АПАРИНА Кристина Геннадьевна
Московский государственный технический университет гражданской авиации, факультет авиационных систем и комплексов, аспирантка
kggorshkova@yandex.ru

КОРОЛЕВ Сергей Евгеньевич
Московский государственный технический университет гражданской авиации, факультет прикладной математики и вычислительной техники, студент
karalski@mail.ru

ТЕХНИЧЕСКИЕ и ПРОГРАММНЫЕ РЕШЕНИЯ для ЗАЩИТЫ ИНФОРМАЦИИ

Проблема плагиата очень актуальна в наше время. Она затрагивает как авторов, так и редакторов научных журналов. Одним из способов решения проблемы, считают авторы статьи, могут стать соответствующие меры по защите информации, которая передается в редакции журналов.

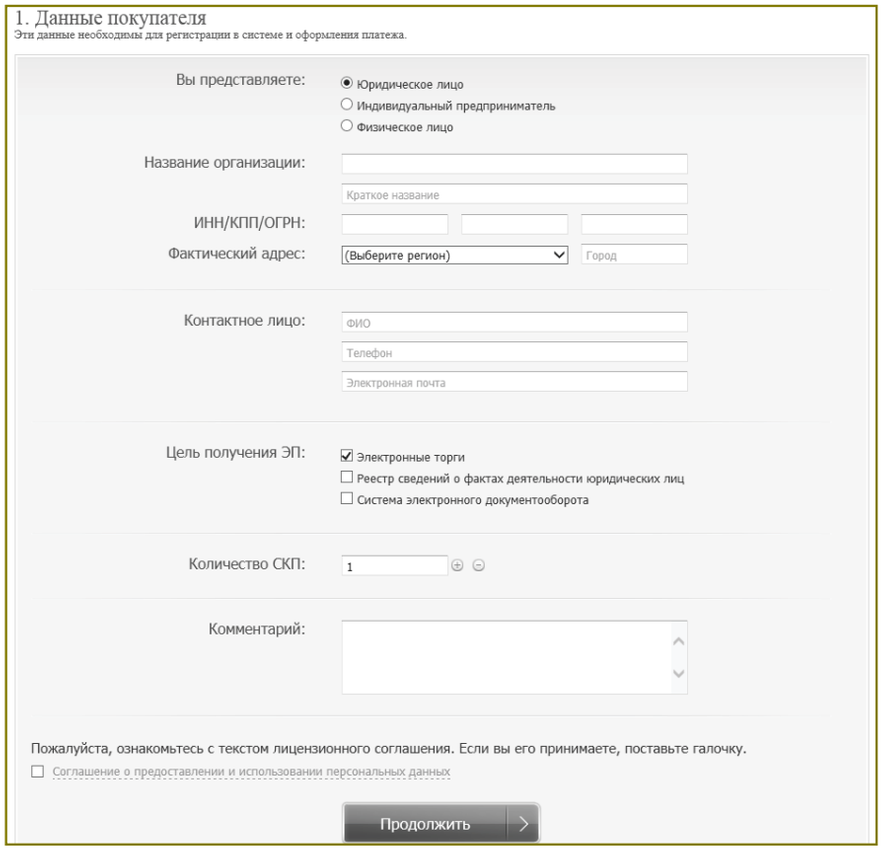
Плагиат может быть нарушением авторско-правового законодательства и патентного законодательства и может повлечь за собой юридическую ответственность. Иными словами, плагиат затрагивает конфиденциальность частной переписки. В соответствии со 149 ФЗ [1] «Об информации, информационных технологиях и о защите информации», статья 9, пп. 2 и 5: «Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации».

