**УДК 004.056.53(004.773.3)**

# МЕТОДЫ ЗАЩИТЫ ОТ СРЕДСТВ СЛЕЖЕНИЯ ЗА ЭЛЕКТРОННОЙ ПОЧТОЙ

***А.В. ЛОБАНОВ***
***(Представлено: Е.С. ГАТИХО)***

*Рассматриваются основные способы и механизмы защиты от средств слежения за электронной почтой. Приводятся примеры технологий обеспечения конфиденциальностии сокрытия реальной информации о пользователе во время работы с электронной почтой.*

На данный момент остро встает вопрос о поиске средств, стратегий, принципов обеспечения Интернет безопасности и предотвращения несанкционированного получения какой-либо информации о конечном пользователе. Информационная безопасность является необходимым условием развития современного общества. Обеспечение информационнойбезопасности является одной из приоритетных задач многих государств. Сохранность конфиденциальности получаемой и передаваемой информации – это жизненно важный аспект в современном мире. Пользователю необходимо иметь средства защиты личных данных.

Существует несколько подходов по обеспечению защиты пользователя от почтовых сервисов слежения:

- отключение отображения изображений в электронном письме;
- ручное ограничение доступа для определенных адресов, используемых сервисами отслеживания [1].

Ни одни из этих вариантов не является универсальным. При отключении изображений большая часть писем потеряет презентабельный вид, а также пользователь может вообще не увидеть необходимуюи важную информацию.

Во втором случае для каждого конкретного сервиса слежения необходимо собственноручно искать актуальные адреса, которые постоянно обновляются. Также стоит отметить, что количество сервисов постоянно растет. Поэтому этот вариант защиты представляется неудобным для обычного пользователя электронной почты [2].

Основная задача системы для защиты от слежения за электронной почтой состоит в сокрытии, подмены реальной информации о пользователе, чтобы сделать работу отслеживающих систем бессмысленной или невозможной. Самым логичным решением на первый взгляд является подмена изображения, но существует проблема при данном подходе – изменение содержимого сообщения возможно только в сторонних почтовых клиентах.

Система, которая бы могла полностью защищать пользователей во время работы с электронной почтой, должна удовлетворять следующим критериям:

- работа со всеми современными браузерами, так как большая часть пользователей использует только их при работе с электронной почтой;
- мобильные приложения для всех популярных платформ. По статистике, после браузеров, самым популярным методом для работы с электронной почтой являются мобильные устройства;
- расширения для популярных клиентов для работы с электронной почтой.

Если программное обеспечение удовлетворяет всем перечисленным качествам, она может гарантированно защитить пользователя от средств слежения, независимо от используемых платформ.

В случае с работой системы с расширениями для браузера или другими клиентами существует механизм защиты, основанный на перехватах загрузки изображений, и подмены отслеживаемого контента [3]. В момент загрузки всех изображений и другого контента он должен быть просканирован на соответствие определенным маркерам, которые, в свою очередь, указывают на то, что данный контент является отслеживаемым [4]. В этот момент возможно два варианта развития событий:

- изменение содержимого контента, либо полный отказ от его загрузки;
- передача контента другим пользователям в реальном времени и полная загрузка его на клиенте.

Первый способ обеспечивает высокий уровень защиты, но потенциально искажает конечное электронное сообщение. Второй же способ позволяет конечному пользователю скрыться среди множества других пользователей, которые загрузят контент по той же ссылке.

Основные *преимущества* применения разработанной системы:

- возможность прочтение электронной почты без видимых изменений структуры документа;
- обеспечение конфиденциальности данных.

Примерная схема защиты от систем отслеживания электронной почты изображена на рисунке 1.

