

Как сделать электронную переписку юридически значимой

RTM TECHNOLOGIES — первая экспертная компания, специализирующаяся на проведении нормативных и нормативно-технических экспертиз в области ИБ и ИТ.



СОДЕРЖАНИЕ

01 **Исследование электронной переписки**

- С помощью каких сервисов может осуществляться электронная переписка?
- В каких случаях происходят обращения к экспертам с целью исследования переписки в электронном виде?
- Для чего необходима фиксация электронной переписки?
- Почему экспертное заверение электронной переписки надёжнее, чем у нотариуса?
- Какие сведения фиксируются при экспертном исследовании электронной переписки?

02 **Аудиосообщения, документы и видеозаписи в переписке как самостоятельные объекты исследования**

- Какие методы анализа могут применяться для исследования аудиосообщений, документов и видеозаписей?
- Как проводится исследование аудиосообщений, документов и видеозаписей при заверении электронной переписки?

03 **Фальсификация электронной переписки – как мы выявляем подделку**

04 **Примеры имитации электронных сообщений**

05 **Возможно ли однозначно подтвердить истинность или ложность электронного письма?**

С помощью каких сервисов в подавляющем большинстве осуществляется электронная переписка



Мессенджеры (WhatsApp, Viber, Telegram и т.д.)



Электронная почта (Mail.ru, Яндекс.Почта, Gmail, корпоративные почтовые сервера)



В каких случаях происходят обращения к экспертам с целью заверения переписки в электронном виде?

Споры о взыскании задолженности по договору

Споры между заказчиками и исполнителями работ

Угрозы и оскорбления в социальных сетях

Споры между банками и клиентами

Споры при трудовых отношениях

Для чего необходимо заверение электронной переписки?

Переписка должна предоставляться в суд на материальном носителе для приобщения её к делу

Для предоставления электронной переписки в суд она может быть заверена нотариусом или подвергнута экспертному исследованию

Нотариус может установить факт наличия переписки, но не факт её фальсификации

Некоторые нотариусы осуществляют заверение совместно с экспертами

Почему экспертное заверение электронной переписки надёжнее, чем у нотариуса?

- 1 Анализ реквизитов сообщения в электронной почте/мессенджерах
- 2 Анализ служебных заголовков электронных почтовых сообщений
- 3 Анализ резервных копий и данных, содержащихся на серверах мессенджеров
- 4 Определение IP-адреса отправителя электронных сообщений
- 5 Анализ метаданных файлов, являющихся вложениями к электронным сообщениям



Какие сведения фиксируются при заверении электронной переписки?



Сведения об отправителе/получателе
(почтовый адрес, ФИО или номер телефона)

Вторичные получатели (при наличии)

Дата и время отправки/получения сообщений

Тема электронной переписки (при наличии)

Содержание сообщений электронной переписки,
в том числе, приложения к сообщениям

Аудиосообщения, документы и видеозаписи в переписке как самостоятельные объекты исследования.

Сведения о файлах, содержащихся в электронной переписке, которые фиксируются при исследовании:



Наименование файла

Формат файла

Размер файла

Дата и время отправки/получения

Почтовый адрес, номер телефона или ФИО отправителя и получателя

Тема электронной переписки (при наличии)

Значение хеш-функции

Какие методы анализа могут применяться для исследования аудиосообщений, документов и видеозаписей?

Органолептический и
инструментальный
анализ

Проводится при использовании специализированного программного обеспечения для анализа аудио/видеофайлов.

Анализ метаданных

Осуществляется для всех файлов вложений.

Как проводится исследование аудиосообщений, документов и видеозаписей при заверении электронной переписки?



Исследование содержания текстовых документов



Поиск изменений неситуационных в аудио/видеофайлах



Установление дословного содержания разговора,
зафиксированного в аудио/видеофайлах

Фальсификация электронной переписки – как мы выявляем подделку.

