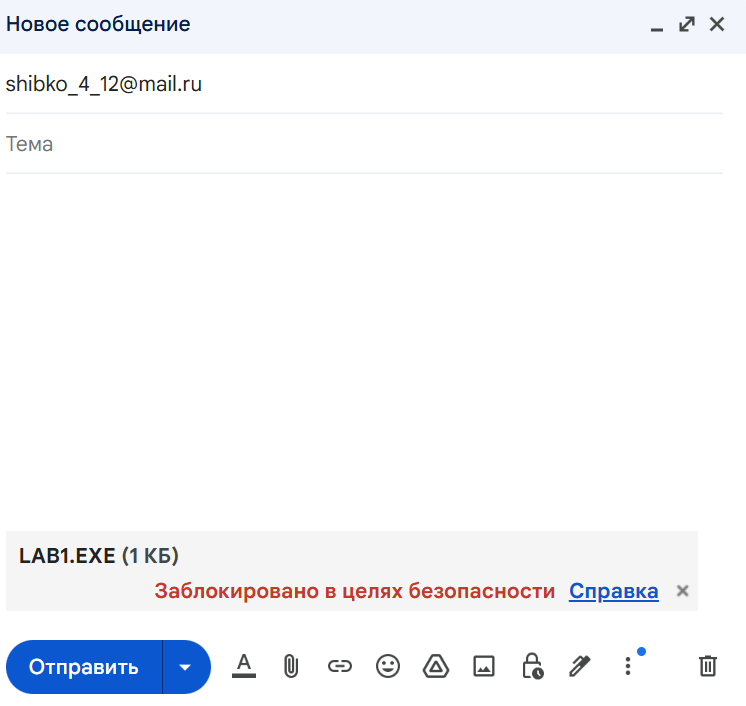
**Условие:**

б). Изучаем вопрос, каким образом различные «почтовики» БОРЯТСЯ с ПЕРЕСЫЛКОЙ исполнимых модулей и как можно «обмануть» подобных «почтовиков» и всё-таки переслать файлы, содержащие исполнимые модули. Для этого используем (заводим) почтовый ящик на gmail.com и проверяем, что происходит, если попытаться переслать исполнимый модуль из почты gmail на почту mail.ru, и что происходит, если из почты mail.ru пересылать на gmail (фиксируем эти факты в виде соответствующего скрин-шота), потом изменяем ТИП файла на txt и пытаемся снова пересылать и фиксируем, что не получилось, затем архивируем исполнимый модуль и проверяем, что происходит если пересылать заархивированный исполнимый файл с gmail на mail.ru, и меняется что-либо, если пересылать исполнимый модуль когда ЭТОТ файл имеет тип txt, и снова с фиксацией результата, после чего архивируем исполнимый модуль с заданием ПАРОЛЯ Zuka2024 и смотрим, что получается и снова фиксируем. Если всё равно не получается отправить, ещё раз архивируем уже заархивированный файл с тем же паролем и фиксируем результат. ДО КОНЦА ДНЯ присылаем мне на почту РЕЗУЛЬТАТ — ОТЧЕТ О ПРОДЕЛАННОЙ РАБОТЕ И ФАЙЛ, СОДЕРЖАЩИЙ ИСПОЛНИМЫЙ МОДУЛЬ, ОТПРАВЛЕННЫЙ ПО ПОЧТЕ из почтового ящика на gmail. в) Исследовать вопрос, что имеет место быть при использовании сервера bsu, проделав всё, что сделано в пункте б.

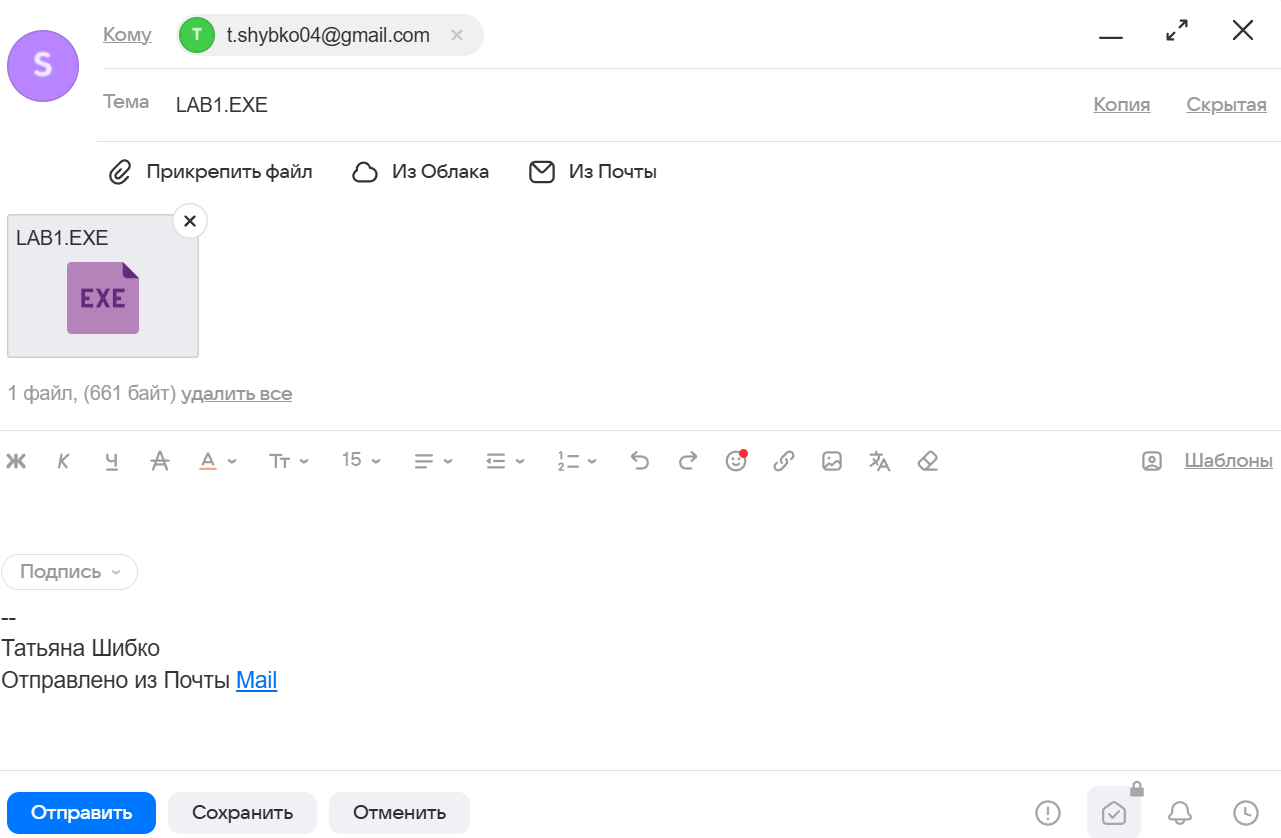
**Ход решения:**

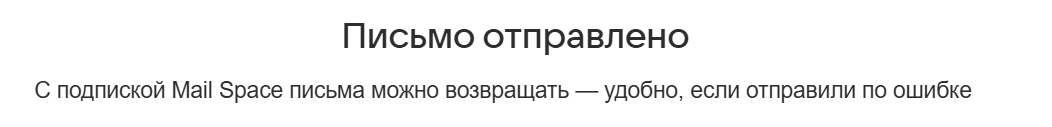
Перейдём к части б.

Сначала попробуем отправить исполнимый модуль с gmail на mail.

