ТЕХНИЧЕСКИЕ НАУКИ

Шестолаева Татьяна Геннадьевна
студентка
Орлова Анна Юрьевна
канд. экон. наук, доцент

ФГАОУ ВПО «Северо-Кавказский федеральный университет»
г. Ставрополь, Ставропольский край

ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ В INTERNET

Аннотация*: данная статья посвящена проблеме защиты электронной почты в сети Интернет. Авторы полагают, что данные электронной почты в настоящее время уязвимы для вирусов, спама, хакерских атак, а потому необходимо предпринять меры по дополнительной защите почты.*

Ключевые слова*: Internet, защита, электронная почта.*

В настоящее время данные электронной почты уязвимы. Часто возникающими проблемами, с которыми встречаются пользователи электронной почты, являются: вирусы, спамы, разнообразные атаки на конфиденциальность сообщений и т. д. Это обусловлено недостаточной защитой современных почтовых систем.

Данная тема актуальна, так как с этими проблемами приходится иметь дело, как пользователям, так и разработчикам. Решить проблему защиты электронной почты невозможно. Причиной этому являются хакеры, спамеры, создатели и распространители вирусов, и поэтому защита электронной почты оказывается недостаточной. Для максимального уровня защиты электронной почты, необходим комплексный и систематичный подход к решению данной проблемы, учитывающий возможные угрозы.

Некоторые проблемы, которые связанны именно с конфиденциальностью почтовых сообщений, закладывались при появлении электронной почты. Многие из них не разрешены и сейчас. К ним можно отнести следующее:

– отсутствие надёжной защиты протоколов, что даёт возможность создавать письма с фальшивыми адресами;

– стандартные протоколы: SMTP, POP3, IMAP4, не включают механизмов защиты, которые давали бы гарантию конфиденциальности переписки;

– отсутствие гарантий доставки письма;

– легкое изменение электронных писем.

При выборе необходимых средств защиты электронной почты, обеспечивающих конфиденциальность и целостность информации, системному администратору или пользователю необходимо знать самые распространенные средства и методы, которые использует злоумышленник для атак систем электронной почты. К ним можно отнести следующее:

1. Использование снифферов (программы, которые перехватывают все сетевые пакеты, которые передаются через определённый узел.) С их помощью можно узнать текст сообщения, имена пользователей и пароли.

2. IP-spoofing – возможен, когда злоумышленник, находится внутри организации или вне её и выдаёт себя за санкционированного пользователя. Его задачей является получение важных файлов.

3. Получение пароля на почту. Существует много методов, одним из них является использование IP-spoofing. Однако чаще всего пользуют обычный перебор паролей с помощью специальной программы.

4. Нарушение конфиденциальности – Man-in-the-Middle («человек в середине»). Его цель заключается в перехвате информации, получении доступа к частным сетевым ресурсам, искажении передаваемых данных. Также он используется для перехвата паролей и имён пользователей.

5. Методы атак на уровне приложений используют хорошо известные недоработки серверного программного обеспечения (sendmail, HTTP, FTP). То есть, можно получить доступ к компьютеру от имени пользователя, работающего с приложениями той же электронной почты.

Рекомендуемые меры и средства для защиты электронных сообщений:

1. Использование технологии двухфакторной аутентификации.

2. Создание коммутируемой инфраструктуры и администрирование сети.

3. Криптография, основанная на сильных криптоалгоритмах (симметричные – RC4, RC5, CAST, DES,AES, приемлемая длина ключа которых = 128 разрядов, ассиметричные – RSA, Diffie-Hellman и El-Gamal, приемлемая длина которых до 2048 разряда).

1. Использование SSL помогает защитить сообщения только при передаче и если не применяются другие средства крипто защиты, то письма при хранении в почтовых ящиках и на промежуточных серверах содержатся в открытом виде.

2. Если криптографический алгоритм, который применяется в системе, является прочным, а генератор случайных чисел, который используется для создания ключей, никуда не годится, любой опытный криптоаналитик сразу сосредоточит внимание именно на нем.

3. Если генератор улучшен, но ячейки компьютера не закрыты, после того, как в них уже был сгенерированный ключ, то такая безопасность никуда не годится.

4. Большая часть сбоев в обеспечении информационной безопасности случается не из-за ненайденных уязвимостей в криптографических алгоритмах и протоколах, а из-за ошибок в их осуществлении.

Следуя из выше сказанных средств и методов защиты потока данных и архитектуры построения сети, произведен обзор стандартов, существующих в настоящее время и дающих гарантию на надёжную передачу данных электронных сообщений по почте, при условии, что эксплуатируемое нами программное обеспечение поддерживает требования этих стандартов.

Таким образом, данная проблема не может быть решена в полном объеме. Для ее решения требуются более совершенные методы защиты информации, которые в настоящий момент не разработаны.