Некоторые сведения о передаче электронных сообщений:



На каждом этапе передачи в электронное сообщение добавляются служебные пометки серверов и клиентов электронной почты



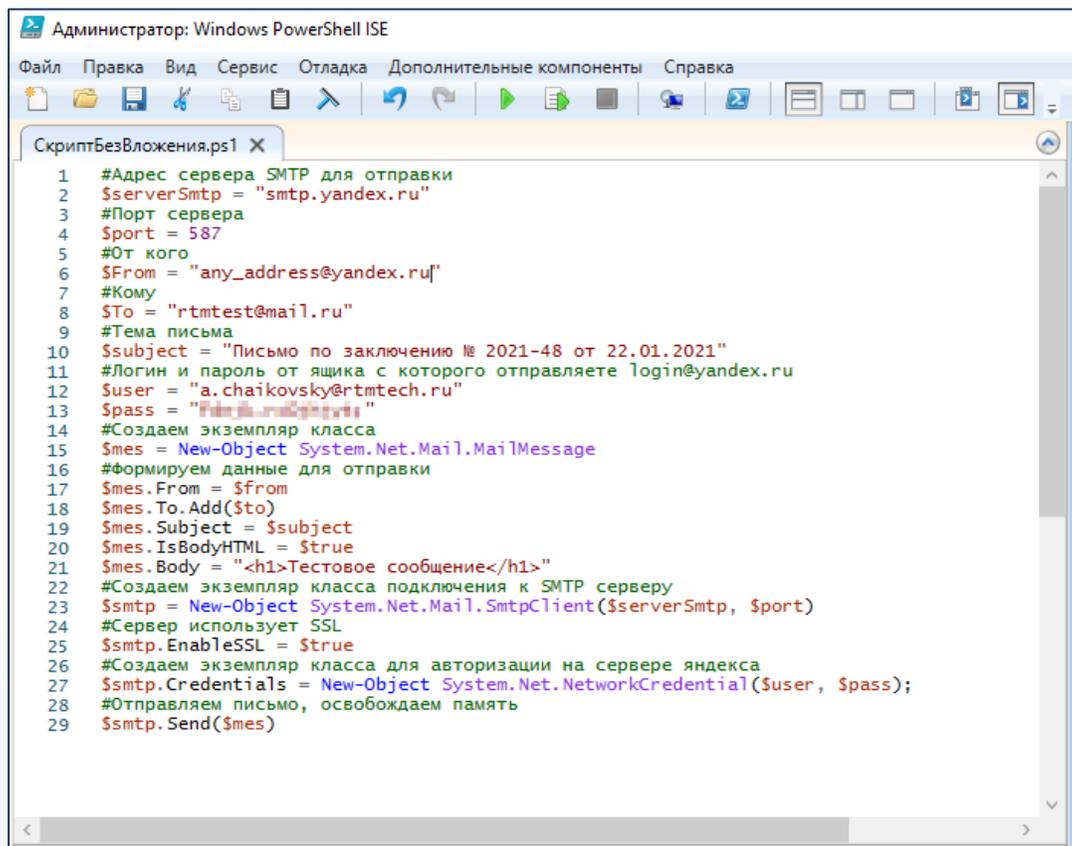
При пересылке почтового сообщения через WEB-клиенты автоматически добавляются дополнительные сведения



Одинаковые по содержанию, но разные по теме электронные письма не могут иметь идентичный URL-адрес

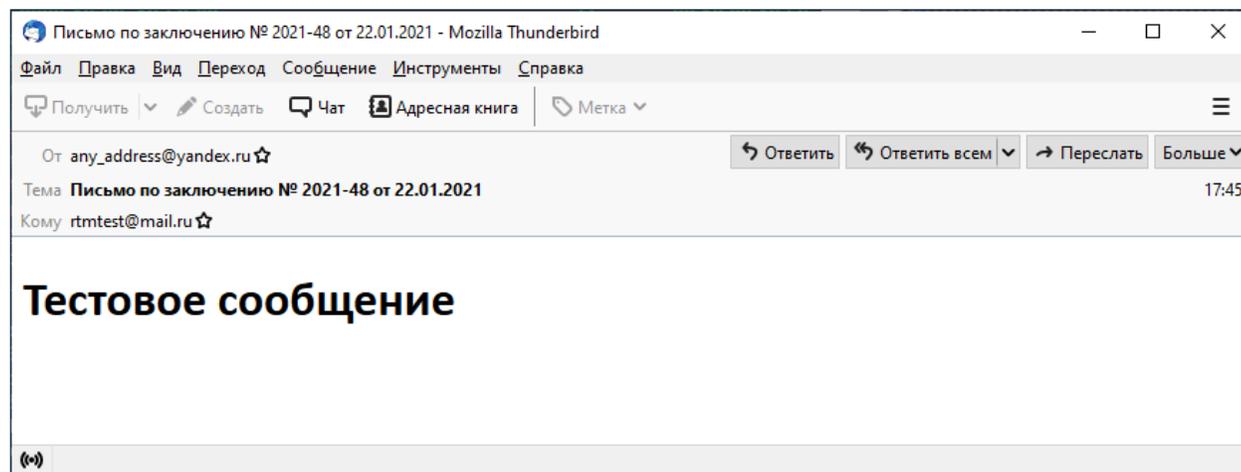
Пример имитации электронных сообщений №1

