Безопасность систем электронной почты: проблемы и решения

Секция 3: Технологии обработки и защиты информации

Докладчик: Хамидов Шерзод Жалолдинович
(стажёр-соискатель)
ТУИТ имени Мухаммада ал-Хоразмий,
Ташкент,Узбекистан

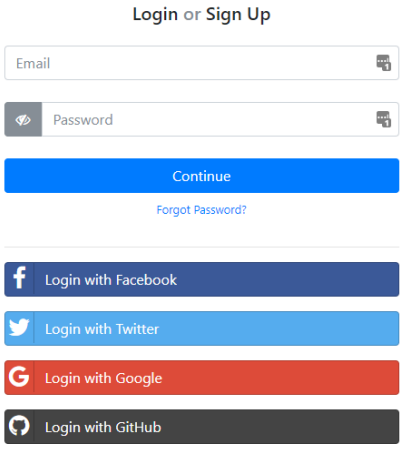

AOL.


zoho


GMX


YAHOO!

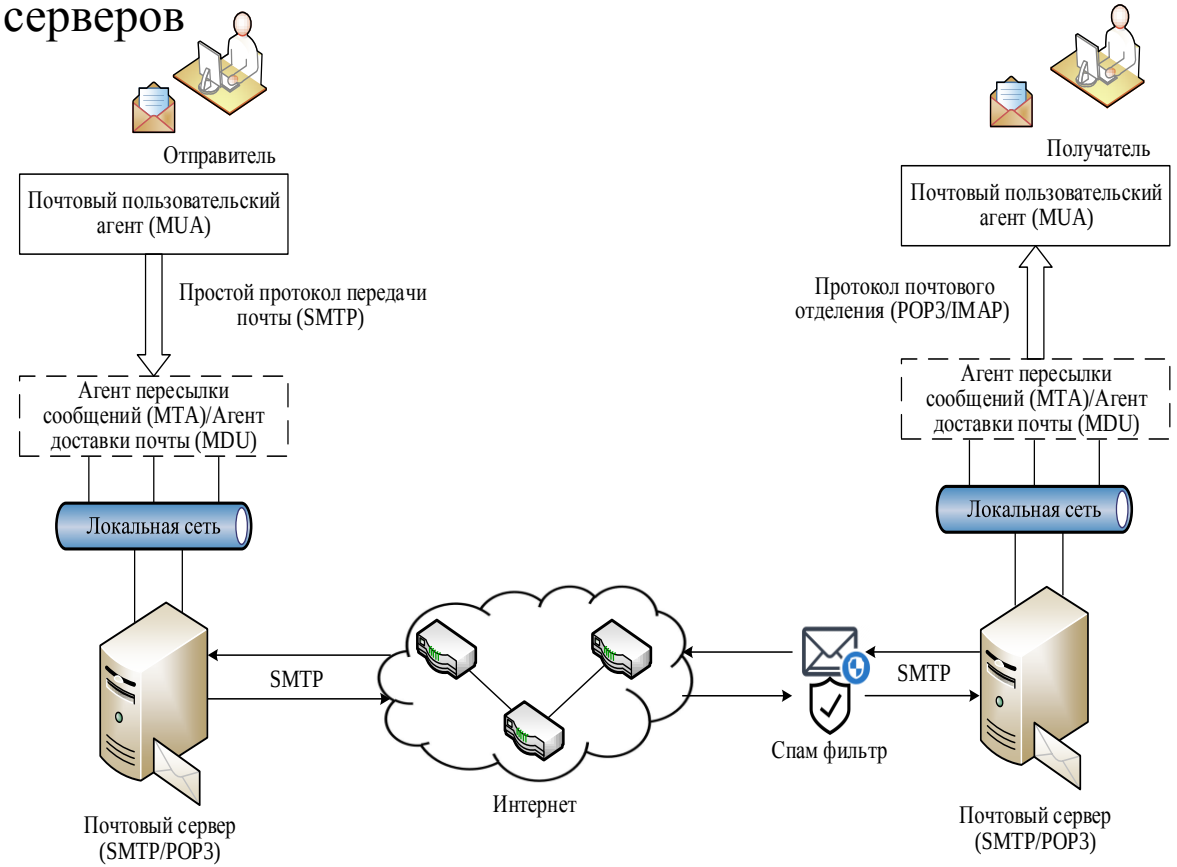

iCloud


Login or Sign Up
Email
Password
Continue
Forgot Password?
Login with Facebook
Login with Twitter
Login with Google
Login with GitHub

Система электронной почты

Система электронной почты состоит из двух основных компонентов, которые находятся в ИТ-инфраструктуре организации: почтовых клиентов и почтовых серверов.

