

ЭКСПЕРТНОЕ ИССЛЕДОВАНИЕ № [REDACTED]

от «[REDACTED]» [REDACTED] 2019 года

по результатам анализа профиля электронной почты

[REDACTED].ru

Производство исследования начато «[REDACTED]» [REDACTED] 2019 г.

Производство исследования завершено «[REDACTED]» [REDACTED] 2019 г.

Основанием для производства исследования послужил: договор № [REDACTED]
[REDACTED] от «[REDACTED]» [REDACTED] 2019 г. с [REDACTED], в лице Генерального
директора [REDACTED], действующим на основании
Устава.

На исследование представлены:

Логин и пароль для доступа к профилю электронной почты
[REDACTED].ru.

На разрешение эксперту поставлен вопрос:

1. Имеет ли место факт отправки электронного письма с адреса
[REDACTED].ru на адрес [REDACTED].ru [REDACTED]
года в [REDACTED] часов дня темой «[REDACTED]» и
приложены ли документы в сообщении??

Производство исследования поручено [REDACTED]

[REDACTED], уровень подготовки: высшее образование, квалификация - инженер по специальности Информационные системы и Технологии, специальная экспертная подготовка в области производства судебных экспертиз, ученая степень - кандидат физико-математических наук, доцент кафедры Информационных технологий моделирования и управления ВГУИТ. Стаж экспертной работы с июля 2010 года, стаж работы в сфере информационных технологий с мая 2006 года.

Использованы следующие материалы и справочно-нормативная литература:

- ФЕДЕРАЛЬНЫЙ ЗАКОН №73-ФЗ О ГОСУДАРСТВЕННОЙ СУДЕБНО-ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ от 31 мая 2001 г.;
- Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография / В. Б. Вехов. – Волгоград: ВА МВД России, 2008. – 404 с. с илл.;
- Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М., 2001;
- Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М.: Диалектика, 2004. — 432 с. — 3000 экз. — ISBN 5-8459-0733-0, ISBN 0-4712-2357-3;
- [https://www.\[REDACTED\].ru/](https://www.[REDACTED].ru/).

При проведении экспертизы использовались следующие программные и аппаратные средства:

- Интернет-браузер Mozilla Firefox;
- Ноутбук Asus N76V, операционная система Windows 7 Домашняя Расширенная;
- Программное обеспечение Hash Tab;
- Программное обеспечение Notepad ++;
- Дистрибутив Kali Linux Live USB.

===== ОБСТОЯТЕЛЬСТВА ДЕЛА =====

Заказчику необходимо подтвердить либо опровергнуть факт отправки электронного письма и его содержание.

===== ИССЛЕДОВАНИЕ =====

Исследование проводилось в офисе экспертного учреждения по адресу 111398, город Москва, улица Плющева, дом 17, корпус 2, пом. I, ком. 1.

В ходе исследования был запущен интернет-браузер и открыт общедоступный портал электронной почты [REDACTED].ru. Далее были введены учетные данные, предоставленные заказчиком экспертизы.

В связи с доступом из региона ([REDACTED]), отличного от региона пребывания заказчика ([REDACTED]), порталом запрошена дополнительная аутентификационная информация – номер телефона, указанный при регистрации почтового ящика [REDACTED].ru. Данная информация была запрошена посредством электронной почты с адреса эксперта [REDACTED]@rtmtech.ru на адрес представителя заказчика [REDACTED].ru. Ответным сообщением данная информация получена.

В профиле электронной почты произведен поиск полученных сообщений с адреса [REDACTED].ru за указанный период времени.

В результате поиска обнаружено электронное сообщение (см. илл. 1-2).



Иллюстрация 1. Искомое сообщение в профиле почтового ящика.