Для отправки электронного письма могут использоваться как специализированные почтовые клиенты, так и средства программирования на скриптовых языках (power shell, bash и т.д.) либо на языках высокого уровня (java, c++, c# и т.д.).



```
Администратор: Windows PowerShell ISE
Файл  Правка  Вид  Сервис  Отладка  Дополнительные компоненты  Справка

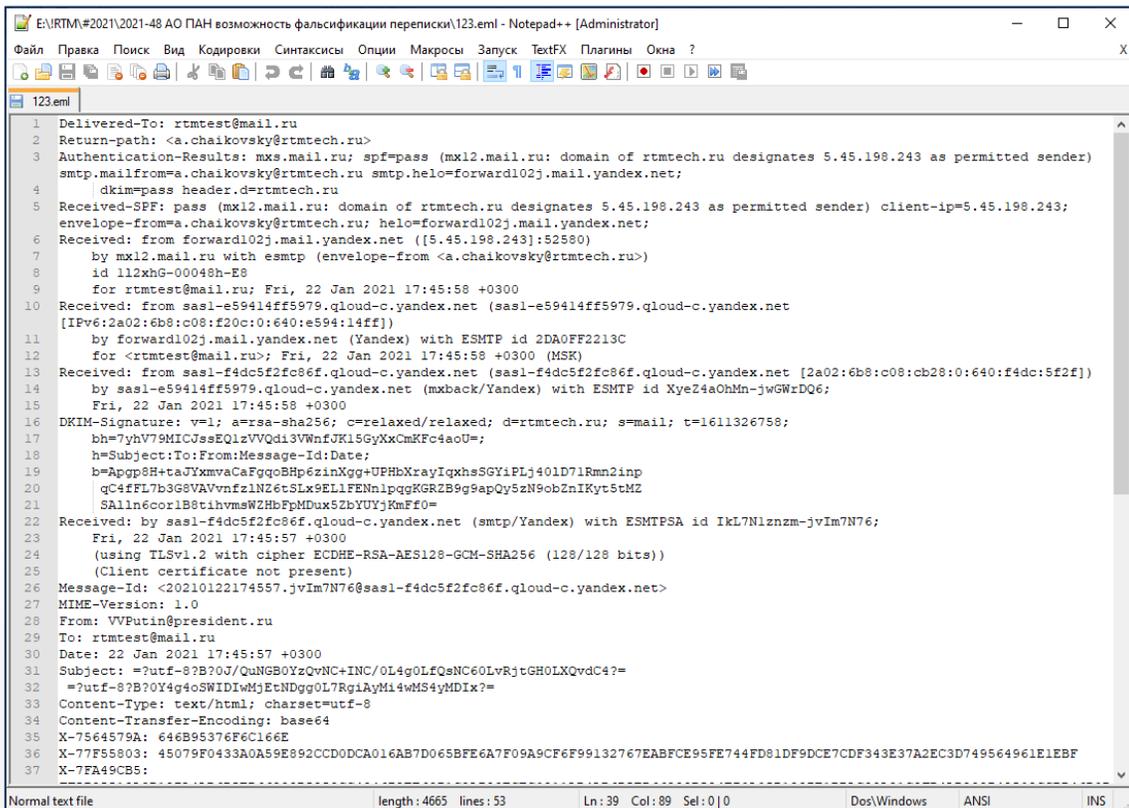
СкриптБезВложения.ps1 X
1 #Адрес сервера SMTP для отправки
2 $serverSmtp = "smtp.yandex.ru"
3 #Порт сервера
4 $port = 587
5 #От кого
6 $from = "any_address@yandex.ru"
7 #Кому
8 $to = "rtmtest@mail.ru"
9 #Тема письма
10 $subject = "Письмо по заключению № 2021-48 от 22.01.2021"
11 #Логин и пароль от ящика с которого отправляете login@yandex.ru
12 $user = "a.chaikovsky@rtmtech.ru"
13 $pass = "P@ssw0rd123456789"
14 #Создаем экземпляр класса
15 $smes = New-Object System.Net.Mail.MailMessage
16 #Формируем данные для отправки
17 $smes.From = $from
18 $smes.To.Add($to)
19 $smes.Subject = $subject
20 $smes.IsBodyHTML = $true
21 $smes.Body = "<h1>Тестовое сообщение</h1>"
22 #Создаем экземпляр класса подключения к SMTP серверу
23 $smtp = New-Object System.Net.Mail.SmtpClient($serverSmtp, $port)
24 #Сервер использует SSL
25 $smtp.EnableSSL = $true
26 #Создаем экземпляр класса для авторизации на сервере яндекса
27 $smtp.Credentials = New-Object System.Net.NetworkCredential($user, $pass);
28 #Отправляем письмо, освобождаем память
29 $smtp.Send($smes)
```