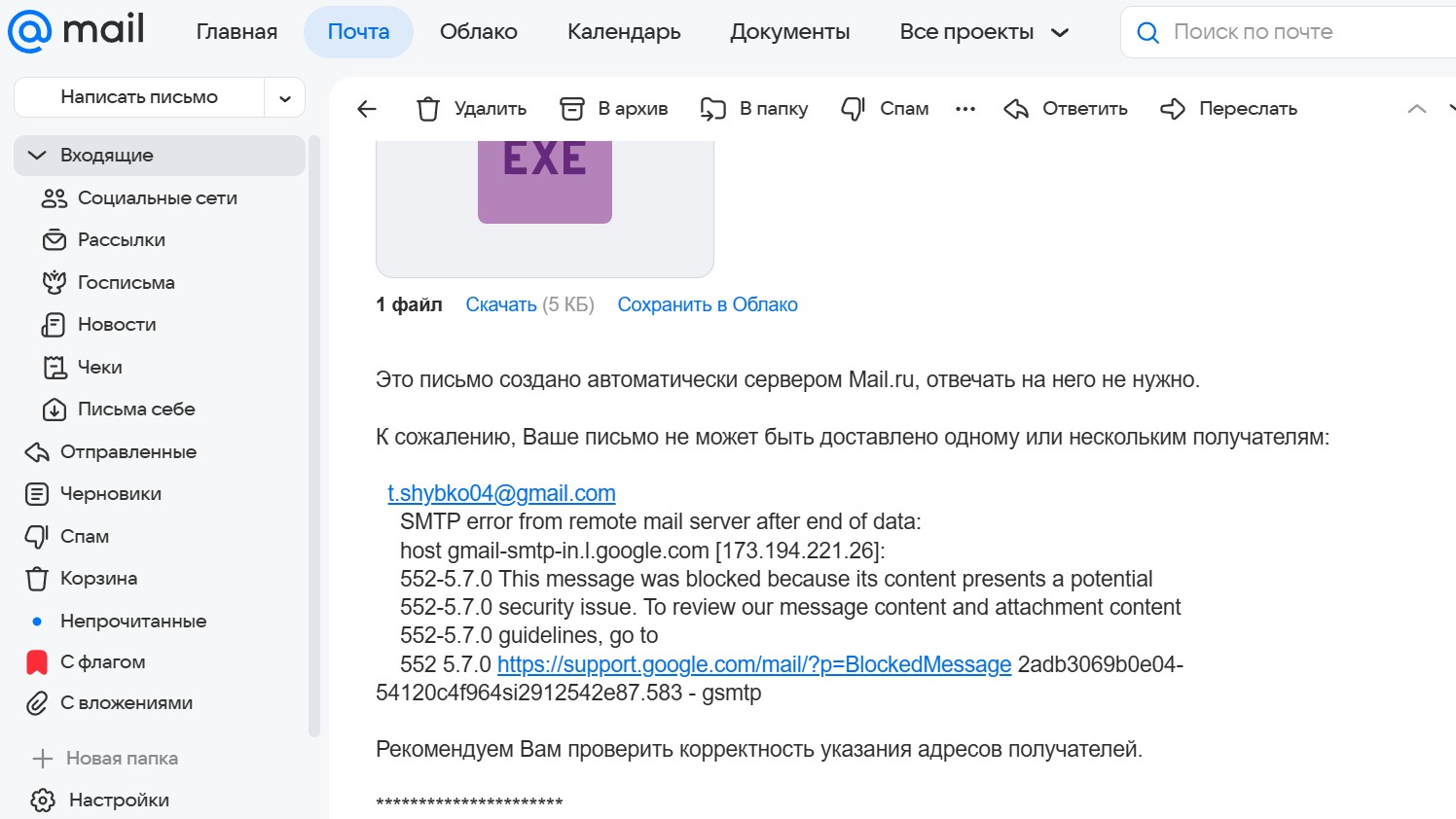


Теперь наоборот:

