Секция

ИНФОРМАЦИОННОЕ ПРАВО

УДК 004.62

УТЕЧКА ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Барткив Н.Н.
Курсант 3 курса ФКП
Академии МВД ДНР имени Ф.Э. Дзержинского

Аннотация: в современном мире социальные сети стали неотъемлемой частью жизни человека. Мы спокойно пишем личную информацию на страницах, выкладываем множество личных фотографий. При этом забываем, что социальные сети – это открытая платформа, где каждый может найти информацию про интересующего его гражданина. Эта информация доступна не только в социальных сетях, но и через обычные поисковые системы только по имени и фамилии. Следовательно, благодаря стремительному развитию сети Интернет, частная жизнь граждан должна быть защищена не только на законодательном уровне, но и самими пользователями социальных сетей.

Ключевые слова: социальная сеть, пользователь, аккаунт, конфиденциальность, утечка информации, искусственный интелект.

INFORMATION LEAKAGE ON SOCIAL NETWORKS

Bartkiv N.N.

Annotation: in the modern world, social networks have become an integral part of human life. We calmly write personal information on the pages, post a lot of personal photos. At the same time, we forget that social networks are an open platform where everyone can find information about the citizen they are interested in. This information is available not only on social networks, but also through regular search engines only by first and last name. Consequently, thanks to the rapid development of the Internet, the private life of citizens should be protected not only at the legislative level, but also by the users of social networks themselves.

Key words: social network, user, account, privacy, information leakage, artificial intelligence.

Перед тем как начать рассуждать о проблеме утечки информации в социальных сетях следует дать определение тому, что такое социальная сеть.

Социальная сеть – онлайн-платформа, которая содержит в себе сервисы мгновенной отправки сообщений, СМИ, создания сообществ и групп различной тематики по интересам, маркетинга, личного информирования и рассылки об объекте интереса пользователей, содержит элементы искусственного интеллекта, имеет возможности персонализации и создания представительской страницы аккаунта, а также которую люди используют для создания социальных отношений с другими людьми, с которыми могут иметь офлайн-связь и/или схожие интересы и повод к взаимодействию, ознакомления и изучения публикуемой информации различными источниками и развлечения, заработка финансовых средств путём создания продукта, либо услуги, которая пользуется спросом среди пользователей социальной сети и для удовлетворения потребности во внимании, занятием социальной, волонтерской и политической, общественной деятельностью, влиянием на людей, публикацией собственно произведенного контента, ведением блога, охватом аудитории различных социальных слоёв. Социальным сетям характерно то, что они доступны для различных социальных слоёв общества, вне зависимости от территориальной и юридической принадлежности к какому-либо государству.

На заре создания социальных сетей, когда они ещё не вошли в моду и не воспринимались как должное, уже тогда скептические умы, недоверчивые люди, учёные и специалисты в области информационных технологий заявляли о небезопасности социальных сетей в плане сохранения личной тайны, конфиденциальности и приватности пользователей. Они утверждали, что социальные сети это проекты спецслужб для сбора информации о населении, управления их мнением и главенствующими идеями, а также получения экономической выгоды от населения транснациональными компаниями. Анализируя и исследуя проблему можем утверждать, что основания так считать имеются. Не раз мир мог наблюдать в новостях, как вскрывались факты слежки, нарушения конфиденциальности, утечки информации, влияния на общество, осуществление революций, распространения ложной информации, цензуры в социальных сетях.

Социальные сети собирают информацию о пользователях несколькими способами:

- пользователи сами её выдают, публикуют;
- собирают информацию вне ведома и без согласия пользователей;
- составляют портрет пользователя на основе анализа поведения искусственным интеллектом (ИИ) узкой специализации.

Кратко рассмотрим эти способы. Начнем с первого способа. Всё начинается с регистрации. Вы вводите свои имя, фамилию, дату рождения, номер телефона, адрес электронной почты и т.д. и т.п. в различном порядке, в зависимости от вида соцсети. И самый главный момент. Пользователь ставит галочку о том, что ознакомился с правилами соцсети, политикой конфиденциальности и согласен с ними, принимает условия и обязуется им следовать. Собственники социальной сети тем самым снимают с себя обязательства за нарушение международных и конституционных прав и свобод человека касаемо приватности.

Далее пользователи в социальной сети рассказывают о своих интересах, работе, обучении, службе в силовых структурах, хобби, прочей деятельности, месте проживания, родном городе, публикуют фотографии о местах, которые посещают, семье, имуществе, какой-либо деятельности, рассказывают о своих страхах, фобиях, слабостях, определяющие их психотип и соответствующие потребности, “подписываются” на сообщества, группы, каналы, чаты соответствующие их интересам, публично на своей странице рассказывают о своих планах, целях, мировоззрении, “добавляя в друзья” круг общения соответствующих их интересам, участвуя в опросах, заполняя анкеты, выказывая одобрения о каком-либо контенте.