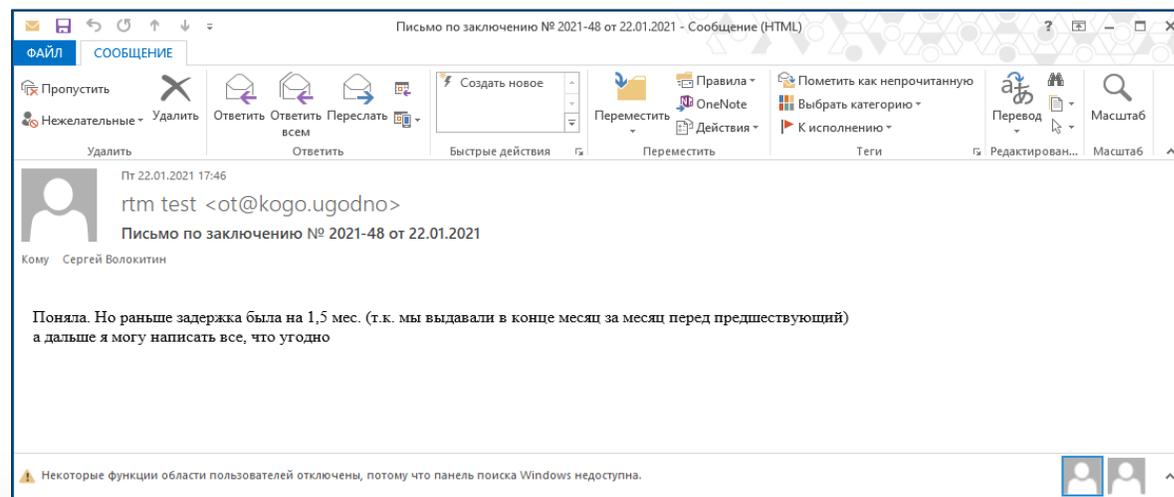
Поддельное электронное письмо будет включено в состав реально существующей переписки.