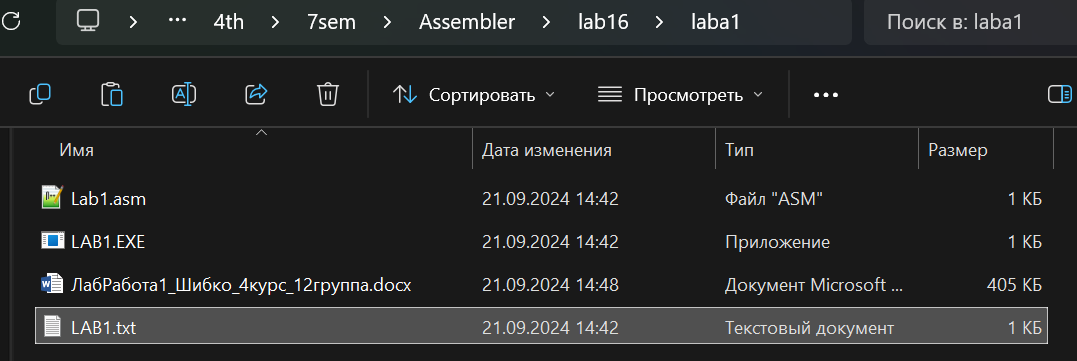


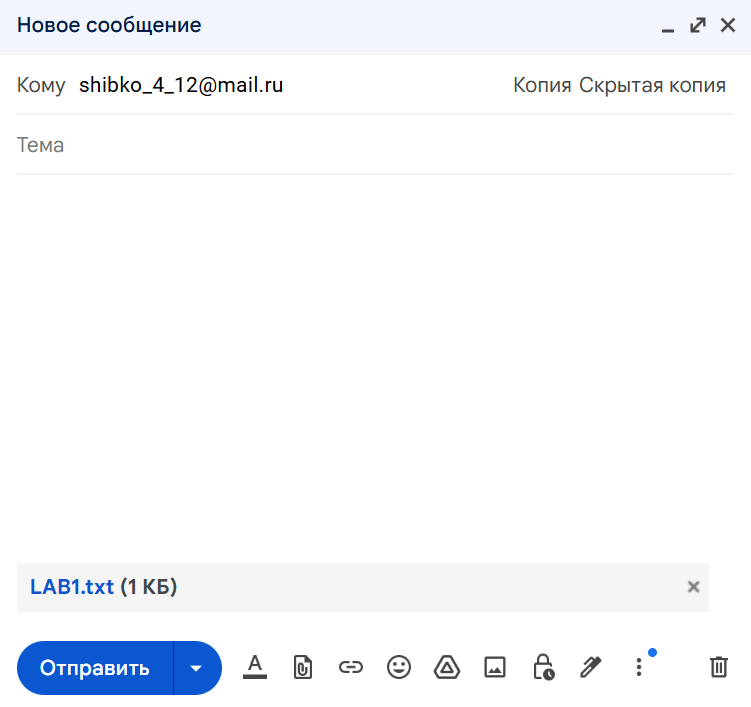


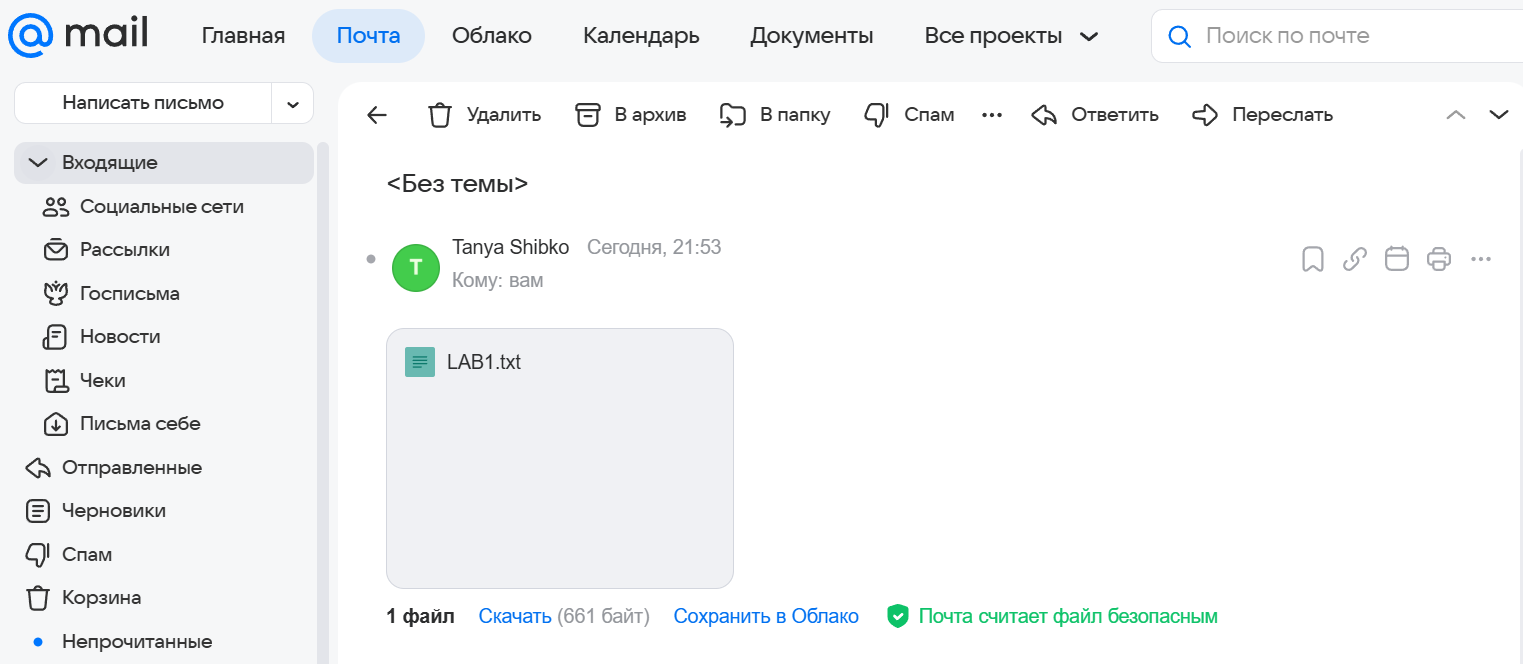
В ответ получаем вот такое письмецо:



Теперь я скопирую этот файл и переименую его как «lab1.txt». Далее на скриншотах будет изображены попытки отправить из gmail в mail и наоборот.

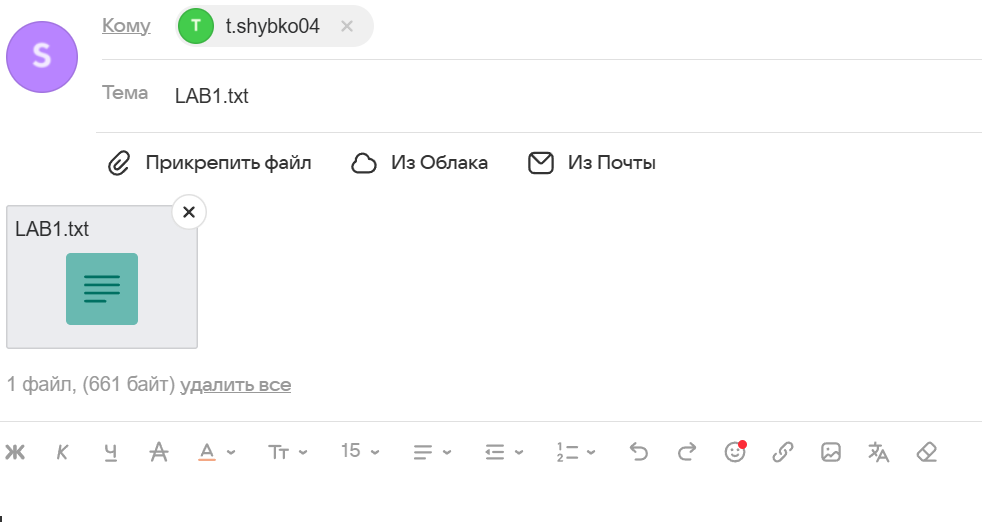


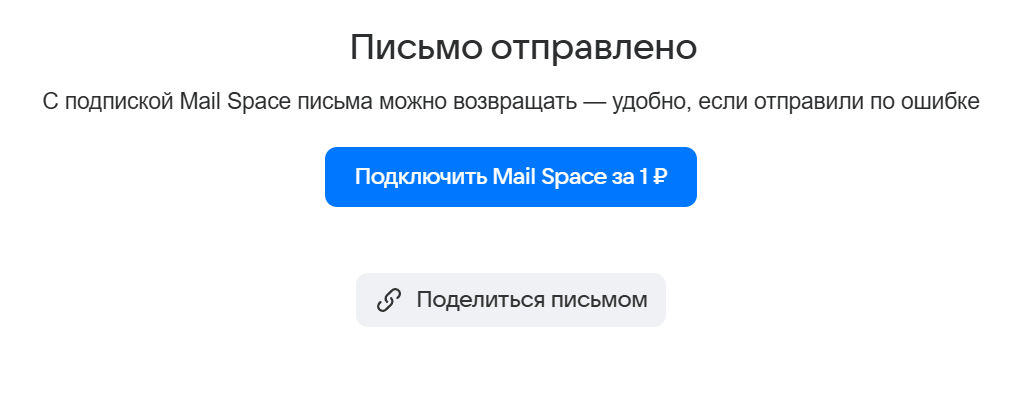


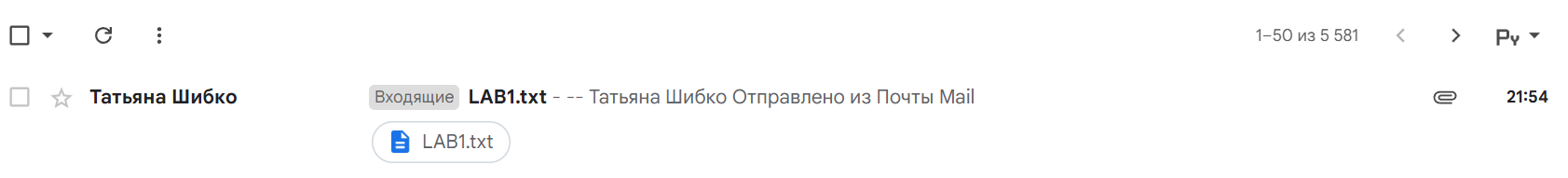


Как видим, письмо дошло и всё в порядке.

Попробуем наоборот.

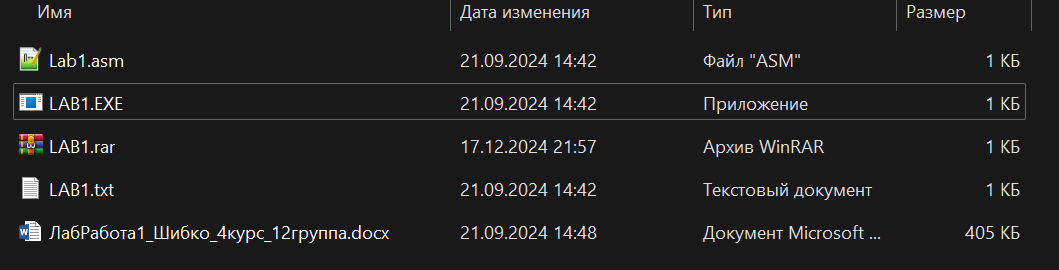




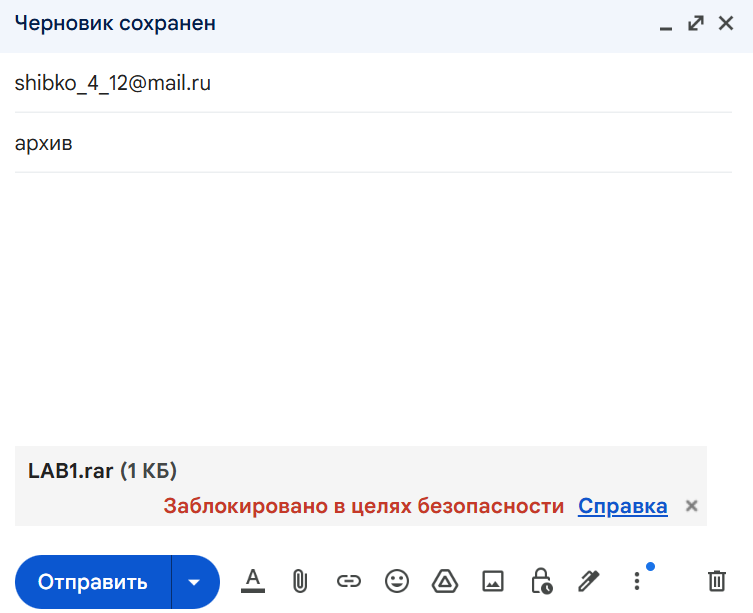


Всё везде пришло. Чудесно.

