ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ИНФОРМАЦИОННОЙ ЭПОХИ

Лысак Б.В., студент (гр. РК-51 РТФ КПИ им. Игоря Сикорского);
Чикунова-Васильєва Н.П., ассистент (каф. ОТПГБ КПИ им. Игоря Сикорского)

Введение. Конец XX века задал тенденцию на стремительный рост информационной среды и её дальнейшую интеграцию в повседневную жизнь. Одно (и самое популярное) из проявлений интеграции – социальные сети. На сегодняшний день Facebook – самая популярная социальная сеть с охватом более 2 млрд пользователей [1]. Интеграция информационной среды в нашу жизнь привносит однозначно огромное количество удобств, но не стоит забывать о силе и возможностях информационно-телекоммуникационных систем, о негласном контроле социальных сетей и о необходимости осторожного обращения с персональными данными. Многие пользователи про это забывают до тех пор, пока не убедятся в этом на личном примере.

Актуальность темы. В США происходит невероятно важное расследование – в течении нескольких лет компания CambridgeAnalityca с помощью одного из приложений собрала информацию о более чем 87 млн пользователей Facebook [2]. Утечке подверглись публикации, отметки «Мне нравится» не только пользователей приложения, но и их друзей. Направлений использования данной информации множество. Некоторые из них: манипулирование сознанием избирателей во время организации и проведения выборов всех уровней; формирования общественного мнения «в нужном направлении» по любым вопросам. Так, по некоторым данным, благодаря именно таким манипуляциям Дональд Трамп стал президентом США [3]. Известно, что вопрос сохранения конфиденциальности персональных данных и предотвращения их использования в целях манипуляции на данный момент самый актуальный вопрос информационной безопасности.

Предмет исследования. Информация в социальных сетях и возможности ее использованиями третьей стороной.

Цель исследования. Оценить последствия использования информации, которая находится в социальных сетях и рассмотреть способы минимизации возможности использовать персональную информацию.

Основные результаты исследования. Общеизвестно, что информация – самое ценное, чем может владеть человек. Чем больше нужной информации известно, тем легче принимать правильные, взвешенные решения. В военном деле и политике информация невероятно важна. Досконально зная не только сильные и слабые стороны противника, но и все параметры внешних обстоятельств, можно успешно выполнить действия, которые были задуманы. Именно поэтому существуют шпионы, их основная цель – завладеть информацией противника. В XX веке произошло несколько значимых шпионских операций, без которых мир бы не был таким, какой он есть сейчас.

С конца XX века ситуация несколько изменилась: во все сферы деятельности проник Интернет, а с 1999 года информация буквально витает в воздухе, поскольку многие устройства начали использовать такие

беспроводные технологии как Wi-Fi для доступа в Интернет. На сегодняшний день информации настолько много, что для того, чтобы ею завладеть, нужно только знать где её перехватывать. Иногда информация защищена, и для того, чтобы пользоваться ею, её следует расшифровать. Но защита не безупречна, поэтому иногда дешифровать информацию могут и третьи лица, для использования её в целях манипулирования, шантажа, вымогательства.

Благодаря социальным сетям, таким как Facebook, Twitter, Instagram и др., информация о вас, о вашей семье и о ваших знакомых находится буквально на поверхности. Если вы ведёте активную социальную жизнь, узнать о чём вы думаете, где живёте, кто вам нравится меньше, а кто - больше можно даже не прибегая к дешифрации ваших личных данных. Многие вещи в Сети появляются только из-за того, что вы (или кто-то другой) считаете нужным поделиться со всем миром своей точкой зрения или фотографией. Анализ вашего профиля (или небольшой группы профилей) в социальной сети, на удивление, довольно нетрудное занятие, которое позволяет злоумышленникам воздействовать на вас.