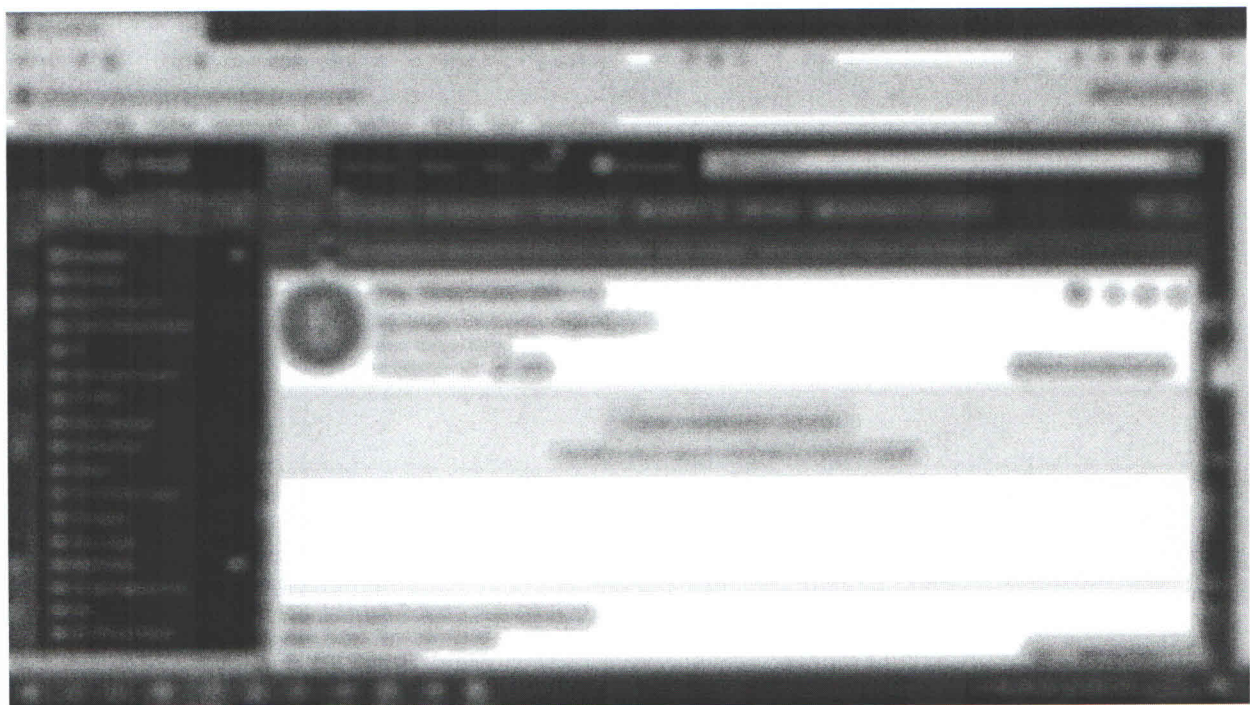


Иллюстрация 2. Искомое сообщение в профиле почтового ящика в открытом виде по ссылке: [https://\[redacted\]](https://[redacted])

Текст письма приведен в приложении 1 к данному заключению (пустые строки удалены).

Письмо имеет вложение – файл [REDACTED]. Файл имеет контрольную сумму (по протоколу MD5) [REDACTED]. Содержимое файла приведено в приложении 2 к данному заключению.

Поскольку исследованию подвержен профиль электронной почты-получателя электронного сообщения, а на разрешение поставлен вопрос о факте отправки, произведен поиск возможных подделок электронного письма методом анализа заголовочной информации.

Для этого произведено сохранение электронного письма на компьютер эксперта штатными средствами портала (см. илл. 3).