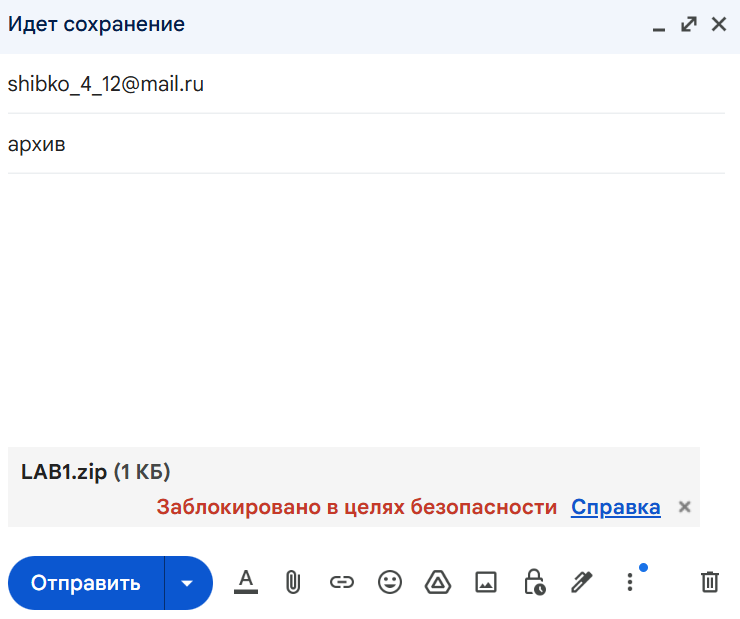
Теперь попробуем проверить архивацию. Я воспользуюсь WinRar.



Чтоб не засорять отчёт, будем пересылать с gmail на mail. Если дойдёт, то и в обратную сторону сработает. По крайней мере, мы будем в это верить.



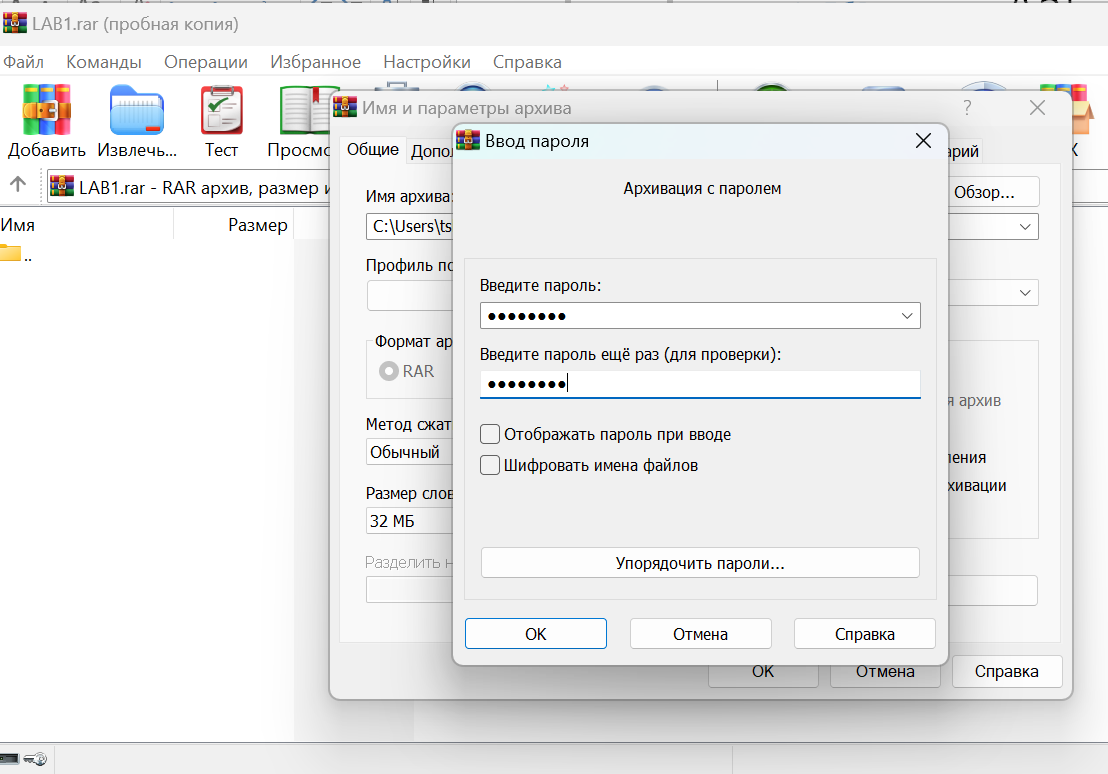
Значит, не судьба нам переслать. Ради эксперимента попробую через зип.



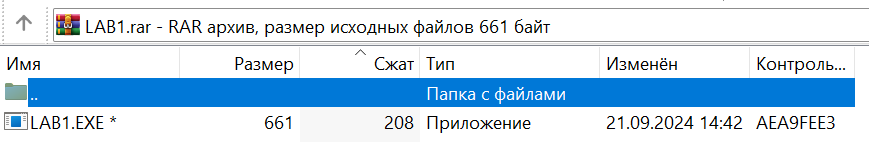
Видимо, никак.

Если мы заархивируем lab1.txt и попытаемся отправить, то оно отправиться 100%. Файл и без архива отправлялся спокойно, так что данный момент я фиксировать не буду.

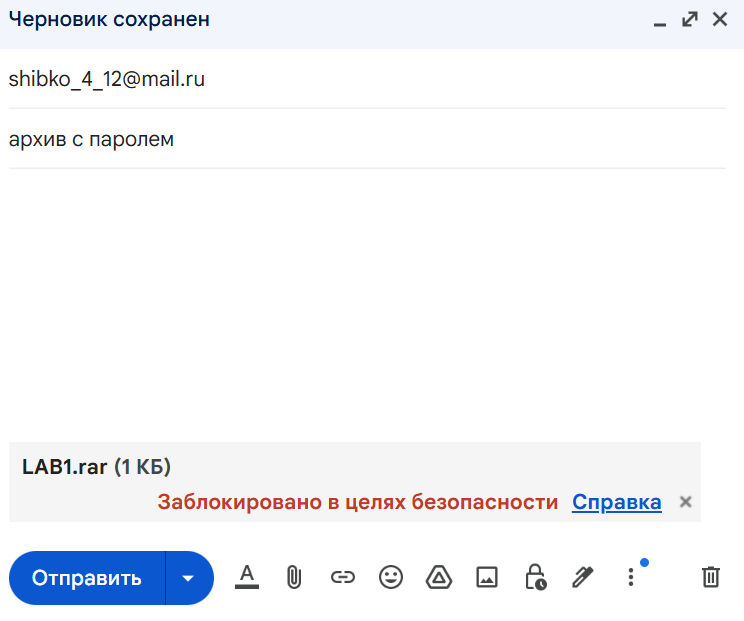
Перейдём к фиксации с паролем Zuka2024.