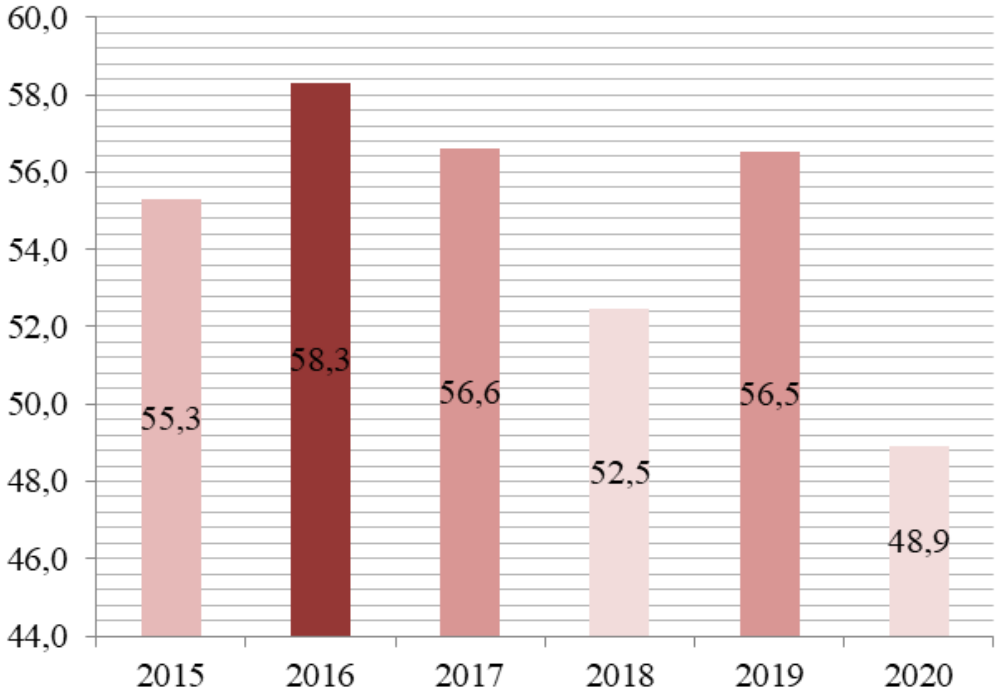
Стандарты (например, SMTP, ESMTP, POP, IMAP) для форматирования, обработки, передачи, доставки и отображения электронной почты гарантируют взаимодействие между множеством различных почтовых клиентов и серверов



Вредоносные электронные письма – содержащий программы или файл, который может повлиять на работу устройства или нанести ущерб данным без разрешения.

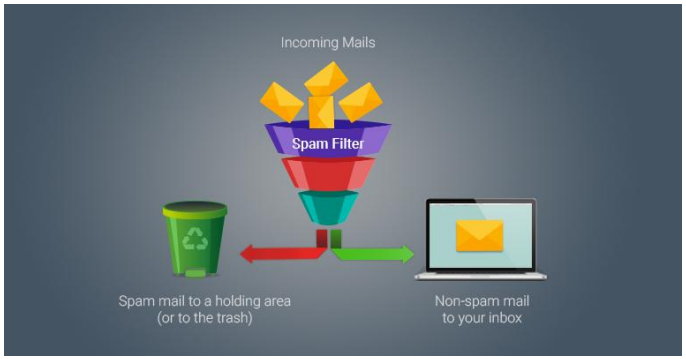
Фишинговые электронные письма – вид интернет-мошенничества, цель которого получить идентификационные данные пользователей.

