ЦИФРОВАЯ БЕЗОПАСНОСТЬ, ЗАЩИЩЕННОСТЬ И АНОНИМНОСТЬ В ИНТЕРНЕТ ПРОСТРАНСТВЕ КАК НОВЫЕ ЦЕННОСТИ СОВРЕМЕННОГО ОБЩЕСТВА

Назаретян А. Р. (Москва, Россия)

Аннотация: *В связи с переходом в цифровое пространство многих процессов, ученые все больше обращают внимание на безопасное пребывание интернет-пользователей в сети и угрозы, связанные с процессом цифровизации. В данной статье рассмотрена актуальность вопросов цифровой безопасности и анализ последствий ее нарушения, который позволяет выявить формирование нового запроса у современного общества на сохранение приватности и защиту личных данных.*
Ключевые слова: *современное общество, цифровая безопасность, анализ данных, защита данных, интернет-пользователь.*

DIGITAL SECURITY, SECURITY AND ANONYMITY IN THE INTERNET SPACE AS NEW VALUES OF MODERN SOCIETY

Nazaretyan A. R. (Moscow, Russia)

Abstract: *Due to the transition into the digital space of many processes, scientists are increasingly paying attention to the safe stay of Internet users in the network and the threats associated with the digitalization process. This article examines the relevance of digital security issues and analyzes the consequences of its violation, which allows us to identify the formation of a new request from modern society to preserve privacy and protect personal data.*
Keywords: *modern society, digital security, data analysis, data protection, Internet user.*

Каждый день мы не замечаем, как цифровая среда все больше взаимодействует с нами. Рабочие процессы хранения документов и счетов, личные переписки и покупки теперь происходят в интернет–пространстве. Но каждое наше посещение сайта, приложения, запрос в поисковике могут перестать быть сугубо нашими. Сегодня распространено мнение о том, что информационный век поставил под угрозу конфиденциальность и безопасность человека. Невероятное количество данных о пользователях собирается каждую минуту, как только мы начинаем взаимодействовать с глобальной сетью. Эти данные собираются и контролируются крупными корпорациями, такими как Facebook, Google, Яндекс и другими.

Сосредоточение таких возможностей у крупных игроков рынка делает их «феодалами данных», поскольку именно данные пользователей в эпоху цифровизации играют существенную роль.

На данном этапе у современного человека нет даже выбора не выходить в интернет и не пролистать новостную ленту в Instagram, не написать сообщение в WhatsApp мессенджере или не забить в поисковике свой запрос– эти действия стали неотъемлемой частью нашей жизни, от которой мы уже вряд ли сможем отказаться.

В своей статье от 2015 года политолог Роксана Раду писала, что более 90% пользователей сети интернет в США используют поисковые системы. Одной из таких поисковых систем является Google. Данной системе принадлежит более 90% рынка онлайн-поиска. В 2014 году средний годовой доход корпорации составил 66 миллиардов долларов [1]. С появлением таргетинга действия компании сосредоточены на постоянном сборе данных о пользователях по всеми миру. Взаимодействия с пользовательскими данными имеют определенные цели – разработка и реализация бизнес модели, которая основана на предсказании запросов пользователей на основе их интересов для рекламы и дальнейшей бизнес–аналитики. При этом компания создает отдельные сервисы по анализу и сбору аналитики пользователей для клиентов. Например, всем, кто зарегистрирован в Google Аналитик и имеет платный пакет, доступны услуги, которые позволяют отследить поведение пользователей своего сайта: интересы пользователей, частые запросы, пол, возраст, город и многое другое. Большинство посетителей сайтов не знают о том, что их действия потом будут переданы аналитикам. Почти на каждом сайте можно увидеть push-уведомление о том, что данный сайт собирает cookie. На первый взгляд сбор небольших фрагментов данных, которые и собирают cookie, может показаться безобидным, но в руках злоумышленников могут привести к взлому доступов от приватных аккаунтов, распространению ложной информации, хищению личных данных и другим последствиям, которые нарушают приватность пользователей и могут пагубно повлиять на жизнедеятельность человека [2].

Похожие действия по сбору пользовательских данных можно наблюдать со стороны американской социальной сети Facebook, которая с недавнего времени владеет также популярной социальной сетью Instagram и мессенджером WhatsApp. С каждым годом противников политики Марка Цукерберга, основателя и руководителя

Facebook Inc, все больше. В 2018 году множество людей и даже представители американского правительства стали жертвами хищения их личных данных из социальной сети Facebook. Неизвестными злоумышленниками были раскрыты и похищены данные и информация о более чем 50 миллионов пользователей. Этот инцидент вызвал агрессивную критику в сторону политики безопасности компании и ее отношения к личным данным пользователей. Кроме утечки данных Цукерберг признался в том, что британская фирма «Cambridge Analytica», которая занимается аналитикой и работала вместе с командой Трампа в рамках предвыборной президентской компании, крала личную информацию миллионов пользователей Facebook [3].