МЕТОДЫ ЗАЩИТЫ РУКОПИСИ ОТ ПЛАГИАТА

1. Использование электронно-цифровой подписи

Как можно защитить статью, если вместо компьютера автор писал на реальной бумаге реальными чернилами? Печать, роспись, дата? Пожалуй, только так. Оказывается, в электронном мире, мире ноликов и единичек, тоже можно поставить подпись, только электронную. В рамках данной статьи не будем углубляться в структуру криптографии и принципы шифрования, рассмотрим технологию электронной цифровой подписи максимально понятно и просто.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный



Ключевые слова:
плагиат,
электронно-цифровая подпись,
облачные сервисы,
шифрование писем

Keywords:
plagiarism,
digital signature,
cloud services
encrypting messages

Рис. 1. Регистрационная карта для получения ЭЦП
Источник: http://www.iecp.ru/eds/make-eds/

в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе [8]. Что это значит? Итак, чтобы воспользоваться благами технологий, стороны, между которыми передаются электронные документы (в нашем случае это автор и редактор), должны договориться об использовании средств ЭЦП. В России есть специальный интернет-портал www.iecp.ru [7], посвященный электронной цифровой подписи, где необходимо получить персональную цифровую подпись, заполнив регистрационную карту (*рис. 1*) и выполнив необходимые пункты, указанные на портале.

ЭЦП представляет из себя пару ключей – «открытый» (обычный текст) и «закрытый» (текст, зашифрованный при помощи какого-либо ключа) [2]. Ключи выглядят как файлы с расширением ".req"; они могут храниться на дискете, диске, флешке, в реестре Windows или специальных носителях ЭЦП «eToken» и «ruToken». Примеры ЭЦП с ключом представлены на *рис. 2*.

«Закрытый» ключ необходимо держать в строжайшем секрете, а «открытыми» следует обменяться с получателем, т.к. в процессе отправки документы с помощью специальной программы шифруются двумя ключами – своим закрытым и чужим открытым [3, 4]. После отправки и принятия получатель расшифровывает документы с помощью его закрытого ключа и открытого ключа отправителя. В случае если электронный документ, подписанный цифровой подписью, попадет в чужие руки, то без пары ключей документ прочитать будет невозможно. Одной из функций открытого ключа является идентифика-

Рис. 2. Примеры ЭЦП в виде физических носителей
Источник: http://ru.wikipedia.org/wiki/

Рис. 3. Структура сертификата
Источник: http://www.inssl.com/x509-open-key-specifications.html

ция пользователя ЭЦП (например, редактор может определить, кто ему прислал документ, а автор – кому он его отправляет). Здесь появляется маленький нюанс. Злоумышленник Вася может выдать свой открытый ключ за ключ редактора и прислать его автору. В итоге весь материал получит и расшифрует Василий. Для того чтобы этого не произошло, созданы сертификаты открытого ключа (структура сертификата представлена на *рис. 3*, а пример сертификата представлен на *рис. 4*) [9].

```
Имя пользователя: C = RU, org = ACME, cn = UserName
Имя издателя: C = RU, org = ACME
Номер сертификата:  #12345678
Открытый ключ пользователя:
   Алгоритм: GOST open key
   Значение ключа: 010011101001001010000001
Сертификат действует с:  01.01.2006 00:00:00
Сертификат действует до: 31.12.2008 23:59:59
Дополнительная информация (X.509 v3 Extensions)
   Регламент использования сертификата: Только для платежей
   Секретный ключ действует с:  31.12.2006 23:59:59
   Секретный ключ действует до: 31.12.2007 23:59:59
   Область применения ключа: Идентификатор 1
   Область применения ключа: Идентификатор i
   Область применения ключа: Идентификатор N
   Права и полномочия: Администратор
   Атрибуты пользователя: IP, DNS, URI, RFC822, Номер счета,
Адрес
   ...
Подпись Удостоверяющего Центра:
   Алгоритм: GOST P 34.10-94 sign algorithm
   Значение: 010011101001001010000001
```

Рис. 4. Пример сертификата открытого ключа
Источник: http://www.inssl.com/x509-open-key-specifications.html

Идея сертификата – это наличие третьей стороны, которой доверяют две другие стороны информационного обмена. Третьими сторонами являются удостоверяющие центры, выдающие сертификаты на открытый ключ. Удостоверяющий центр – сторона (отдел, организация), чья честность неоспорима, а открытый ключ широко известен. Задача центра сертификации – подтверждать подлинность ключей шифрования с помощью сертификатов электронной подписи. Таких удостоверяющих центров немного. Если редактор сформирует сертификат со своим публичным ключом, и этот сертификат будет подписан одним из удостоверяющих центров, список которых также можно посмотреть по ссылке: http://www.iecp.ru/juristic/companies/cert-a/ca-list/, то любой, доверяющий этому центру, сможет удостовериться в подлинности открытого ключа редактора и быть уверенным в том, что только он прочтет отправленные документы.