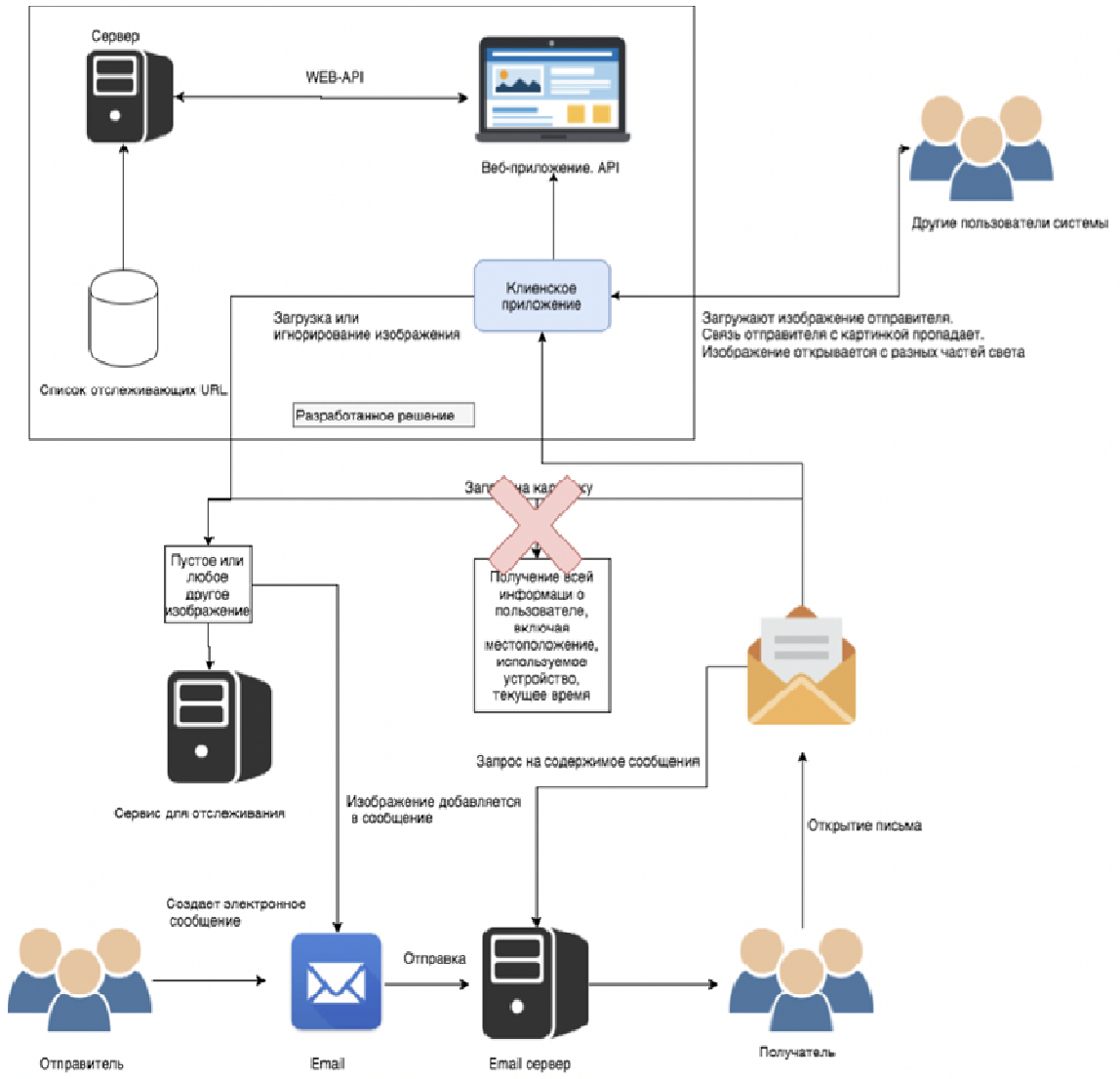


**Рисунок 1. – Схема защиты от слежения за электронной почтой**

ЛИТЕРАТУРА

1. Howstopemailtracking [Электронныйресурс]. – Режим доступа: http://www.wikihow.com/Stop-Email-Tracking. – Дата доступа: 20.09.2017.
2. Blockemailtracking [Электронныйресурс]. – Режим доступа: https://nordvpn.com/blog/how-to-block-email-tracking/. – Дата доступа: 24.09.2017.
3. Prevent loading images in browser [Электронныйресурс]. – Режим доступа: http://www. thewindowsclub. com/disable-images-chrome-firefox-ie. – Дата доступа: 18.09.2017.
4. Howtrackemailserviceswork [Электронныйресурс]. – Режим доступа: http://blog.rocketbolt.com/how-does-email-open-tracking-work/. – Дата доступа: 25.09.2017.