УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЗАЩИТА ОТ СПАМА

Бартошевич А.В.
(научный руководитель – Стрелюхин А.В.)
Белорусский национальный технический университет
Минск, Беларусь

Аннотация. В работе рассмотрено одно из направлений информационной безопасности – защита от спама. Рассмотрены виды и способы распространения спама, его содержание, эффективность и методы борьбы с ним.

Введение

Основной задачей информационной безопасности является создание и реализация комплекса мер для защиты информации, а также сохранения ее конфиденциальности и целостности.

С точки зрения компьютерных технологий спам представляет собой не что иное, как нарушение защиты информации в почтовом протоколе.

Если рассматривать наиболее распространенное определение, то спам – это массовая рассылка рекламных писем пользователям, которые не давали своего согласия на их получение [1].

Основная часть

Слово «спам» (англ., «spam») имеет следующее происхождение. Изначально, SPAM – это торговая марка американской компании, под именем которой в 1936 году начали выпускать мясные консервы. Во время Второй мировой войны их изготовили настолько много, что пришлось срочно проводить рекламную кампанию, целью которой был сбыт товара раньше окончания срока годности. Реклама консервов проводилась везде, включая газеты, телевидение и радио.

Современное значение слово «spam» приобрело в 1986 году, когда началась настойчивая реклама финансовой пирамиды с многообещающим названием «заработай кучу денег».

Виды спама и способы его распространения

Выделяют следующие виды спама [2, 3]:

1. Массовая рассылка писем – один из самых известных видов спама, суть которого заключается в рассылке писем с коммерческими и рекламными предложениями, используя базы почтовых адресов.
2. Сообщения в социальных сетях и мессенджерах. Ранее такие рекламные сообщения имели то же содержание, что и письма. Однако сейчас нарастает популярность схемы, в ходе которой взламывается аккаунт пользователя, от имени которого идет рассылка.
3. Спам на форумах. Спамеры оставляют сообщения в обсуждениях либо отправляют личные сообщения пользователям, что используется для увеличения ссылочной массы какого-либо сайта.
4. Спам в комментариях на сайте, цель которого заключается в рекламе товаров или услуг.
5. Спам по SMS. Спамеры покупают базы данных пользователей сотовых операторов и высылают рекламные сообщения, часто мошеннического характера.

По характеру содержания спам-сообщения бывают следующие:

1. Реклама легальных товаров или услуг. Это обычные письма рекламного характера, но с особенностью, что пользователи не давали своего разрешения на их получение.
2. Реклама запрещенных законодательством товаров или услуг.
3. «Письма счастья». Такие письма содержат просьбу переслать текст сообщения другим пользователям, чтобы «что-то хорошее случилось» или «что-то плохое не случилось». В большинстве случаев такие письма используются спамерами с целью получения баз адресов для последующих рассылок.

4. Фишинг. Мошенники присылают сообщение, похожее на стандартное письмо от партнеров, банка и т.д., в содержании которого есть ссылка на поддельный сайт, визуально не отличающийся от оригинального. На поддельном сайте настаивают на введении персональных данных, в том числе данных карточек. Если пользователь выполнит эти действия, то его персональные данные станут известны злоумышленникам. В случае с банковскими данными это может обернуться серьезными финансовыми проблемами.

5. «Нигерийские письма» – получили свое название из-за первоначального распространения в Нигерии. Суть таких писем заключается в обещании отправить адресату крупную сумму денег, но перед этим пользователь обязан произвести небольшой взнос. После получения денег мошенниками связь с ними прекращается.

6. Вредоносные программы. В теле письма или в ссылке, находящейся в письме, может содержаться вредоносный программный код (вирус, сетевой червь или троян). Такой вредоносный код заражает компьютер, что позволяет злоумышленникам украсть личные данные, пароли, получить удаленный доступ к компьютеру и т.д.

Методы борьбы со спамом

В информационной безопасности выделяют следующие факторы, повышающие результативность защиты информации – технический и человеческий.

Технический фактор, в своем большинстве, связан с ошибками или недоработками в программном обеспечении, что позволяет их использовать злоумышленниками.

Взлом сайтов, почты дает возможность доступа не только к персональной информации пользователя и его переписке, но и базе данных контактов самого пользователя.

Такие ошибки обычно устраняются с помощью пакетов обновлений и/или дополнений («заплаток», patch), выпускаемых производителем программного обеспечения для оперативного исправления или нейтрализации возникшей проблемы.

Человеческий фактор чаще всего связан с низкой квалификацией пользователя или его невнимательностью [3].

1. Невнимательность при регистрации на сайте. Достаточно часто в форме регистрации автоматически выставляется «галочка» – согласие на получение рекламной информации. Отказаться от рассылки спама в этом случае достаточно просто: в конце каждого письма обычно находится ссылка «Отписаться от рассылки».

2. Пользователь вводит данные на «подставных» сайтах: фамилию, номер карточки, пароль и т.д., тем самым предоставляя злоумышленникам полную информацию о себе.

Основные советы по защите от спама следующие [3].

– создайте несколько электронных адресов, один из которых используется для личной и деловой переписки, а второй – для регистрации на коммерческих сайтах;

– используйте безопасный почтовый сервис (например, Gmail). В таких сервисах действует фильтрация спама, благодаря которой бóльшая часть нежелательных писем будет сразу попадать в папку «Спам». В случае поступления сомнительного письма в основную папку с письмами, необходимо его отметить как «спам», тогда все дальнейшие письма от этого адресанта будут автоматически отправляться в специальную папку;

– используйте почтовые сервисы, которые позволяют самому создавать фильтры и правила фильтрации писем (почта Яндекс).

Эффективность спама

Тестирование и анализ результатов «спамовой» рассылки неизменно показывает его исключительно низкую эффективность, а часто и почти полную безрезультативность. Например, во время рекламной кампании в Калифорнии с 75 869 компьютеров за 26 дней были разосланы 350 миллионов извещений о продаже нового лекарства на натуральной основе. В итоге фирма получила всего 28 заказов [4].

Заключение

В настоящее время, спам является одной из серьезных угроз информационной безопасности. Результатом таких рассылок является обилие нежелательных писем, которые заполняют почтовые ящики ненужной информацией и создают проблемы пользователям.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Интернет-ресурс: ru.wikipedia.org, дата обращения: 05.04.2023;
2. Интернет-ресурс: securelist.ru, дата обращения: 05.04.2023;
3. Интернет-ресурс: timeweb.com, дата обращения: 05.04.2023;
4. Эффективен ли спам?, Е. Л. Лозовская, Наука и жизнь, № 6, 2009 г.