Видим, что пароль установился:

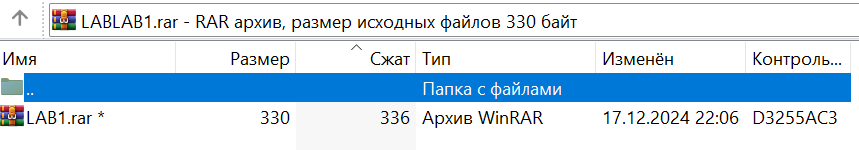


Теперь к пересылке.

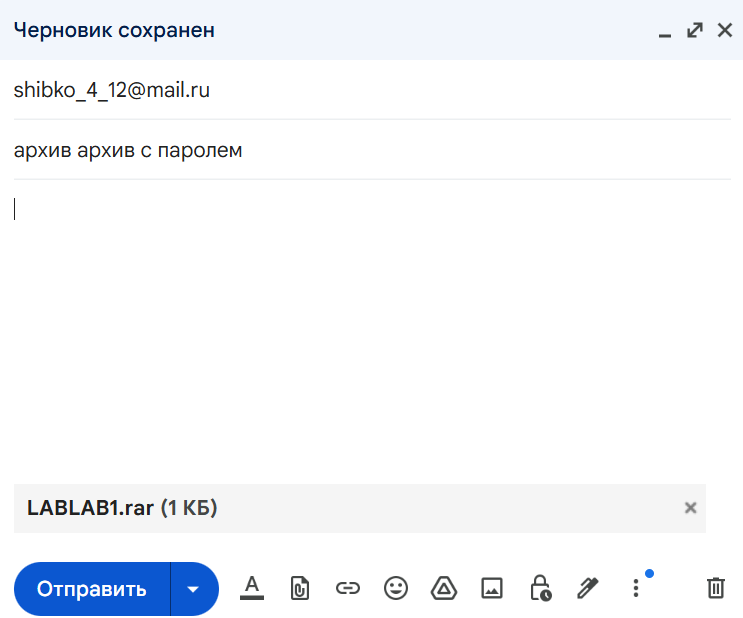


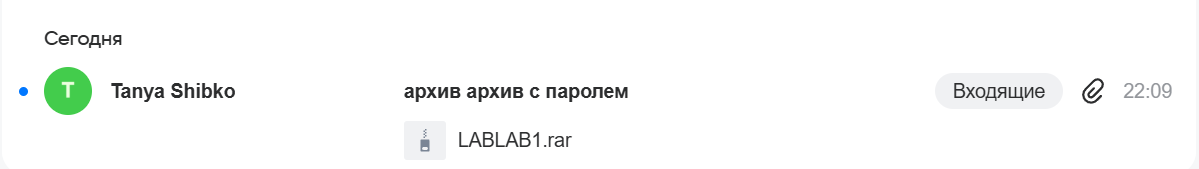
И снова нельзя.

Заархивируем архив:



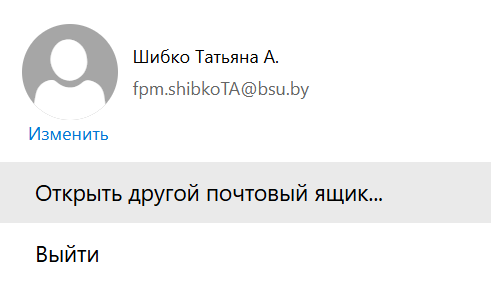
Снова перешлём.





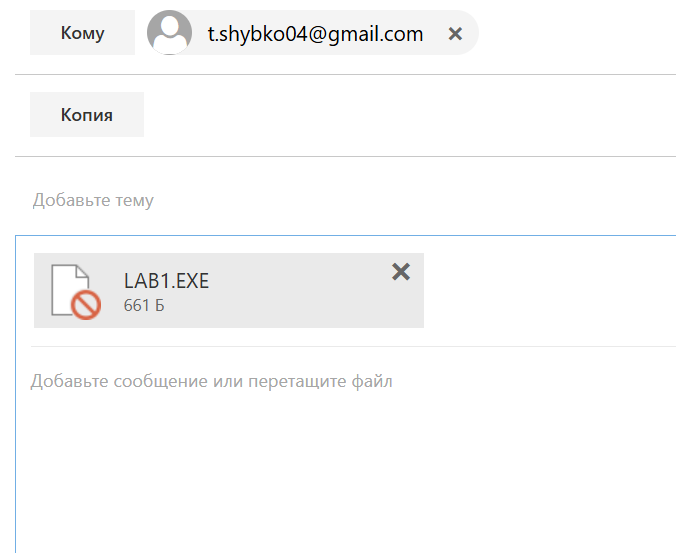
Получилось.

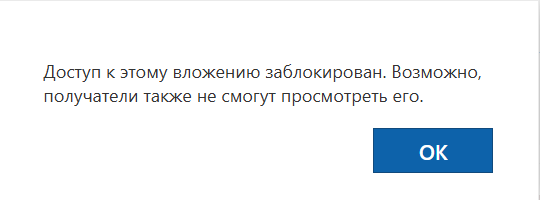
Для финальной части мне понадобиться университетская почта:



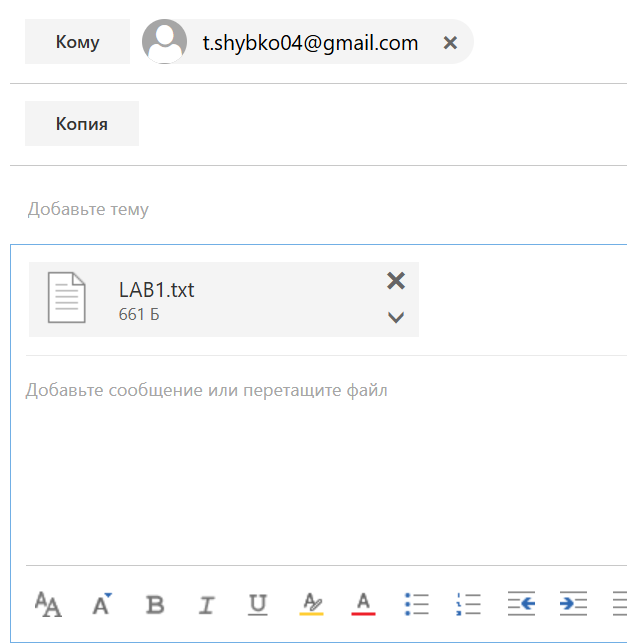
Пересылка будет с outlook на gmail. Для разнообразия.

Начнём с обычного исполнительного модуля.