Итак, главный плюс ЭЦП – доказательное подтверждение авторства документа. Так как создать корректную подпись можно, лишь зная закрытый ключ, который известен только владельцу, то он может доказать свое авторство

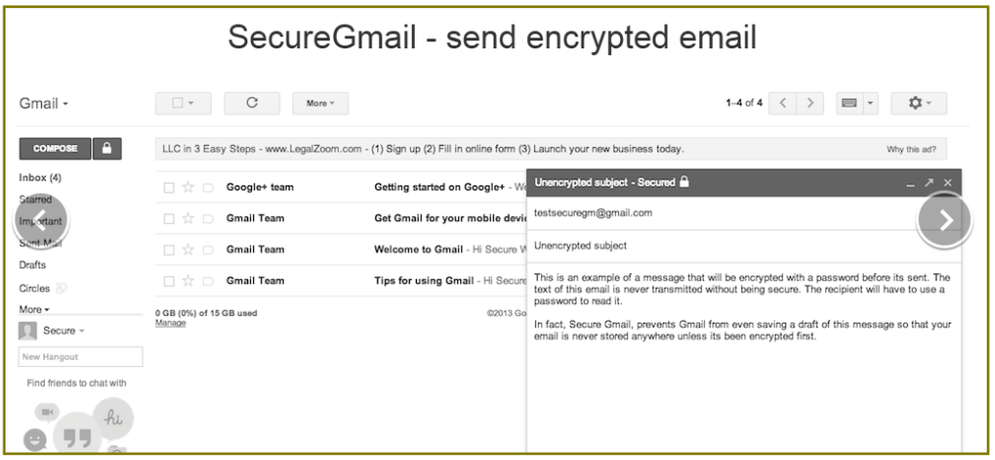


Рис. 5. Шаг 1. Шифрование письма Источник: https://www.streak.com/securegmail

подписи под документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесенные изменения», «метка времени» и т.д.

2. Шифрование электронных писем

Если нет желания связываться с получением электронной цифровой подписи, платить деньги за регистрацию, предоставлять свои данные удостоверяющему центру для изготовления сертификата ключа ЭЦП, то можно просто зашифровывать письма в электронной почте. Правда, в таком случае теряется возможность доказать свое авторство. Удобство шифрования могут оценить пользователи электронного почтового ящика от Google – Gmail, с установленным на компьютер браузером Google Chrome, так как для него есть решение от разработчиков – SecureGmail. Пользоваться данной функцией крайне легко – необходимо указать пароль для шифруемого письма и подсказку, которая позволит вспомнить пароль, если вдруг он будет забыт. После отправки зашифрованного письма останется лишь сообщить пароль получателю, чтобы тот беспрепятственно расшифровал и прочитал письмо. Минусом можно считать то, что на компьютере получателя также должен быть установлен браузер Google Chrome.

Пример шифрования сообщений с помощью данной функции [10]:

1. Выбираем сообщение, которое хотим зашифровать, и нажимаем на «замочек», расположенный в левом верхнем углу *(рис. 5)*.

Теперь письмо зашифровано, о чем свидетельствует надпись вверху «Unencrypted subject – Secured».

2. Чтобы расшифровать данное сообщение и прочесть его, нужно ввести в специальное поле пароль, который был присвоен этому сообщению при шифровании *(рис. 6)*.

При верном вводе пароля сообщение будет расшифровано *(рис. 7)*.