Пример имитации электронных сообщений №2

Электронное письмо сохраняется в отдельный файл формата *.eml. Формат *.eml универсален, поэтому загрузка и выгрузка применимы для большинства почтовых клиентов.



```
1 Delivered-To: rtmtest@mail.ru
2 Return-path: <a.chaikovsky@rtmtech.ru>
3 Authentication-Results: mxs.mail.ru; spf=pass (mx12.mail.ru: domain of rtmtech.ru designates 5.45.198.243 as permitted sender)
smtp.mailfrom=a.chaikovsky@rtmtech.ru smtp.helo=forward102j.mail.yandex.net;
4 dkim=pass header.d=rtmtech.ru
5 Received-SPF: pass (mx12.mail.ru: domain of rtmtech.ru designates 5.45.198.243 as permitted sender) client-ip=5.45.198.243;
envelope-from=a.chaikovsky@rtmtech.ru; helo=forward102j.mail.yandex.net;
6 Received: from forward102j.mail.yandex.net ([5.45.198.243]:52580)
7 by mx12.mail.ru with esmtp (envelope-from <a.chaikovsky@rtmtech.ru>)
8 id 1l2xhg-00048h-E8
9 for rtmtest@mail.ru; Fri, 22 Jan 2021 17:45:58 +0300
10 Received: from sasl-e59414ff5979.qcloud-c.yandex.net (sasl-e59414ff5979.qcloud-c.yandex.net [IPv6:2a02:6b8:c08:f20c:0:640:e594:14ff])
11 by forward102j.mail.yandex.net (Yandex) with ESMTPE id 2DA0FF2213C
12 for <rtmtest@mail.ru>; Fri, 22 Jan 2021 17:45:58 +0300 (MSK)
13 Received: from sasl-f4dc5f2fc86f.qcloud-c.yandex.net (sasl-f4dc5f2fc86f.qcloud-c.yandex.net [2a02:6b8:c08:cb28:0:640:f4dc:5f2f])
14 by sasl-e59414ff5979.qcloud-c.yandex.net (mxback/Yandex) with ESMTPE id XyeZ4aOhMn-jwGwRDQ6;
15 Fri, 22 Jan 2021 17:45:58 +0300
16 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=rtmtech.ru; s=mail; t=1611326758;
17 bh=7yhV79MICJssEQlzVVQdi3VWnfJK15GyXxcmKFC4aoU=;
18 h=Subject:To:From:Message-Id:Date;
19 b=Appq8H+taJYxmvCaFgqoBHp6zinXgg+UFHbXrayIqxhaSGYiPLj401D7lRmn2inp
20 qC4FLL7b3G8VAVvfnz1N26tSLx9ELLFENnlpqgKGRZB9g9apQy5zN9ob2nIKyt5tMZ
21 SAlln6corlB8tihvmsWZhbFpMDux52hYUYjKmFf0=
22 Received: by sasl-f4dc5f2fc86f.qcloud-c.yandex.net (smtp/Yandex) with ESMTPE id 1kL7N1znzm-jvIm7N76;
23 Fri, 22 Jan 2021 17:45:57 +0300
24 (using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
25 (Client certificate not present)
26 Message-Id: <20210122174557.jvIm7N76@sasl-f4dc5f2fc86f.qcloud-c.yandex.net>
27 MIME-Version: 1.0
28 From: VVPutin@president.ru
29 To: rtmtest@mail.ru
30 Date: 22 Jan 2021 17:45:57 +0300
31 Subject: =?utf-8?B?0Y4g0QuNgB0YzQvNC+INC/0L4g0LQeNC60LvRtGH0LXQvdC4?=?
=?utf-8?B?0Y4g0SWIDIwMjEtNDQg0L7RgiAyMi4wMS4yMDIx?=?
32 Content-Type: text/html; charset=utf-8
33 Content-Transfer-Encoding: base64
34 X-7564579A: 646B95376F6C16E
35 X-77F5803: 45079F0433A0A59E892CCD0DCA016AB7D065BFE6A7F09A9CF6F99132767EABFCE95FE744FD81DF9DCE7CDF343E37A2EC3D749564961E1EBF
36 X-7FA49CB5:
37
```



Несоответствие реального отправителя и отображаемого говорит о факте подделки имени отправителя электронного письма.

Возможно ли подтвердить истинность или ложность электронного письма?

Подтвердить истинность или ложность электронного письма можно в результате комплексного анализа:



Служебных отметок в заголовке письма



Журналов работы почтового сервера отправителя/получателя электронного письма



Информации о факте отправке и/или содержания электронного письма от независимого владельца почтового сервера (Mail.ru, Yandex.ru и т.д.)

Примеры дел



А79-6533/2019 Общество обратилось в Арбитражный суд с заявлением к ИФНС о признании незаконным и отмене решения налогового органа в части предложения уплатить НДС, в обоснование заявленных требований Общество указывает на необоснованный вывод налогового органа об отсутствии документального подтверждения реальности выполненных работ, предъявленных Обществу от имени другого ООО.



А40-107587/2020 Общество обратилось в Арбитражный суд с иском к гражданину, являвшемуся генеральным директором, о взыскании убытков.

СПАСИБО ЗА ВНИМАНИЕ!

Музалевский Федор Александрович

Кандидат физико-математических наук

Ведущий судебный эксперт

Директор технического департамента RTM Group

Волокитин Сергей Анатольевич

Ведущий эксперт компьютерно-технического направления RTM Group



8 800 201-20-70



info@rtmtech.ru



<https://rtmtech.ru>



GroupRTM



rtm.group



@GroupRtm



rtm.group.Russia



t.me/kurilka_ib