Помимо мелких злоумышленников, информацию, которая лежит в свободном доступе могут использовать для более серьёзных целей. Так, компания CambridgeAnalityca собрала невероятно большой массив данных пользователей Facebook и с помощью определённого рода инструментов смогла создать психологические портреты американских избирателей для правильного продвижения кандидатуры Дональда Трампа во время президентских выборов [3]. Эта информация поддалась огласке, но наверняка есть не одна компания, направление деятельности которой схоже направлению CambridgeAnalityca. Вашу публичную информацию могут использовать и велика вероятность, что уже используют для составления психологических портретов населения или какой-либо целевой аудитории для продвижения желаемых целей.

Для предотвращения подобного рода манипуляций следует относиться к выкладываемой информации бережно, как и к любой исходящей от вас информации в жизни. Прежде всего, ставьте перед собой вопрос: «А стоит ли эта информация того, чтобы быть выложенной в Интернете или же её отсутствие не критично?». Далее следует ознакомиться с политикой конфиденциальности (privacypolicy) сервиса, которым вы пользуетесь. У каждого сервиса, который так или иначе владеет информацией, должен быть документ, регламентирующий какую информацию сервис может обрабатывать, например, для контекстной рекламы, а какая остаётся необработанной, вашей сугубо личной. Если вы согласны с политикой конфиденциальности, то далее следует просмотреть настройки вашего профиля в выбранном сервисе, возможно, настроить параметры публичной доступности публикуемых вами данных так, как вам захочется – оставить их полностью публичными или же ограничить к ним доступ. Никогда не делитесь паролями ваших учетных записей, это наносит вред вашей конфиденциальности. Проведя эти действия, вы точно будете знать насколько публична ваша информация и какой уровень защиты предлагается определённым сервисом.

Однако, информацию собирают не только злоумышленники, но и спецслужбы разных государств. Тут речь идёт не только о той информации, которая находится в социальных сетях и условно «не защищена», но и про информацию о ваших перемещениях, посещении мероприятий и разного рода мест, даже о ваших крупных покупках. На сегодняшний день известно, что информацию о своих гражданах собирает США, РФ, КНР.

После событий 9 сентября 2001 г. АНБ США была создана специальная программа в целях борьбы с терроризмом, основная задача которой – следить за определёнными гражданами продолжительное время, записывая действия последних вплоть до минуты. Летом 2013 г. эта информация стала известной благодаря Эдварду Сноудену и ресурсу «TheGuardian» [4]. Однако, была доказана неэффективность этой программы, за всё время работы она сыграла ключевую роль лишь в одном случае [5]. В феврале 2016 г, тоже прикрываясь целями борьбы с терроризмом, ФБР потребовало Apple реализовать обход блокировки устройств компании [6]. Глава корпорации, Тим Кук, написал открытое письмо, в котором сполна осветил сложившуюся ситуацию и дал отказ реализации обхода, поскольку это сильно вредило бы безопасности всех устройств. Стоит заметить, что через некоторое время ФБР разблокировали устройство без помощи Apple [7].

В РФ почти год как принят «антитеррористический пакет» законопроектов, предложенный Ириной Яровой. Согласно последнему, вся информация, которая была опубликована вами в Интернете, сохраняется год, телефонные звонки и СМС – до трёх лет, а каждый сервис, который поддерживает шифрование данных обязан помочь ФСБ расшифровать эти данные [8], иначе будет заблокирован. Сервис по обмену сообщений «Telegram» отказался обеспечивать подобную помощь ФСБ. Объясняется это двумя причинами. Во-первых, имея универсальный алгоритм дешифрации (так называемый «ключ») сообщений ставится под вопрос защита любой переписки от третьих лиц, ведь любой может завладеть этими «ключами». Во-вторых, «Telegram» использует такой тип шифрования, при котором «ключи» случайным образом генерируются на устройствах самих пользователей, а не на серверах сервиса, так информация остаётся наиболее защищённой.