Аналогичная функция существует и у браузера Firefox – Encrypted Communication, но и в этом случае отправитель и получатель шифрованного письма должны пользоваться только этим браузером.

Вариант шифрования писем электронной почты в браузерах можно заменить компьютерной программой для шифрования – PGP (Pretty Good Privacy) *(рис. 8)* [11]. Программа подходит для настольных почтовых клиентов Thunderbird и Postbox, а также большинства веб-приложений (Gmail, Outlook, Google Apps, Yahoo и т.д.). Программа, по аналогии с ЭЦП, использует два ключа – публичный (открытый) и приватный (закрытый), с помощью которых письма шифруются и дешифруются. Получатель должен знать публичный ключ. Для этого отправитель может опубликовать его, например, на своем сайте, или

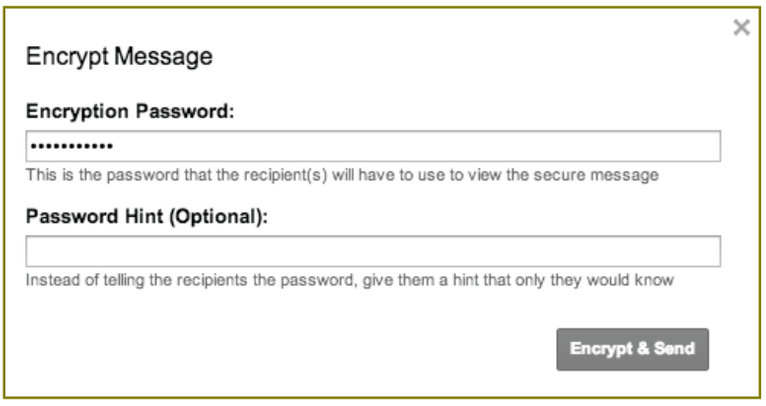


Рис. 6. Ввод пароля и расшифровка сообщения Источник: https://www.streak.com/securegmail

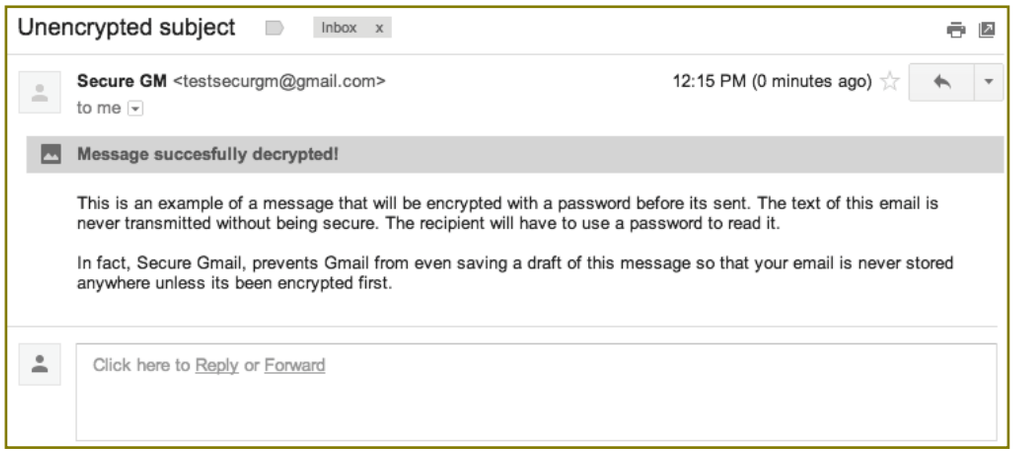


Рис. 7. Пример расшифрованного сообщения
Источник: https://www.streak.com/securegmail

