

УДК 366.636.2

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ВИДЕОСЕРВИСАХ И СОЦИАЛЬНЫХ СЕТЯХ

Мокеров В.С., студент гр.061402

Белорусский государственный университет информатики и радиоэлектроники¹

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук

Аннотация. Автором статьи описан личный опыт обнаружения социальной инженерии при использовании социальных сетей и видеоресурсов. В статье представлены примеры попыток манипулирования социальным поведением пользователей с помощью рекламы запрещенных товаров, предоставления недостоверной прополитической информации, блокировки государственных каналов средств массовой информации, описаны методы и приемы, которые используются журналистами и видеоблогерами с целью привлечения внимания пользователей и навязывания недостоверной информации, приведены меры по анализу достоверности информации и ограничения возникновения нежелательной рекламы при посещении видео ресурсов и социальных сетей.

Ключевые слова. Социальная инженерия, социальные сети, видео сервисы, недостоверная информация.

На фоне стремительного развития приложений, веб и видео ресурсов увеличилось число попыток воздействия на пользователей посредством социальной инженерии [1]. Социальная инженерия в контексте информационной безопасности – психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации [2].

Многие платформы видеосервисов и социальных сетей за последнее время неоднократно предоставляли рекламу запрещённых товаров, услуг, различных игровых сервисов и услуг мошенников. Одним из таких примеров является видеохостинг YouTube, при просмотре которого возникает прополитическая реклама, целью демонстрации которой является дестабилизации ситуации в некоторых странах и увеличения энтропии общества, что является нарушением статьи 130 Уголовного Кодекса Республики Беларусь и Закона Республики Беларусь № 15-3 «О внесении изменений и дополнений в некоторые законы Республики Беларусь по вопросам рекламы» [3]. Необходимо отметить, что такая реклама относится к детскому контенту [4] и распространяется на детских каналах, что может сформировать неправильное представление у подрастающего поколения. При этом на YouTube блокируются некоторые официальные государственные каналы средств массовой информации, по причине нарушения правил пользования платформой. В то же время другие политические каналы с иными взглядами не подвержены такой блокировке [5]. Возникает проблема восприятия и анализа информации пользователями данного видеохостинга в виду отсутствия альтернативных источников, результатом чего является принятие заведомо ложной информации в качестве достоверной. Во многих социальных сетях, например, в Facebook появляются ложные официальные аккаунты, публикующие недостоверную информацию и продвигаемые данной платформой в виде рекламы и рекомендаций, что способствует намеренному формированию отрицательных отношений к русскоговорящему населению [6]. В распространение ложных сведений участвуют представители различных организаций, преследующих определенные цели и выгоду в дестабилизации социального настроения, нанося тем вред политическому и экономическому секторам государства, путем оплаты специальной провокационной рекламы на платформах видео сервисов и социальных сетей. Согласованность действий таких организаций увеличивает эффективность влияния на мнение пользователей и их настроения.

На основе обзора и изучения множества источников, придерживающихся различных взглядов, и выступлений журналистов и блогеров, можно выделить используемые ими приемы для убедительности представляемых ими недостоверных фактов:

- однополярность, представление одной точки зрения;
- синхронность – резкая одновременная подача одного и того же материала, зачастую даже без изменения текста;
- попытки избавиться от инакомыслия;
- использование минимального количества фактов и максимального количества эмоциональных высказываний.

Кроме того, многие журналисты и видеоблогеры используют в своей работе эффект доктора Фокса, психологический эффект, заключающийся в том, что выразительность диктора может полностью завуалировать для слушающих бесполезность и вымышленность всего материала. Точнее говоря, имеется корреляция между положительными оценками слушателей по части качества выступления и степенью импрессивности журналиста [7].

Таким образом, такое представление информации является спланированным действием, направленным не на информирование пользователей, а на дестабилизацию мнений.

Автором данной статьи разработаны меры для эффективного анализа и углубленного понимания новой информации, а именно:

- обращать внимание на эмоциональность подачи, количество фактов;
- оценить, не противоречит ли заявления, изложенные в сообщении, информации из других источников;
- оценить репутацию автора данных материалов, благодаря чему можно оценить его объективность;
- наличие ссылок на первоисточник;
- обратить внимание на детали, при возможности их в других источниках;
- проверить историю взаимодействия с данным объектом.
- правила использования цитат, которые зачастую используются без контекста и ссылок.

Использование ресурсов, специализирующихся на проверке информации, такие как «Проверено» и «Fakecheck», также могут помочь в анализе достоверности информации, но интернет-издания могут совершать ошибки, поэтому также необходимо анализировать логические ошибки.

Для борьбы с распространением недостоверной информации должна проводиться быстрая реакция на любые события и даваться подробная своевременная информация. Поддержка общественных организаций по информированию населения и организации государственных информационных источников во всех возможных ресурсах интернета так же способствует правильному информированию населения. В правовом регулировании вводятся ряд запретов на осуществление информационно-психологического воздействия, проводится идеологическая информационная работа среди населения [8].