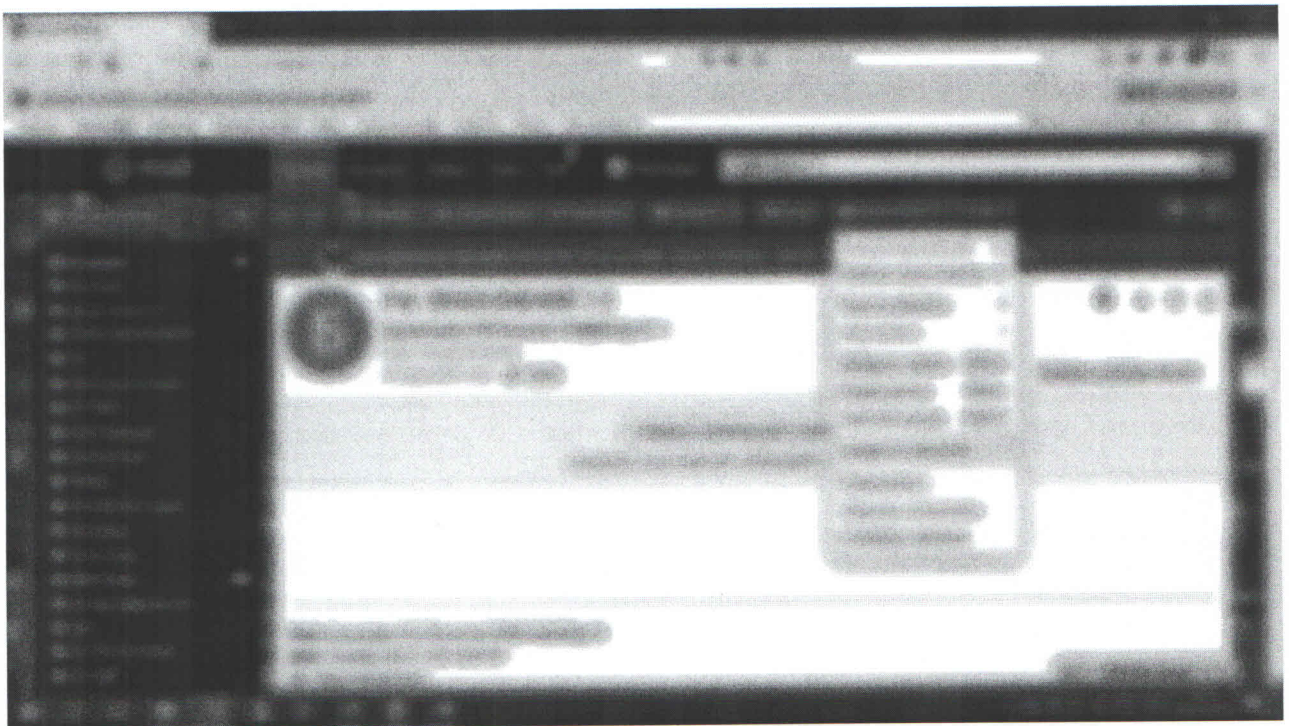


Иллюстрация 3. Механизм сохранения электронного сообщения с портала электронной почты mail.ru

Сохраненный файл поименован [REDACTED].eml и имеет контрольную сумму (по протоколу MD5) [REDACTED].

Непосредственно анализ осуществлялся при помощи редактора Notepad++. Заголовочная информация приведена в приложении 3 к заключению.

В ходе анализа было выявлено, что отправка электронного письма осуществлялась с почтовых серверов [REDACTED].ru, а не [REDACTED].ru. В связи с этим посредством сервиса whois запрошены сведения о почтовом сервере имени [REDACTED].ru. Сведения подтверждают, что доменным именем [REDACTED].ru используются сервисы [REDACTED].ru для отправки и получения электронных сообщений.

Данный факт, а также полное соответствие структуры и содержания заголовочной информации искомого электронного письма подтверждают его оригинальность и факт отправки именно с адреса [REDACTED].ru и именно в запрошенный период времени.

===== В Ы В О Д Ы =====

По результатам исследования необходимо сделать следующие выводы:

Факт отправки электронного письма с адреса [REDACTED].ru на адрес [REDACTED].ru [REDACTED] года [REDACTED] часов дня темой «[REDACTED]» имеет место. Вложенный в электронное сообщение файл распечатан и приложен к исследованию.

Приложение 1 к экспертному исследованию № [REDACTED] от « [REDACTED] » [REDACTED] 2019 г.

Текст искомого письма (пустые строки удалены)

From: Бухгалтерия*****

Приложение 2 к экспертному исследованию № [REDACTED] от « [REDACTED] » [REDACTED] 2019 г.

Содержание вложения в искомое письмо.



Приложение 3 к экспертному исследованию № [REDACTED] от « [REDACTED] » [REDACTED] 2019 г.

Содержание заголовка искомого письма.

Delivered-To:*****