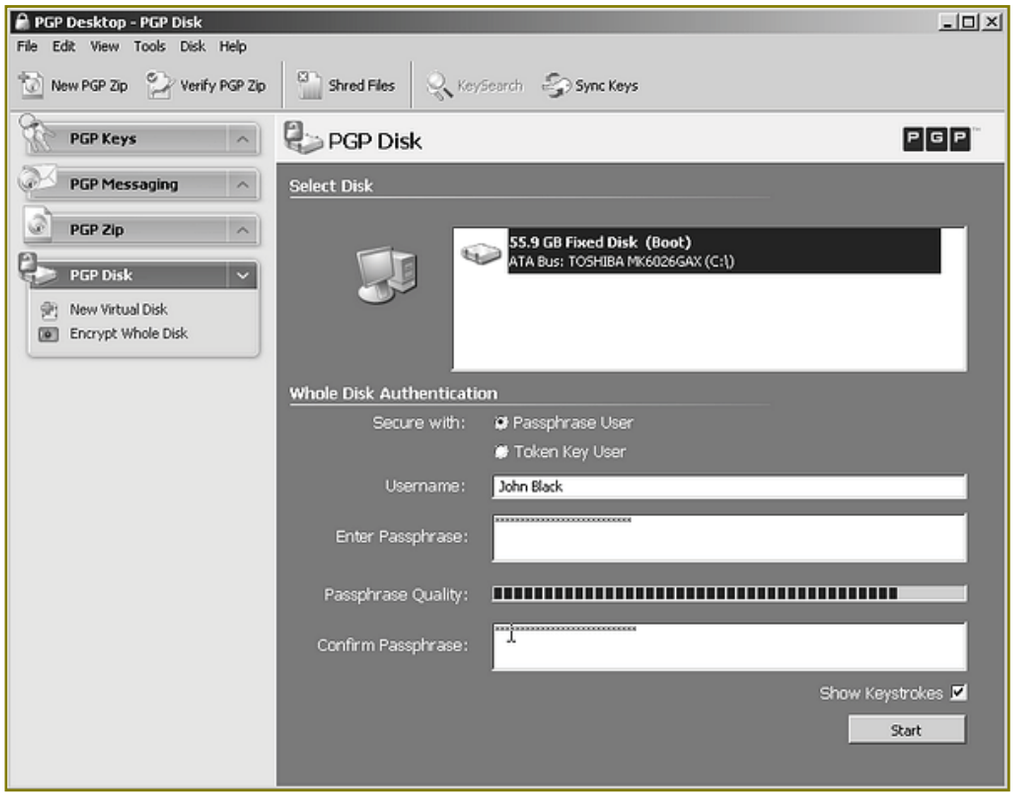


Рис. 8. Программа шифрования файлов PGP
Источник: http://softoroom.net/ptopic5570.html

разослать обычным письмом всем потенциальным получателям.

На рисунке 8 видна начальная страница данной программы, где можно зашифровать файлы, находящиеся на компьютере. Они шифруются при помощи введенного пароля (пароль придумывает пользователь). Также можно выбрать “GP Messaging”, и тогда сообщение, которое нужно отправить по электронной почте, будет зашифровано.

С помощью функции “PGP Zip” можно создать зашифрованный архив.

Использование такой программы для шифрования писем занимает больше времени, однако преимущества перевешивают недостатки: одной парой ключей (паролей) можно пользоваться при шифровании файлов как на своем компьютере, так и при отправке писем; PGP-шифрование зарекомендовало себя с положительной стороны; программа абсолютно бесплатна.

3. Хранение и передача информации в «облаках»

Этот метод будет полезен владельцам издательств, т.к. он представляет собой глобальную реорганизацию IT-инфраструктуры компании – организацию «облачных» серверов.

Рис. 9. Модели развертывания «облачного» сервиса
Источник: http://verapetrovna.ucoz.net/publ/oblachnye_servisy_v_obrazovanii/1-1-0-9

«Облачные» технологии (вычисления) – это модель обеспечения повсеместного и удобного сетевого доступа по требованию к общим вычислительным ресурсам (сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены с минимальными эксплуатационными затратами [5, 6]. Облачные технологии в настоящее время стали очень популярны при создании систем обработки данных, программного обеспечения, используемого в различных отраслях жизнедеятельности человека. Это происходит из-за того, что помимо экономии ресурсов главным достоинством перевода информации Компании в «облака» является доступность корпоративных данных для сотрудников из любой точки мира. Это получается потому, что информация хранится не на обычном сервере, который зачастую находится в Компании и доступ к нему имеют сотрудники, находясь на своем рабочем месте, или сотрудники, получившие удаленный доступ, а на «облачном» сервере. Доступ к нему обеспечить проще, чем к обычному серверу, и данные на нем так же защищены.