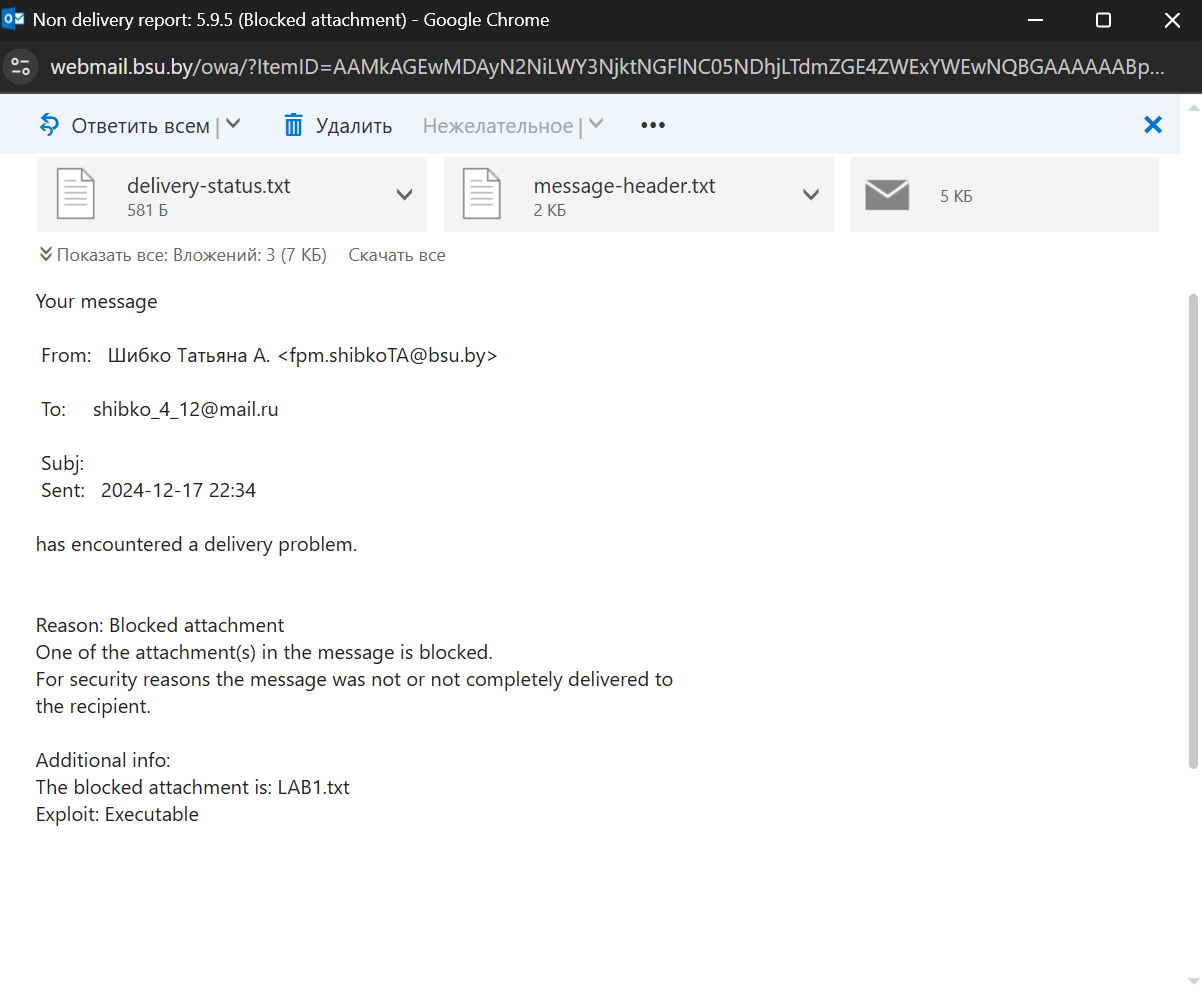




Не получилось. Пробуем .txt

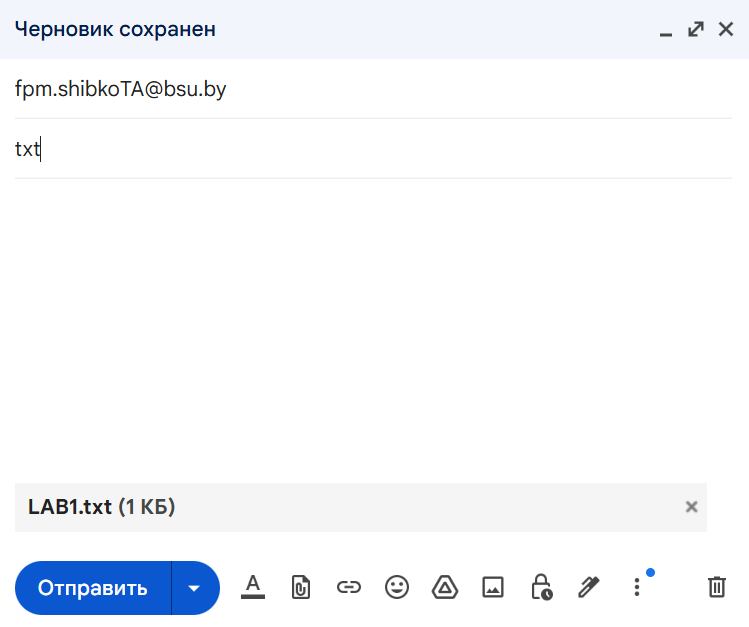


Далее была попытка отправить сообщение на другую почту. И тут я заметила, что мне приходило уведомление:

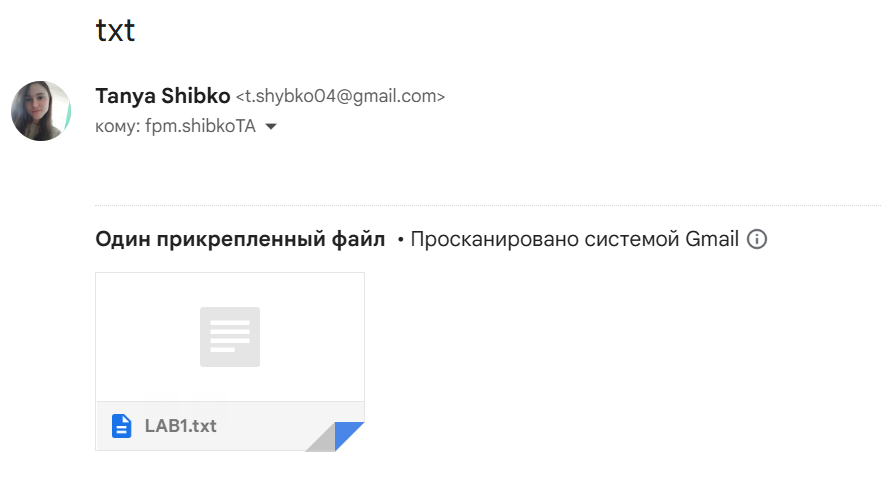


Есть кратко – мне заблокировали вложение, поэтому письмо не отправлено.

Попробую отправить с gmail.

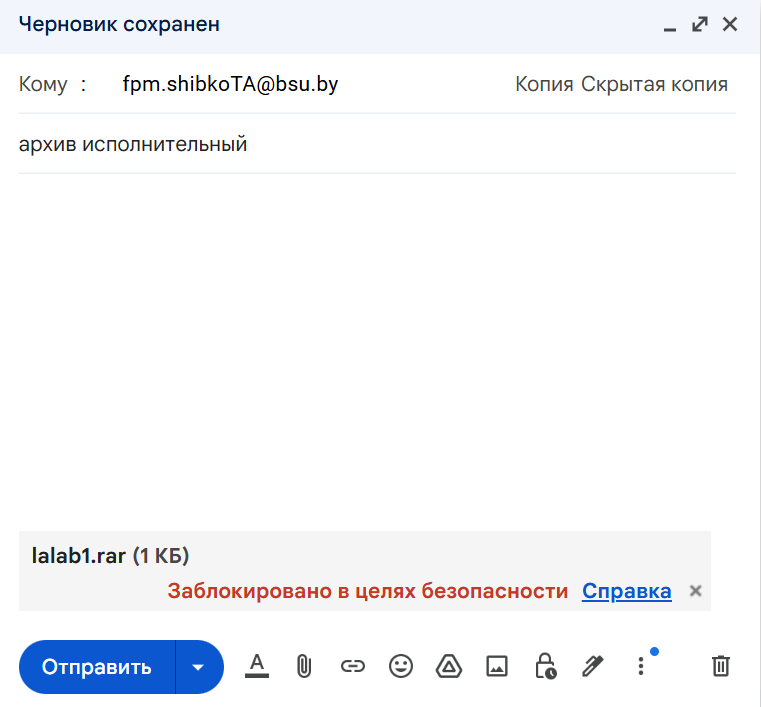


Само письмо отправлено:

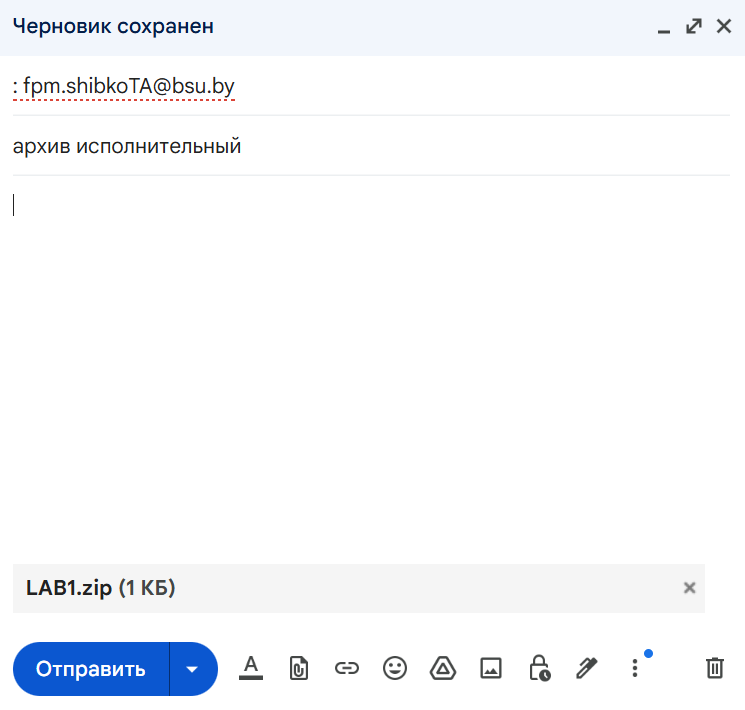


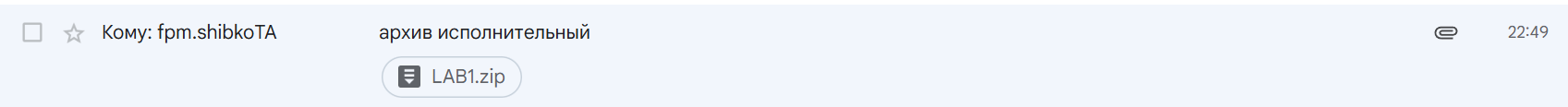
Но так и не дошло. Ладно, будем считать, что не вышло и двигаться дальше.

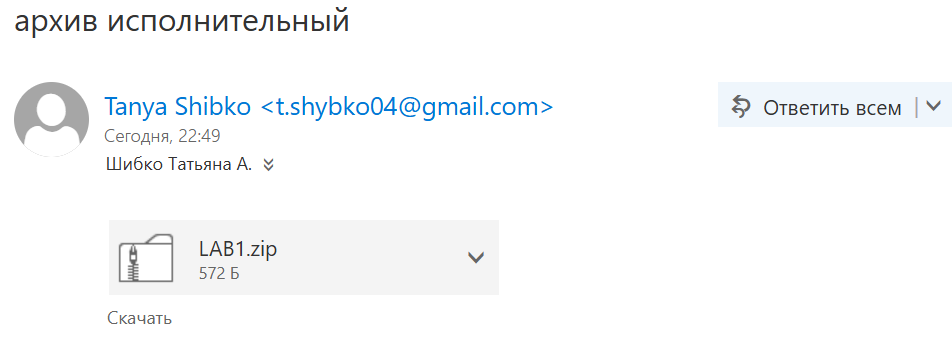
Теперь попробуем заархивированный Lab1.exe. Буду пересылать с gmail на outlook.



Это мы уже проходили. Перейдём к архиву с txt.