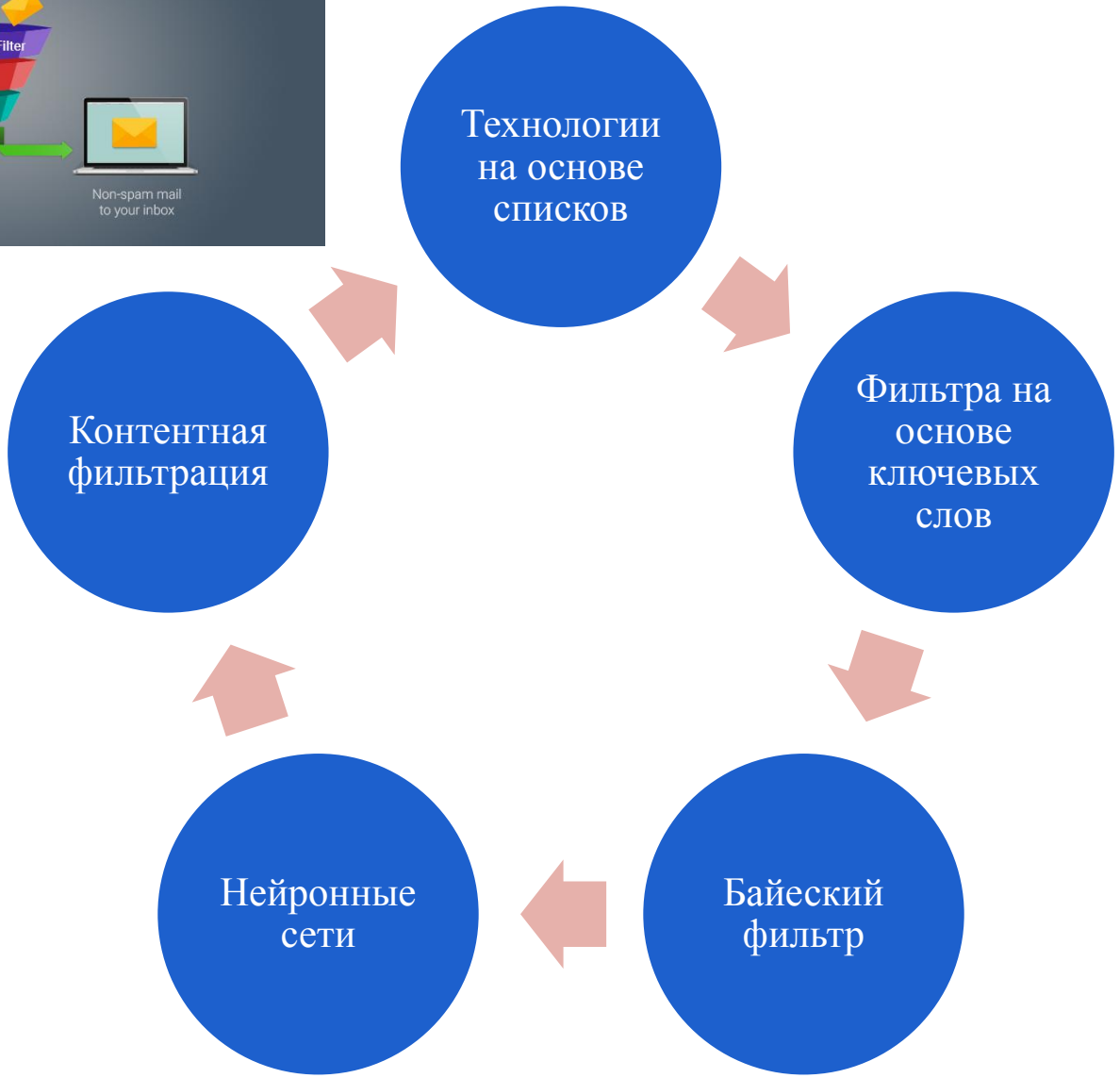
Спам письма - одна из основных проблем сегодняшнего дня, приносящая финансовый ущерб компаниям и раздражающая пользователей электронной почты.



Статистика доли спама в мировом трафике

Функции	S/MIME	DKIM
Стандарт	RFC 3851	RFC 4871
Защита от подслушивания	Да	Нет
Прозрачен для пользователя	Нет	Да
Сообщение доступно для ESP	Нет	Да
Конфиденциальность сообщений	Да	Нет
Тип аутентификации	Индивидуальный	Доменный
Тип сертификата	X.509	Нет спецификаций
Целостность сообщения	Да	Да
Доступ к веб-почте	Ограничено	Да
Неотказуемость	Да	Нет
Мобильность электронной почты	Ограничено	Да


Incoming Mails
Spam Filter
Spam mail to a holding area
(or to the trash)
Non-spam mail
to your inbox


Технологии на основе списков
Фильтра на основе ключевых слов
Байеский фильтр
Нейронные сети
Контентная фильтрация

Спам фильтр	Подходящее состояние	Недостаток
Черный список	если подозреваемые спам IP-адреса являются фиксированными или известными	обнаружение подозреваемых IP-адресов затруднено и содержит ошибки
Список в реальном времени	если IP-адреса, подозреваемые в спаме, являются фиксированными или известными, и третья сторона надежна.	обнаружение подозреваемых IP-адресов затруднено и содержит ошибки
Белый список	если подозреваемые спам IP-адреса исправлены	неизвестная подлинная почта может быть объявлена спамом
Серый список	если доверенный отправитель всегда отправляет сообщение два раза	если доверенный отправитель не отправит сообщение два раза, почта будет потеряна.
Фильтр на основе слов	подозреваемые ключевые слова известны	подлинная почта может содержать подозрительные ключевые слова
Байесовский фильтр	подозреваемые ключевые слова известны своей вероятностью спама	подлинная почта может содержать подозрительные ключевые слова
Нейронные сети	подозреваемые ключевые слова известны и доступна лучшая эвристическая функция	подлинная почта может содержать подозрительные ключевые слова

Заключение

В этой работе были рассмотрены угрозы почтовых служб, протоколы безопасности и методы фильтрации спамов. Систем и методов по обнаружению и распознаванию спам писем электронной почты главной целью является обеспечение целостность данных и конфиденциальность личных данных пользователей. Среди методов, применяемых для фильтрации данных, а в частности электронной почты и сообщений, имеется множество как производительных, но имеющих высокую вероятность ложного срабатывания, так и точных. Совместное использование нейронных сетей с классическими алгоритмами позволяет уменьшить количество спам писем, а также уменьшить вероятность их пропуска фильтром.

Спасибо за внимание !