СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ С ПОМОЩЬЮ МАТРИЦЫ УГРОЗ

Жидкова Любовь Сергеевна

магистрант, Институт экономики и управления Самарский национальный исследовательский университет имени академика С.П. Королёва, РФ, г. Самара

Клёвина Мария Васильевна

магистрант, Институт экономики и управления Самарский национальный исследовательский университет имени академика С.П. Королёва, РФ, г. Самара

Красносельцева Ирина Евгеньевна

магистрант, Институт экономики и управления Самарский национальный исследовательский университет имени академика С.П. Королёва, РФ, г. Самара

Электронная почта — один из наиболее широко используемых видов сервиса, как в корпоративных сетях, так и в Интернет. Она является не просто способом доставки сообщений, а важнейшим средством коммуникации, распределения информации и управления различными процессами в бизнесе.

Электронная почта обладает многочисленными достоинствами, но именно из-за этих достоинств возникают основные риски, связанные с ее использованием. В конечном итоге любой из этих рисков может привести к серьезным последствиям для компании. Это и потеря эффективности работы, и снижение качества услуг информационных систем, и разглашение конфиденциальной информации. Недостаточное внимание к данной проблеме грозит значительными потерями в бизнесе, а в некоторых случаях даже привлечением к юридической ответственности в связи с нарушением законодательства [1].

Для удобства составим общую таблицу 1 преимуществ и недостатков каждого средства защиты электронной почты [3].

Таблица 1.

Сравнительная таблица средств защиты почты

№	Средство	Преимущества	Недостатки
1	PGP Desktop	Наличие сервера ключей. Простота настройки почтовых клиентов.	Расшифрованные письма ничем не з клиенте. Если программа не запущена, а защ сообщение получено, непонятно, ка расшифровать.
2	S/MIME	S/MIME поддерживает большинство почтовых клиентов, в том числе и мобильные. Сообщения на клиенте хранятся в зашифрованном виде.	Необходим сервер ключей для комф Сложность настройки. Необходимо каждый почтовый клие отдельно.

		Расшифровка осуществляется средствами почтового клиента, а не стороннего ПО.	
3	Hushmail	Простота использования.	Возможность расшифровки сообщен администрацией сервиса или по реш Шифрование производится на стороне клиента.
4	PGP Mail	Шифрование/расшифровка на стороне клиента.	Поддерживаются не все браузеры. Для большей безопасности нужно ис что может вызвать затруднения у не пользователей
5	SecureGmail	Простота использования.	Только для Chrome. Ключ известен, как отправителю, та сообщения.
6	Encrypted Communication	Простота использования.	Только для Firefox. Ключ известен, как отправителю, та сообщения.
7	Плагин Enigmail	Удобен в использовании.	Требует GnuPG. Поддерживает только Thunderbird P

При построении таблицы 2 за основу взята матрица угроз проекта «HushMail». Номер средства в этой таблице соответствует номеру средства в таблице 1. Значение «Да» означает, что вы защищены от угрозы. Значение «Да/Нет» означает, что есть какие-либо ограничения, о которых мы расскажем.

Таблица 2.

Сравнение средств защиты электронной почты в разрезе матрицы угроз

Угроза	**PGP Desktop**	**S/MIME**	**Hushmail**	**PGP Mail**	**Secure Gmail**
Злоумышленник прослушивает ваше Интернет-соединение	Да	Да	Да	Да	Да
Злоумышленник получает доступ к e-mail, хранящемся на сервере	Да	Да	Да	Да	Да
Злоумышленник компрометирует веб-сервер после того, как вы получили доступ к e-mail	Да	Да	Нет	Да	Да
Злоумышленник контролирует веб-сервер, пока вы смотрите e-mail	Да	Да	Нет	Да	Да
Злоумышленник получает доступ к вашему компьютеру после того, как вы просмотрели ваше e-mail	Нет	Да	Да	Да	Да
Злоумышленник получает доступ к компьютеру до того, как вы посмотрели e-mail, и может установить программы по типу keylogger	Нет	Да/ Нет	Нет	Нет	Нет
Злоумышленник получил доступ к вашему жёсткому диску	Да/Нет	Да	Да	Да	Да

Проанализируем результаты, полученные для средств защиты «PGP Desktop» и «Huhsmail» (колонки 1 и 3). Поскольку шифрование осуществляется на стороне клиента, то программа

«PGP Desktop» защищает переписку от прослушивания Интернет-соединения, в «HushMail» приходится полагаться только на SSL. Поскольку на сервере письма хранятся в зашифрованном виде, то если злоумышленник узнает ваш пароль от почтового ящика, ничего страшного не произойдет — максимум, что он сможет прочитать — это спам [2].

Оба средства защиты уязвимы при использовании keylogger. Если злоумышленник перехватит ваши пароли (в частности, от сертификатов), то вам уже ничто не поможет. Разве что переход на токены вместо ввода паролей.

Все остальные средства защиты используют шифрование на стороне клиента, поэтому им не страшен ни перехват, ни доступ к почтовому ящику — сообщения будут зашифрованы. Предоставляет угрозу для этих средств защиты — перехват ввода с клавиатуры. Злоумышленник может получить доступ не только к паролям, но и к обычному тексту, который вводится в теле сообщения перед тем, как оно будет зашифровано.

Таким образом, самый простой способ защиты электронной почты — это использование симметричного шифрования. Для его реализации можно использовать плагины браузера «SecureGmail» и «Encrypted Communication» или использовать программы, позволяющие создавать архивы, защищенные паролем (например, WinRAR, 7-Zip). Создавать архив для каждого нового сообщения — довольно рутинно. Плагины «SecureGmail» и «Encrypted Communication» делают симметричное шифрование более удобным.

Список литературы:

1. Портал Helpu group. Способы защиты электронной почты от взлома –[Электронный ресурс]. – URL: https://helpugroup.ru/sposoby-zashhity-elektronnoj-pochty-ot-vzloma/(дата обращения: 28.12.2019)

2. Сайт компании Open Vision. Защита электронной почты –[Электронный ресурс]. – URL: https://www.open-vision.ru/solutions/information-security/email-protection/(дата обращения: 04.01.2020)

3. Портал StudRef.com. Средства защиты электронных сообщений –[Электронный ресурс]. – URL: https://studref.com/347588/ ekonomika/sredstva_zaschity_elektronnyh_soobscheniy#373(дата обращения: 24.12.2019)