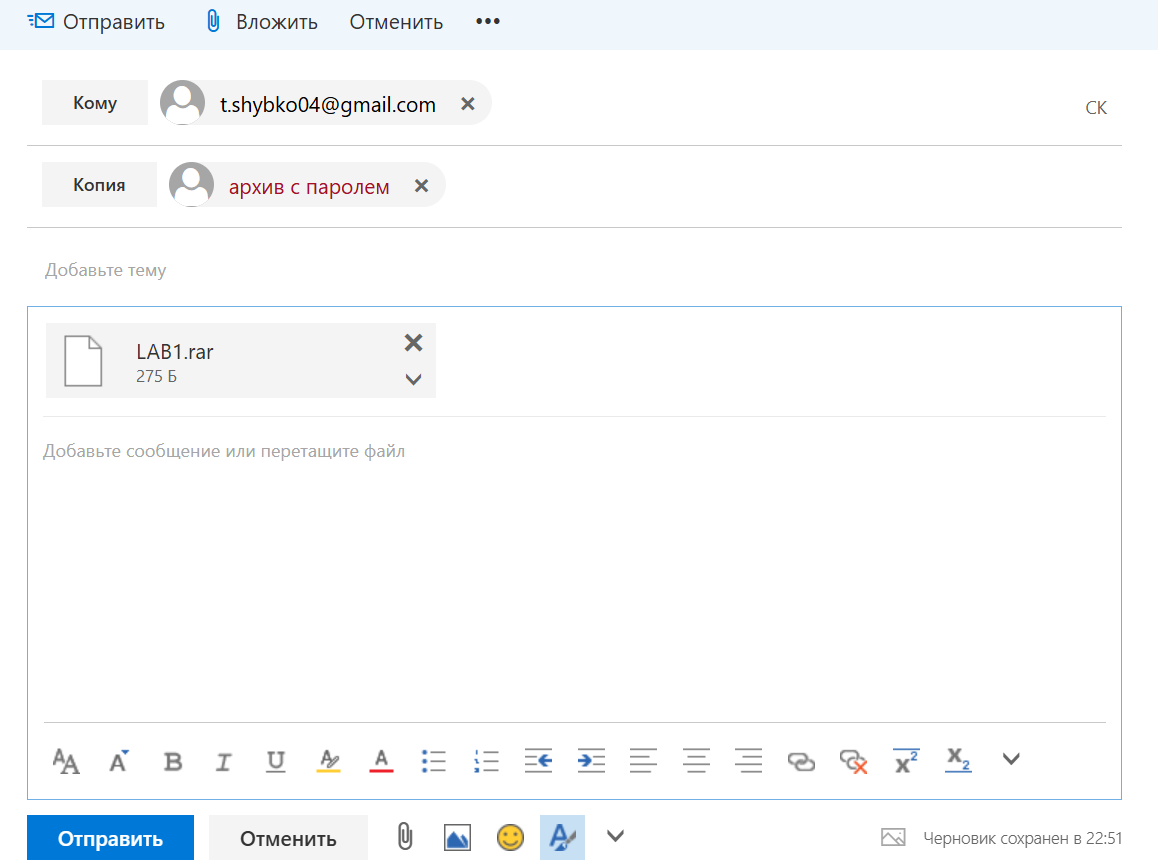


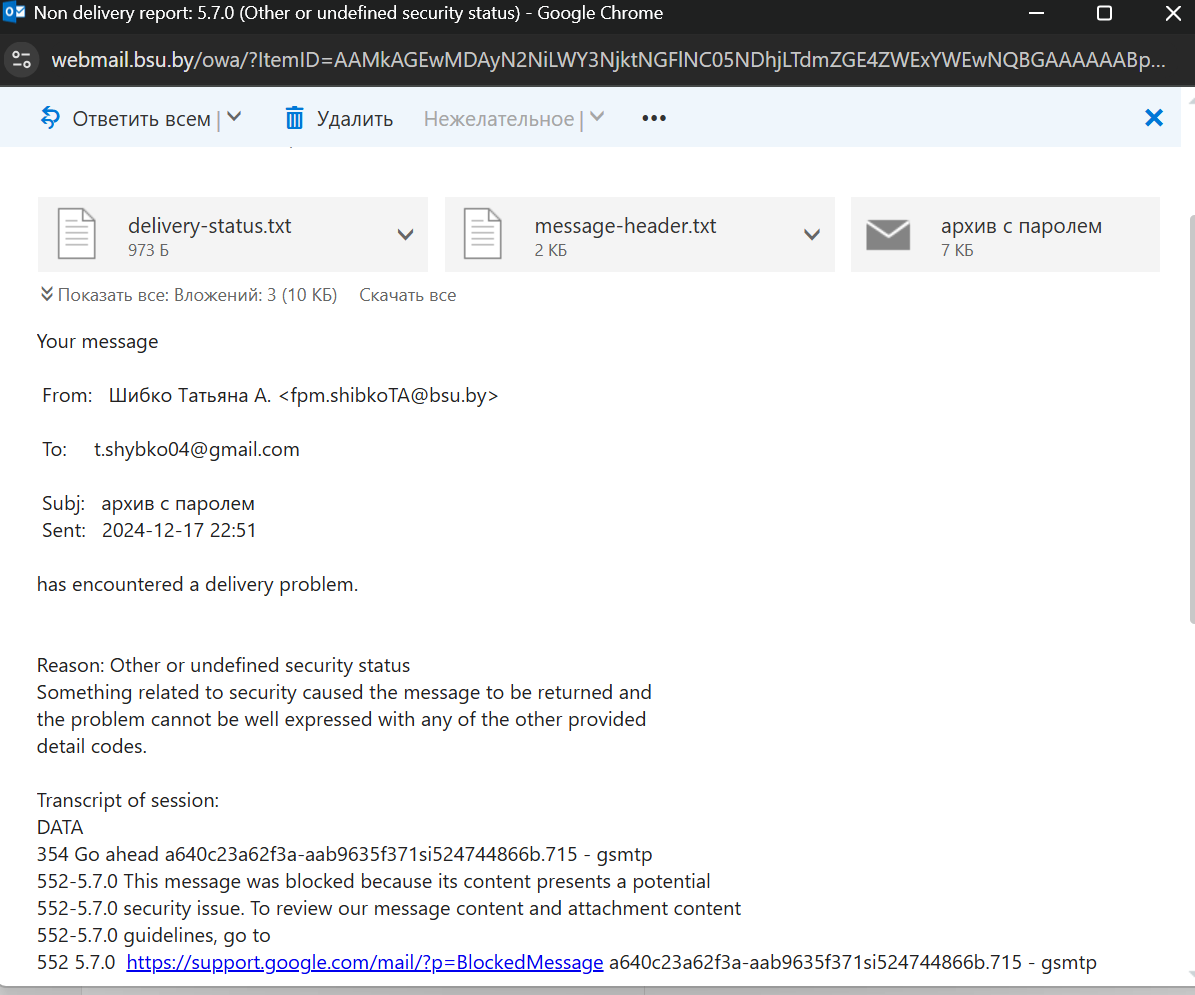




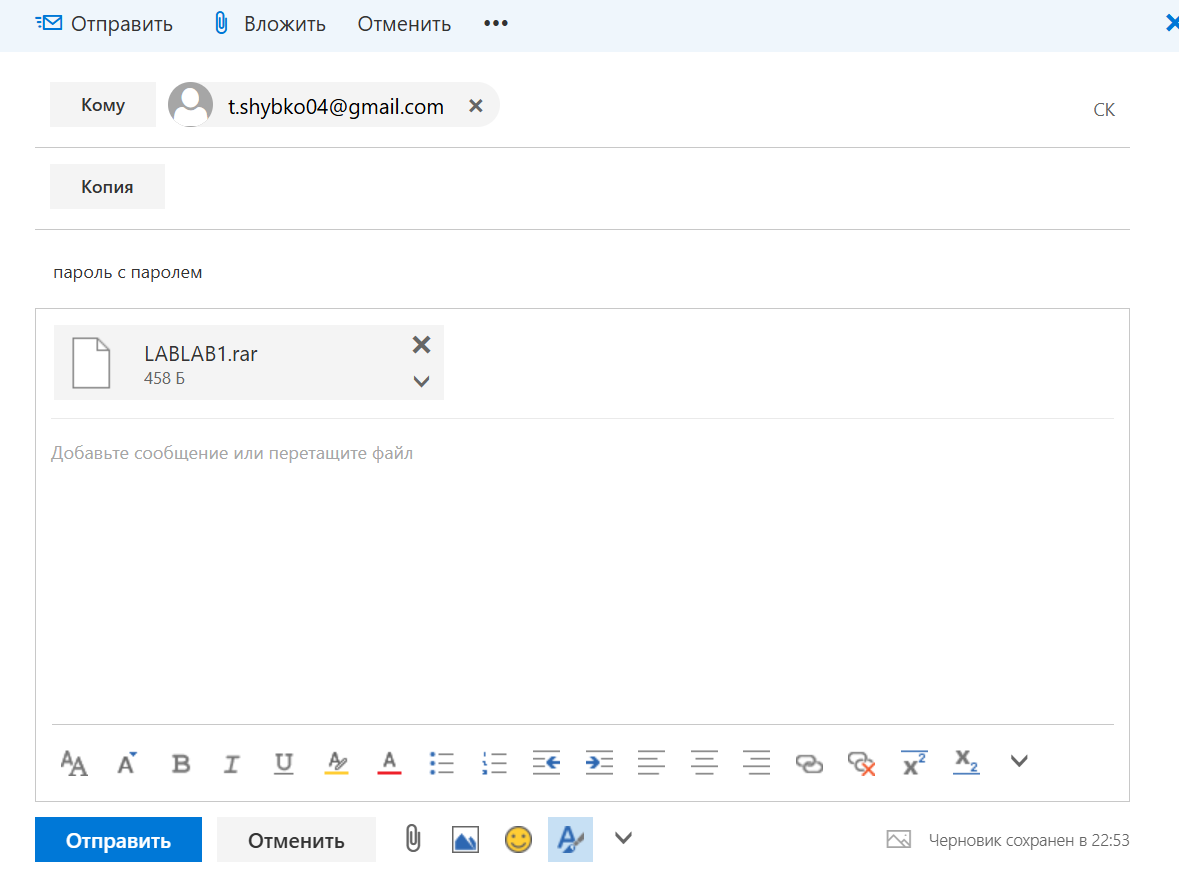
Дошло. Отлично.

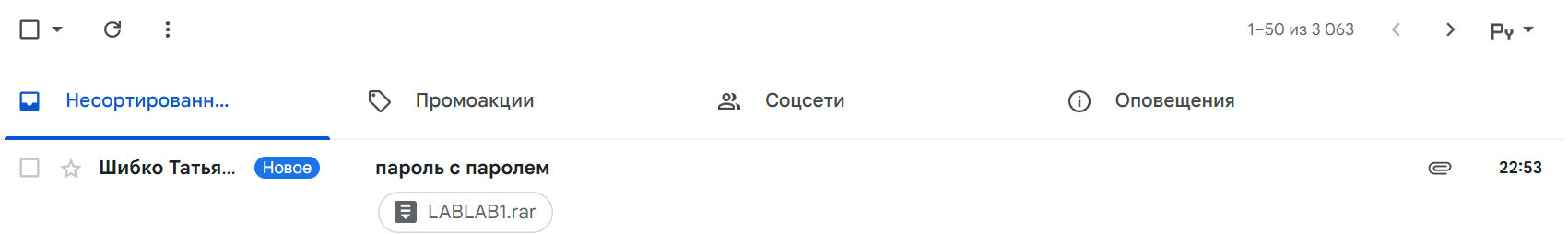
Переходим к паролям. Сначала просто с одним паролем.





Уже знакомая нам ошибка. Значит, отправим запароленный архив.





Как можем видеть, всё пришло.

Ответ на вопрос «Каким образом gmail определяет, что делается попытка переслать отдельно исполнимый модуль и исполнимый модуль в заархивированном виде»:

Gmail и другие почтовые сервисы используют несколько способов для определения исполняемых файлов. Они проверяют расширения файлов, например, .exe и .bat, и блокируют их, чтобы избежать вредоносного ПО. Кроме того, некоторые сервисы могут анализировать содержимое файлов, чтобы выявить исполняемые модули, даже если они находятся в архиве. Запароленные архивы не подвергаются проверке, поэтому могут проходить фильтры, в то время как обычные зашифрованные архивы могут быть проанализированы. В итоге, Gmail и Mail.ru более гибкие в фильтрации, чем Outlook, который строже относится к потенциально опасным файлам.