В.И. Шаповалова

ВОПРОСЫ ЗАЩИТЫ ЛИЧНЫХ ДАННЫХ

(Томский государственный архитектурно-строительный университет)

Информационная безопасность в современном мире в значительной степени становится главной проблемой безопасности в нашей повседневной жизни. С постоянным увеличением онлайн активности информация становится все более и более важным орудием в руках человека. Важность защиты информации сегодня невозможно переоценить. Владение информацией позволяет человеку контролировать, создавать и разрушать не только компании, бизнес, но и отдельных людей. Сбор и правильное обращение с информацией помогают различным корпорациям расти и увеличивать свою прибыль, оставаясь весьма и весьма конкурентоспособными на рынке. Но не только сбор общей информации играет важную роль. Персональная информация может оказаться чрезвычайно ценной в зависимости от того, как ею воспользоваться[1].

Тем не менее, часто компании и различные организации принимают крайние технологические меры для защиты своей информации, но их работа зачастую оказывается под угрозой, поскольку сотрудники не понимают, что защита их личной информации также имеет немалое значение и утечка абсолютно любой информации может нанести ущерб организации, в которой они работают. Сегодня большинство людей не принимают необходимых мер предосторожности, для защиты своих персональных данных. Представим себе крупную организацию с высочайшим уровнем внутренней информационной защиты, но что может произойти, если личная электронная почта генерального директора или любого другого значимого сотрудника, работающего с огромным количеством данных, будет взломана, а вся информация, хранящаяся там, будет украдена? Есть еще сотни сценариев, подобных этому, которые демонстрируют, что надлежащая информационная безопасность нужна каждому отдельному человеку[2]. Поскольку социальные сети являются важной и неотъемлемой частью нашей жизни, большинство людей получают информацию исключительно оттуда. Но чем чревато массовое распространение ложной информации внутри популярных платформ? Ответ на этот вопрос вполне очевиден – это влечет за собой информационный кризис. С этой проблемой не так просто бороться, потому что зачастую информационный кризис возникает как рефлекс социальных изменений, а они в свою очередь представляют собой непрекращающийся постоянный процесс. Это часто усугубляет и без того сложную ситуацию, поскольку ложная информация распространяется публично, вызывая массовые взрывы реакций, которые, как правило, несут яркий и эмоциональный характер, порождая беспорядки и дальнейшие волнения[3].

Поддельные новости – это пропаганда, которая состоит из преднамеренной дезинформации или обмана, распространяемого в традиционных печатных и вещательных средствах массовой информации или онлайн-социальных сетях. Они пишутся и публикуются с намерением ввести в заблуждение, чтобы нанести ущерб частным лицам, организациям и даже целым сферам жизнедеятельности человека, или же получить финансовую, а возможно и политическую прибыль. Такой вид ложной информации часто подается с приукрашенными и запоминающимися заголовками, скрывающими за собой частично или полностью сфабрикованный пакет информации, нацеленный на увеличение читательской аудитории, онлайн-обмена данными и как следствие дохода. В основном весь этот поток фейковых новостей интегрируется в популярные социальные сети и, что можно легко заметить, вызывает именно негативные эмоции, которые, как известно, являются одними из самых сильных. Получив такую порцию новостей читателю, безусловно, захочется ими поделиться, и таким образом происходит дальнейшее распространение отрицательных эмоций, словно вируса. Часто распространителями являются те, кто просто не понимает, что это может иметь огромные последствия, и относится к этому как к шутке[4].

