УДК 004

Загидуллина А.У.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

ШИФРОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ ДЛЯ ЛИЧНОГО ПОЛЬЗОВАНИЯ

Аннотация. В эпоху цифровых технологий и повсеместного распространения интернета, защита личной информации становится одной из важнейших задач. Личная информация – это ценный ресурс, за обеспечение безопасности которого должен отвечать сам человек.

В данной статье рассматриваются методы шифрования электронной почты для личного пользования, их преимущества и недостатки, а также рекомендации по выбору подходящих инструментов. Особое внимание уделяется практическим аспектам внедрения шифрования в повседневное использование электронной почты.

Ключевые слова: шифрование, электронная почта, информационная безопасность, информация.

Под личной информацией может пониматься все что угодно, например, личная переписка, заметки, статьи (результаты интеллектуальной деятельности человека) и т. д. Соответственно, хранится личная информация может также в различных формах и источниках, будь то записная книжка, цифровые файлы в компьютере и даже электронная почта.

По данным исследований, более 90 % электронных писем содержат спам или фишинг-атаки, что подчеркивает необходимость защиты личной информации.

Защитить свою электронную почту можно различными методами и способами, начиная от организационных – установка сложного пароля и его изменение каждые 3 месяца, заканчивая техническими, куда можно отнести использование защищенного почтового агента, двухфакторную аутентификацию, услуги провайдера по защите электронной почты, а также шифрование.

Шифрование электронной почты позволяет защитить содержимое сообщений от несанкционированного доступа, обеспечивая конфиденциальность и целостность данных. Шифрование электронной почты может быть выполнено различными методами:

Первым методом будет являться полное шифрование любого исходящего письма, для этого пользователь должен использовать программу шифратор и ключ, для шифрования писем. Пользователь пишет необходимый текст в программу шифратор и при обработке текста получает не связанные символы, которые может отправить. Получатель письма копирует эти несвязанные символы, вставляет их в программу шифратор, указывает ключ и получает расширенное послание. Данный способ является очень редким, носит большое количество недостатков, а также является неудобным ни пользователю, ни получателю писем.

Вторым методом будет являться шифрование внутри клиента электронной почты, для этого пользователь и получатели электронных писем должны использовать единый клиент и единый ключ. Пользователь использует свою электронную почту, как и обычно, но через защищенной клиент, в таком случае, если злоумышленник входит в аккаунт электронной почты с обычного клиента он увидит лишь зашифрованные переписки. При этом получатели будут видеть реальный текст письма, только в том случае, если используют защищенный клиент и ввели необходимый ключ или установили необходимый сертификат

Третий метод – шифрование файла, содержащего письмо и отправка по обычному клиенту или веб-версии электронной почты. Пользователь пишет необходимый текст в файле (в word-файле), после чего шифрует этот файл и направляет получателю. Получатель скачивает данный файл и дешифрует его через указанное программное обеспечение или веб-ресурсы (при наличии ключа).

Далее следует рассмотреть сами методы шифрования, а именно симметричное и ассиметричное.

Асимметричное шифрование более безопасно, так как не требует передачи закрытого ключа, однако оно требует больше вычислительных ресурсов и может быть медленнее, чем симметричное шифрование [1].

Следует учитывать, что если шифрование настраивается на специальном клиенте или шифруется сам файл, то для выполнения автоматического шифрования используются особые протоколы.

Наиболее распространенные из них:

- PGP (Pretty Good Privacy [2];
- S/MIME (Secure/Multipurpose Internet Mail Extensions.

Определившись с методами и способами шифрования электронной почты, стоит рассмотреть целесообразность данной процедуры, для этого рассмотрим преимущества шифрования электронной почты.

Главное преимущество обеспечение конфиденциальности. Шифрование защищает содержимое сообщений от посторонних глаз, что особенно

важно для личной переписки. Это позволяет избежать утечек информации, которая может быть использована для мошенничества или шантажа.

Важным преимуществом является сохранение целостности данных. Шифрование гарантирует, что сообщение не было изменено в процессе передачи. Это особенно важно для юридически значимых документов или финансовых транзакций.

