

СЕМАНТИЧЕСКИЕ ОСОБЕННОСТИ МОШЕННИЧЕСКИХ ТЕКСТОВ

Семантика мошеннических текстов является ключевым элементом, позволяющим мошенникам убедительно представить свои предложения и тем самым обмануть потенциальных жертв. Текстовыми маркерами фейков являются особенности построения текста, употребление определенных языковых выражений и подача материала.

В 80 % проанализированного корпуса информации, мошенники используют понятные и привлекательные слова и фразы, которые внушают доверие и создают иллюзию легкости и выгоды: *Бесплатный iPhone X для первых 100 человек! Спешите забрать свой приз!; Получите кредит без справок и проверок за 15 минут; Получите доступ к эксклюзивному контенту, который изменит вашу жизнь навсегда.* Насторожить должны обещания быстрого и легкого получения финансовых выгод, бесплатного доступа к эксклюзивным предложениям или подаркам: *У нас самые низкие цены на рынке, не упустите свой шанс сэкономить; Этот курс обучения гарантирует вам работу с зарплатой от 5000 в месяц.*

Примером использования заманчивой лексики может служить схема «пирамиды», когда мошенники обещают участникам высокие доходы за счет привлечения новых участников в систему: *обеспечит вам стабильный доход; гарантирует вам финансовую независимость и успешную карьеру без усилий; гарантируем вам быструю окупаемость вложенных средств и высокий процент прибыли; поможет вам увеличить свой доход без каких-либо усилий или рисков со стороны клиента; предлагает вам легкий и быстрый способ стать богатым, не требующий больших вложений или времени.* Пример полного сообщения: *Хочешь зарабатывать? Никаких продаж! Зарабатывай с помощью своего жесткого диска от 125\$ до 600\$ в месяц! Включай компьютер и получай ежедневный пассивный доход. Все подробности по телефону [номер телефона] или в личку. Учись зарабатывать, а не работать!*

Еще одним примером – фишинг или мошенничество с помощью фальшивых онлайн-магазинов: на электронную почту поступает сообщение с просьбой изменить пароль или обновить регистрацию на сайте. Жертва переходит по ссылке, затем её просят ввести данные карты, чтобы списать один рубль «для подтверждения». Если это произошло, то появляется «зеркало», т.е. поддельная копия сайта, и таким способом мошенники получают полные данные жертвы.

Разработан индекс потенциальной «фейковости» сообщения, т.е. достоверности информации, учитывающий количественный показатель, которые выявлены как маркеры конкретного текста, свидетельствующие о возможности мошенничества. Он выражается в виде десятичной дроби: если отмечено 8 маркеров, а в процессе анализа подтвердилось 5 маркеров, то он составит $5/8=0,62$. Текст с таким значением вычисленного индекса явно будет требовать серьезной проверки на фейковый характер.