Второй способ. Существуют алгоритмы, которые на основе присвоенного параметра отправляют пользователю в новостные ленты соответствующий контент, подсылают информацию и рекламу на основе этого параметра. Кто присваивает этот параметр? У социальных сетей есть инструменты позволяющие исследовать приватный контент, вроде сообщений, скрытых альбомов, аудиозаписей, музыки, документов, скрытой личной информации, закрытых сообществ и подобного. Также ИИ анализирует содержание сообщений, поведения пользователя и содержание его страницы в пределах и за пределами (приобретая информацию о посещаемых сайтах и запросах в поисковых системах IP адреса пользователя и соответствующих ему аккаунтов и цифровых меток) границ соцсети. И на основании этого ИИ подсовывает пользователю контент, продукты, услуги, которые наиболее ему подходят. То есть, мы уже сталкиваемся с нарушением приватности, ведущей к утечке информации в социальных сетях. И собранные данные могут продавать не только государственным органам безопасности и государственным силовым структурам, но и транснациональным компаниям и частным компаниям, которые собирают статистику о какой-либо социальной группе, имея необходимость влияния на них. Эти инструменты несанкционированного доступа к приватной информации позволяют преступникам публиковать и сливать в сеть приватную и скрытую информацию о пользователях.

Третий способ. Он дополняет предыдущий способ, но несколько отличается от него сутью излагаемого. ИИ сегодня способен на основании информации о действиях пользователя, ключевых слов в сообщениях, комментариях и постах составить детальный и точный на более чем 90% психологический и биологический (раса, возраст) портрет пользователя и отправлять персонифицированную информацию, подходящую пользователю. Это отсылает нас к нарушению приватности. А нарушение приватности ведёт к более широким возможностям шпионажа.

Сегодняшние крупные социальные сети используют и применяют самые современные и эффективные методы и системы безопасности. Так что чаще всего редко кто готов незаконно испытать их эффективность и непосредственно проникнуть в защищенное информационное поле сети и получить информацию о содержании и отчётах об интересах и персональной оценке какого-либо аккаунта.

Но имеют место быть частные случаи утечки информации в социальных сетях. Обойти техническую, программную защиту социальных сетей мало кому под силу, а также за этим следуют разбирательства и наказание за противоправные действия в

отношении соцсети. А значит, чаще всего преступники получают доступ к содержанию и управлению аккаунтом путём введения в заблуждения и манипуляцией пользователем-владельцем аккаунта и выявлением, использованием его личных уязвимостей и неосторожностей [1].

В дело вступает неосторожность и невнимательность людей. Пользователи часто собственными ошибками открывают дорогу для того, чтобы в отношении их удалось совершить преступной деяние. Пользователи много лишнего рассказывают на своих страницах о своих интересах, публикуют достоверную информацию, номера телефонов, следуют трендам. Хакеры, являющиеся опытными психологами, составляют психотип человека и играя на слабостях пользователей подкидывают им ловушки, приманки (спам-рассылки)[2]. Собрав информацию о браузере (cookie, пароли, логины) злоумышленники проникают в аккаунт пользователя. Может быть еще СМС атака на номер телефона пользователя, которые будут подводить пользователя к тому, что он передаст доступ от аккаунта в руки злоумышленников. Таких вариаций множество.

Можно сделать вывод, что причиной утечки личной информации из социальных сетей является беспечность пользователей, недостаточная осведомленность пользователей о способах действий преступников, о методах безопасности и мерах предосторожности во время действия в интернет пространстве.

Важно отметить еще и то, что пользователи часто публикуют информацию, даже не подозревая о том, как близко она может подвести злоумышленника, либо стать инструментом к тому, чтобы привести к утечке информации. Например, часто пользователи, публикуя фотографии с места работы, давая информацию о месте работе, о геолокации своего аккаунта. Что можно использовать как угодно. Например, через социальную сеть внедряют сервисами сообщений или обманом принуждают к скачиванию программного обеспечения, которое уже прослушивает, читает содержание, записывает происходящее вокруг с помощью аппаратного обеспечения устройства, что в итоге приводит к плачевным последствиям не только для пользователя, но и для сообщества, государства[3].

Создавая аккаунт в социальных сетях, следует ни в коем случае не называть реальных данных. Выставить настройки, соответствующие режиму максимальной приватности и закрытости. Ни в коем случае не загружать никаких фотографий, музыки, книг, цитат и ничего, что указывало бы на принадлежность к какой-либо идее либо профессии. Не давать никакой информации, какая могла бы компрометировать и указывать на личность пользователя. Не вести диалога и не обмениваться информацией с непроверенными лицами. Заходить в социальную сеть только через защищенное соединение и через безопасное подключение, вручную ограничить полномочия и возможности приложения социальной сети на устройстве, если таковое приложение установлено, ограничить рассылки и умные ленты для ограничения возможностей создания портрета пользователя. Для обмена документами, личными файлами использовать проверенную электронную почту.

Однако, все эти меры не гарантируют отсутствие утечки информации, но снижают риск того, что такая беда случится.

Список литературы:

1. Понтироли С. Социальная инженерия, или Как «взломать» человека [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/blog/socialnaya-inzheneriya-ili-kakvzlomat-cheloveka/2559/
2. Саймон В.Л., Митник К. Искусство обмана. – Компания АйТи, 2004; ISBN-5-98453-011-2; 0-471-23712-4
3. Гридин А. Краткое введение в социальную инженерию [Электронный ресурс] – Режим доступа: https://habrahabr.ru/post/83415/