Третьим преимуществом является подтверждение, что пользователь, направивший письмо, является тем самым пользователем, т. е. аутентификация. Использование цифровых подписей позволяет подтвердить личность отправителя. Это помогает предотвратить атаки «человека посередине», когда злоумышленник пытается выдать себя за другого человека.

Разумеется, шифрование электронной почты используется и для защиты от утечек. В случае утечки данных, зашифрованные сообщения остаются недоступными для злоумышленников, что снижает риск компрометации личной информации.

Были выявлены недостатки при использовании шифрования электронной почты. Например, сложность использования. Необходимо понимать, что для многих пользователей настройка шифрования может показаться сложной задачей, что может привести к отказу от его использования. Необходимость в установке дополнительных программ и настройке ключей может отпугнуть менее технически подкованных пользователей.

Следующий недостаток – проблемы совместимости. Так как, современные технологии очень сильно развиты в данном вопросе, то не все почтовые клиенты поддерживают одни и те же протоколы шифрования, что может создать трудности при обмене зашифрованными сообщениями. Например, пользователь PGP не сможет отправить зашифрованное сообщение пользователю S/MIME без конвертации.

Пользователю всегда нужно помнить про «управление ключами». Необходимость в безопасном хранении и управлении ключами может стать дополнительной нагрузкой для пользователей. Потеря закрытого ключа может привести к невозможности доступа к зашифрованным сообщениям.

Отдельно стоит выделить проблему зависимости от инфраструктуры. Использование некоторых методов шифрования, таких как S/MIME, требует от пользователя наличие доступа к центрам сертификации, что может быть проблематично в некоторых регионах.

Разобравшись с перечнем достоинств и недостатков перейдем к рекомендации по выбору инструментов.

Выбор почтового клиента: Рекомендуется использовать почтовые клиенты, которые поддерживают шифрование, такие как Thunderbird с плагином Enigmail или Outlook с поддержкой S/MIME. Также стоит рассмотреть использование специализированных сервисов, таких как ProtonMail или Tutanota, которые предлагают встроенное шифрование.

После выбора инструмента пользователю необходимо поддерживать регулярное обновление программного обеспечения. Обновление почтовых клиентов и шифровальных программ поможет защититься от известных уязвимостей. Пользователи должны следить за обновлениями и устанавливать их своевременно.

Рекомендуется создавать резервные копии закрытых ключей и хранить их в безопасном месте. Это поможет избежать потери доступа к зашифрованным сообщениям.

Стоит обратить внимание, что для защиты электронной почты необходимо использование многофакторной аутентификации. Вне зависимости от того, защищенный вы используете клиент или нет. Для повышения безопасности рекомендуется использовать многофакторную аутентификацию при доступе к почтовым аккаунтам и шифровальным программам.

Подводя итог, шифрование электронной почты является важным инструментом для защиты личной информации в цифровом мире. Несмотря на некоторые недостатки, преимущества, которые оно предоставляет, делают его необходимым для обеспечения конфиденциальности и безопасности личной переписки. Пользователи должны быть осведомлены о доступных методах и инструментах шифрования, чтобы эффективно защищать свои данные. Внедрение шифрования в повседневное использование требует усилий, но эти усилия оправданы в условиях растущих угроз для информационной безопасности.

Список использованных источников:

1. Дунюшкина, К.С. Создание служебного канала для обмена информацией конфиденциального характера / К.С. Дунюшкина, А.Ф Фатхелисламов. Текст: непосредственный // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием. Уфа, 2023. Уфа: Уфимский университет науки и технологий, 2023. С. 83–86.

2. Сычев Ю.Н. Защита информации и информационная безопасность: учебное пособие/ Ю.Н. Сычев. М.: ИНФРА-М, 2021. 199 с. (дата обращения 29.03.2025). Текст: непосредственный.

Zagidullina A.U.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

ENCRYPTING EMAIL FOR PERSONAL USE

Abstract. In the digital age and the ubiquity of the Internet, protecting personal information is becoming one of the most important tasks. Personal information is a valuable resource, for ensuring the security of which the person himself must be responsible.

This article discusses email encryption methods for personal use, their advantages and disadvantages, as well as recommendations for choosing appropriate tools. Special attention is paid to the practical aspects of implementing encryption in the daily use of e-mail.

Keywords: encryption, email, information security, information.