Существует 3 модели развертывания «облачного» сервиса *(рис. 9)*:

- приватный;
- общественный;
- гибридный.

Опишем более подробно каждую модель:

- Приватное «облако» представляет собой набор аппаратных средств, сетей, хранения, обслуживания, а также интерфейсы, которыми владеет и управляет организация и которые используют сотрудники, партнеры и клиенты этой организации. Чаще такую модель выбирают большие корпорации, готовые платить большие деньги за их создание исключительно для своих нужд и потребностей.
- Общественное «облако» представляет собой набор аппаратных средств, сетей, хранения, обслуживания, а также интерфейсы, которые принадлежат третьей стороне и управляются ею. Это значит, что услуги «облачных» технологий предоставляются провайдером за установленные тарифы.

В гибридном «облаке» объединяются данные из приватного и общественного «облаков» для создания единой, автоматизированной и хорошо управляемой вычислительной среды.

Гибридные «облака» получили наибольшую распространенность по нескольким причинам:

- собственная IT-инфраструктура становится в несколько раз компактней и проще в эксплуатации;
- сервисы гибридного «облака» уже готовы к использованию, их фактические характеристики доступны для изучения еще до приобретения;
- вынос части сервисов в публичное «облако» (вместе с процессами их внедрения и эксплуатации) позволяет IT-службе сконцентрироваться на корневых бизнес-приложениях.

Использование «облачных» серверов помогает сэкономить время и средства на безопасном хранении и использовании корпоративной информации.

ВЫВОД

Выше были описаны три основных метода для защиты передаваемых третьим лицам файлов от кражи и/или плагиата. Какой из способов использовать, каждый решает для себя сам, поскольку необходимо учитывать

стоимость каждого из решений, а также способ установки и простоту использования на практике.

Главное запомнить, что любая информация, переданная третьим лицам, должна быть защищена от кражи, т.к. информация – это интеллектуальная собственность. А собственность нужно защищать.

Источники

1. ФЗ № 149 «Об информации, информационных технологиях и о защите информации» от 27.07.2006.

2. Иллария Бачило, С. Семилетов, И. Тиновицкая. Электронный документ и документооборот: правовые аспекты. – М.: ИНИОН РАН, 2003.

3. Сухарев Е. Информационная безопасность. Методы шифрования. – М.: Радиотехника, 2011.

4. Панасенко С. Алгоритмы шифрования. Специальный справочник. – СПб: БХВ-Петербург, 2009.

5. Кокорева О. Облачные вычисления. – СПб: БХВ-Петербург, 2011.

6. Antonopoulos, Nick, Gillam, Lee. Cloud Computing: Principles, Systems and Applications. – Springer, 2010.

7. Электронная цифровая подпись: официальный сайт [Электронный ресурс]. – URL: http://www.iecp.ru.

8. Википедия: официальный сайт [Электронный ресурс]. – URL: http://ru.wikipedia.org.

9. Безопасность в сети: официальный сайт [Электронный ресурс]. – URL: http://www.inssl.com.

10. Streak: официальный сайт [Электронный ресурс]. – URL: https://www.streak.com.

11. http://softoroom.net/

Kristina G. APARINA
Moscow State Technical University of Civil Aviation,
Department of aircraft systems and complexes, Postgraduate Student

Sergey E. KOROLEV
Moscow State Technical University of Civil Aviation,
Department of Applied Mathematics and Computer Science

Technical and Software Solutions to Protect Information

The problem of plagiarism is very relevant in our time. It affects both the authors and editors of journals. The authors think that the one way to solve this problem can be be the appropriate measures to protect the information that is transmitted in the journals.