В Китае тоже нет как такового открытого Интернета и всё находятся под наблюдением. КНР по праву заслужила звание не демократичной страны, но нельзя утверждать, что это самая незащищенная страна. В середине апреля этого года китайские полицейские задержали мужчину-злоумышленника среди многочисленной толпы на концерте [9]. С 2015 года в Китае начали собирать национальную базу данных используя функцию распознавания лиц, которая называется «Острый глаз». К 2020 году китайское правительство планирует ввести «рейтинг общественной надёжности». Согласно нему, гражданам с более высоким рейтингом будут предоставляться социальные пособия, открываться туристические визы или кредиты с выгодными процентными ставками [10]. Это довольно интересная инициатива, которая работает по принципу кармы: будь законопослушным гражданином – государство будет

идти к тебе навстречу.

Конечно, приведённые выше примеры показывают, как глобальная слежка ограничивает свободу простого гражданина страны. Но, давая доступ к своим персональным данным, вы можете улучшить безопасность собственного государства от правонарушений разного масштаба и сделать так, чтобы государство помогало вам, в конечном итоге.

Выводы. В XXI веке уделять внимание модернизированию вашей информации, которая находится в Интернете необходимо, особенно информации персонального характера. Социальные сети следует рассматривать не только с позиций коммуникационной среды, но и как составляющую современного оружия – информационного.

Несмотря на то, что государства собирают информацию о своих гражданах, эти действия происходят в целях улучшения национальной безопасности государства и положения каждого гражданина в последнем. К сожалению, вопрос национальной безопасности конфронтируют с вопросом демократизации и свободы общества.

Научный руководитель: Фурашев В.М., к.т.н., доцент (каф. ИППИС НТУУ «КПИ им. Игоря Сикорского»)

Литература

1. Most popular social networks worldwide as of April 2018, ranked by number of active users (in millions), 2018. Електронный ресурс**:**https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
2. David Ingram, Facebook Says Data Leak Hits 87 Million Users, Widening Privacy Scandal, 2018. Електронный ресурс: https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM
3. Как CambridgeAnalytical «выиграла» выборы для Трампа: TheGardian, 23 марта 2018. Електронный ресурс: https://meduza.io/feature/2018/03/23/kak-cambridge-analytica-vyigrala-vybory-dlya-trampa-the-guardian
4. Edward Snowden and the NSA files – timeline, Wed 21 Aug 2013. Електронный ресурс: https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
5. Сбор телефонных метаданных АНБ незначительно помог в борьбе с терроризмом, 13 января 2014. Електронный ресурс: https://zn.ua/WORLD/sbor-telefonnyh-metadannyh-anb-neznachitelno-pomog-v-borbe-s-terrorizmom-136569_.html
6. Apple отказалась исполнять требование ФБР предоставить доступ к айфону террориста из Сан-Бернардино, 17 февраля 2016. Електронный ресурс: https://tjournal.ru/23244-apple-otkazalas-ispolnyat-trebovanie-fbr-predostavit-dostup-k-ayfonu-terrorista-iz-san-bernardino

7. ФБР самостоятельно разблокировало iPhone стрелка из Сан-Бернардино и отозвало судебные претензии к Apple, 29.03.2016. Електронный ресурс: https://itc.ua/news/fbr-samostoyatelno-razblokirovalo-iphone-strelka-iz-san-bernardino-i-otozvalo-sudebnyie-pretenzii-k-apple/

8. «Пакет Яровой» принят. И это очень плохо, 24 июня 2016. Електронный ресурс: https://meduza.io/feature/2016/06/24/paket-yarovoy-prinyat-i-eto-ochen-ploho

9. Facial recognition at a concert leads to arrest of cyber fugitive, 2018-04-11. Електронныйресурс: http://www.ecns.cn/2018/04-11/298786.shtml

10. «Острый глаз» вместо «Большого брата»: как китайские власти массово следят за жителями страны, 15 апреля 2018. Електронный ресурс: https://meduza.io/feature/2018/04/15/ostryy-glaz-vmesto-bolshogo-brata-kak-kitayskie-vlasti-massovo-sledyat-za-zhitelyami-strany?utm_source=telegram&utm_medium=live&utm_campaign=live