В качестве мер по ограничению возникновения нежелательной рекламы при посещении видео ресурсов и социальных сетей рекомендуется установить и правильно настроить системы антивирусной проверки веб ресурсов. Большинство веб-сайтов содержат привлекательные названия, рассчитанные на манипулирование любопытством или иными чувствами пользователей с целью переадресации пользователей на другие сайты и получения их личных данных. Система антивирусной проверки может блокировать вход на подозрительные сайты с нежелательным контентом или низкой репутацией. Также следует установить программы обеспечения безопасности, такие как SIEM-системы, системы учёта рабочего времени и др. При посещении различных веб-сайтов также может возникать всплывающая реклама, которая может нести положительный и отрицательный эффект воздействие, первый заключается в рекламе услуг, интересных пользователям и не нарушающих законы Республики Беларусь, второй – распространение недостоверной информации, призывы к насилию, и иные противоправные действия. Для блокировки всплывающей рекламы в браузере могут использоваться такие приложения как Adguard, AdBlock, Ad Muncher, При этом следует помнить, что использование такого рода программ может привести к некорректной работе некоторых веб-сайтов. В случае получения электронных сообщений от незнакомых лиц не рекомендуется открывать их содержимое и переходить по ссылкам, указанных в таких сообщениях.

Таким образом, на каждого пользователя социальных сетей и видео сервисов возлагается индивидуальная ответственность по анализу информации и определению степени ее достоверности, а также ограждение своих родственников от воздействия нежелательной рекламы. Представленные меры по ограничению возникновения нежелательной информации не являются максимально эффективными, но способствуют защите от социальной инженерии.

Список использованных источников:

1. Социальная инженерия в 2021 году / АО «Лаборатория Касперского». – Оpubл. 20.08.2021. – Режим доступа: <https://docs.cntd.ru/document/499074140> – Дата доступа: 01.04.2022.
2. Светлана Собалева. Социальная инженерия. [Электронный ресурс] – Оpubл. 06.0.2019 – Режим доступа: <https://stekspb.ru/blog/socialnaya-inzheneriya> – Дата доступа: 30.03.2022.
3. Закон Республики Беларусь «О внесении изменений и дополнений в некоторые законы Республики Беларусь по вопросам рекламы» от 03.01.2013 г. № 15-3.
YouTube рекламирует мошенников. [Электронный ресурс]. – Режим доступа: <https://zen.yandex.ru/media/id/5d3c48671ee34f00aed7792c/youtube-reklamiruet-moshennikov-obescaiuscih-vyplatu-ot-gosudarstva-razlichnyh-summ-5ebe1ee28600f212158d078d> – Дата доступа: 30.03.2022.
4. Реклама в контенте для детей и контролируемых аккаунтов. [Электронный ресурс] – Режим доступа: <https://support.google.com/youtube/answer/9713557?hl=ru> – Дата доступа: 30.03.2022.
Пример явного нарушения. [Электронный ресурс] – Режим доступа: <https://www.youtube.com/channel/UC2ErIXePrCMUVGglpgg1SeQ> – Дата доступа: 30.03.2022.
5. YouTube начал блокировку каналов российских медиа. [Электронный ресурс] – Режим доступа: <https://www.rbc.ru/society/11/03/2022/622b865f9a794703dac56740> – Дата доступа: 30.03.2022.
6. Facebook использует свои платформы для распространения фейков и психологических атак. Новости первого канала. [Электронный ресурс] – Режим доступа: https://www.1tv.ru/news/2022-03-02/422433-facebook_ispolzuet_svoi_platformy_dlya_rasprostraneniya_fejkov_i_psihologicheskikh_atak – Дата доступа: 30.03.2022.
Разжигание межнациональной розни. [Электронный ресурс] – Режим доступа: <https://zen.yandex.ru/media/riafan.ru/razjiganie-mejnacionalnoi-rozni-deputat-butina-o-licemernoi-politike-facebook-i-instagram-622b7ddab2c8b30490b3058e> – Дата доступа: 30.03.2022.
7. Эффект доктора Фокса. [Электронный ресурс] – Режим доступа: <https://lifemotivation.online/razvitielichnosti/samorazvitiieffekt-doktora-foksa> – Дата доступа: 30.03.2022.
8. Защита населения от искаженных фактов. [Электронный ресурс] - Режим доступа <https://www.sb.by/articles/u-istiny-ne-byvaet-dvoynikov.htm> – Дата доступа: 30.03.2022.

UDC 366.636.2

SOCIAL ENGINEERING IN VIDEO SERVICES AND SOCIAL NETWORKS

Mokerov V.S., Student of the group 961402

Belarusian State University of Informatics and Radioelectronics¹, Minsk, Republic of Belarus

Belousova E.S. – PhD in technical sciences, associate professor

Annotation. The author of the article describes the personal experience of detecting social engineering when using social networks and video resources. The article presents examples of attempts to manipulate the social behavior of users by advertising prohibited goods, providing false pro-political information, blocking state media channels. The methods and techniques used by journalists and video bloggers in order to attract the attention of users and impose false information are described. The measures for analyzing the reliability of information and limiting the occurrence of unwanted advertising when visiting video resources and social networks are provided.

Keywords. Social engineering, social networks, video services, fakes, false information.