Если в случае с заполнением медиа каналов манипулирующими новостям можно рассчитывать только на собственную осведомленность и объективность, то какие меры можно предпринять непосредственно для защиты собственной информации? Один из способов - аутентификация при попытке получить доступ к каким-либо данным. Она гарантирует, что только уполномоченным лицам разрешен доступ к определенным областям в соответствии с политикой компании, если говорить об общей безопасности, или настройками персональных гаджетов, если говорить о частной безопасности. Еще один способ обеспечения конфиденциальности – это использование шифрования. Сообщения, передаваемые внутри канала, в случае утечки окажутся зашифрованными и недоступными для третьих лиц. Разумеется, не стоит забывать и о том, что параллельно с ростом уровня защиты данных также развиваются и технологии, позволяющие взламывать и обходить эту защиту[5]. Помимо использования технической защиты информации важно не забывать и о собственной бдительности. Первое правило, которого в обязательном порядке должен придерживаться каждый сознательный человек, нужно быть уверенным что вы знаете тех, кто получает вашу личную и финансовую информацию. Не разглашайте личную информацию по телефону, по почте или через всемирную паутину. Если вы получаете электронные письма или сообщения, содержащие ссылки, не переходите по этим ссылкам, сначала проверьте источник-отправитель. Вопрос утилизации информации также имеет немаловажную роль. Прежде чем избавляться от компьютера или любого другого технического устройства, позволяющего хранить данные, избавьтесь от всей личной информации, которая там содержится. Используйте программу очистки, чтобы перезаписать весь жесткий диск компьютера, отформатируйте карту памяти на своем смартфоне, уничтожьте сим-карту, удалите все медиа данные, заметки и

тому подобное. Еще одно, пожалуй, основное правило – не следует распространять слишком много личной информации о себе в социальных сетях, а при выборе паролей для доступа к определенным ресурсам не стоит выбирать сочетание слов или символов, которое можно ассоциировать с вашими личными данными. Эти простые и, как может показаться, тривиальные правила, к сожалению, часто пренебрегаются многими пользователями, а ведь банальное соблюдение этих мер безопасности позволит в большинстве случаев, имеющих место в повседневной жизни, уберечь ваши данные[6].

Персональная информационная безопасность должна быть заботой каждого человека в нашем современном мире. Пренебрежение защитой персональных данных может сделать вас более уязвимыми для их кражи. Помимо этого, пользователи должны ответственно подходить к распространению любой информации и знать, что их действия в сети имеют последствия в реальной жизни. С точки зрения технической защиты хочется отметить, что существование продвинутых, умных технологий, позволяющих обезопасить данные, не может гарантировать полную защиту вашей информации, поскольку с ростом значимости владения информацией появляется бесконечное множество таких же продвинутых и умных способов ее теневого получения.

Литература

1. Грошева Е. К. Информационная безопасность: современные реалии [Текст] / Е. К. Грошева, П. И. Невмержицкий // Бизнес-образование в экономике знаний. – 2017. – №3. – С. 35-38.

2. Лопатин Д. В. Информационно-коммуникационные угрозы [Текст] / Д. В. Лопатин, М. С. Анурьева, Е. А. Еремина, Е. А. Заплатина, Ю. В. Калинина // Гаудеамус. – 2013. – №2(22). – С. 46-51.

3. Чванова М. С. Исследование влияния Интернета на социальные потребности пользователей [Текст] / М. С. Чванова, М. В. Храмова, И. А. Слетков, И. А. Кисилева, А. А. Молчанов, Н. А. Котова // Вестн. Тамбовского ун-та. Серия: Гумантираные науки. – 2016. – №12(164). – С. 7-25.

4. Рассадина Т. А. Интернет-зависимость: информационно-коммуникативный аспект [Текст] / Т. А. Рассадина // Известия высших учебных заведений. Поволжский регион. Общественные науки. – 2015. – №2(34). – С. 98-111.

5. Михнев И. П. Информационная безопасность на просторах мобильного интернета [Текст] / И. П. Михнев // Образовательные ресурсы и технологии. – 2015. – №1. – С. 23-27.

6. Шабуров А. С. О повышении эффективности защиты персональных данных в информационных системах открытого типа [Текст] / А. С. Шабуров, А. А. Миронова // Вестн. Пермского нац-го исслед-го политехнического ун-та. Электротехника, информационные технологии, системы управления. – 2015. – №1. – С.23-34.