Порой от безопасности данных и их системы защиты зависит не только репутация корпораций, но и политический, экономический и социальный аспект.

В 2019 году в самом крупном банке Российской Федерации ПАО «Сбербанк» был установлен факт утечки данных с личной информацией. Несмотря на сложные системы облачного хранения данных, многоуровневые системы идентификации около 60 миллионов данных по банковским картам были выставлены на продажу в некой системе прокси-серверов, которая позволяет совершить анонимное сетевое соединение, а именно в Tope. Но даже Tor, который во всем мире считается местом, где можно оставаться анонимным, не является таковым. Ученый Амирали Санатини в своей статье 2016 года доказывает, что невозможно оставаться анонимным, совершая пользовательские действия даже в Tope [4].

Сбор данных пользователей растет с количеством появления пользователей и появлением на рынке новых компаний, приложений в интернет–пространстве. В отчете «Freedom on the Net» за 2019 год говорится, что девять из каждых десяти пользователей интернета подвергаются активному онлайн–мониторингу. При этом было отмечено, что достижения в области искусственного интеллекта позволили отслеживать миллиарды учетных записей в режиме реального времени за секунды [5].

Можно заметить прямую корреляцию между ростом хищения и незаконного использования личных данных, хранящихся в цифровом пространстве и ростом чувства небезопасности среди пользователей. В связи с этим у современного человека появляются новые запросы на

цифровую безопасность. Центр инноваций в области безопасности США в 2018 году опубликовал свое исследование, в котором приняли участие 1015 американцев. Исследование показало, что двое из трех американских онлайн–пользователей ответили, что высокий рост числа подключенных к продуктам, связанных с глобальной сетью интернет, заставляет их беспокоиться о своей конфиденциальности и безопасности [6].

Хью Кох, профессор права и психологии Бирмингемского университета рассуждает о важности сохранности данных и создания работающих инструментов для их защиты. Ученый акцентирует внимание на растущем стрессе среди людей, связанном с утечкой данных. Последствия, связанные с недостаточной защищенностью данных, могут привести к неблагоприятным жизненным событиям, например, к необходимости переехать в другой город, потере работы, стрессу в отношениях и другим. В своей практике профессор все больше встречает такие случаи, когда у его клиентов после хищения данных уровень беспокойства и разрушения соответствовал признанному психологическому расстройству, например, расстройству адаптации, депрессивному расстройству, тревожному расстройству и, в крайнем случае, посттравматическому стрессу, что логически дает понять, насколько серьезной была проблема [7].

Помимо психологического дискомфорта, который человек испытывает от осознания слежки и незащищенности своих действий в цифровой среде, формируется ощущение сомнительной подлинности своего выбора и действий, совершающихся в интернет–пространстве. Возникает проблема реальности собственного выбора в связи с рекламными компаниями, которые могут предоставлять свои товары и услуги, преследуя пользователя, зная его интересы, характеристику поведения и используя другие инструменты влияния на пользователя.

Кроме того, хищение данных может привести к цифровым террористическим атакам, подрыву экономики, безопасности граждан, дезинформации населения или определенных лиц. Именно поэтому сегодня тенденция осознанного нахождения в интернет–пространстве и защиты своих данных становится все более популярной. Можно сказать, что конфиденциальность данных – это одна из самых растущих потребностей современного общества. Аналитиками предполагается, что в период с 2020-2025 год рынок услуг по защите данных вырастет более чем на 28% [8].

Американский эксперт по безопасности Брюс Шнайер, сотрудник Berkman и участник программы кибербезопасности Белферского центра школы Кеннеди, также рассуждает о важности цифровых данных и их безопасности. Шнайдер отмечает, что нахождение в интернет–пространстве и отсутствие полной защиты данных приводит к тому, что пользователь постоянно находится в стрессе и подвергает сомнению свои действия, поскольку не знает, где находится граница между безопасным и небезопасным в цифровой среде.

Защита данных, конфиденциальность и возможность оставаться анонимным в сети – это новый научный дискурс. Возможность защитить свои данные вскоре может стать привилегией для определенных представителей среди пользователей. Приватность как новая ценность современного общества все более обсуждаема, но пока у людей нет возможности демократически контролировать использование данных и инструментов их защиты в виде признанных законов на мировом уровне, цифровая безопасность так и не будет достижима для всех представителей современного общества, оставаясь триггером для хищения данных.

Литература

1. *Radu R.* Data control and digital regulatory space(s): towards a new European approach // Internet policy review. Journal on regulation. 2015. URL: https://policyreview.info/articles/analysis/data-control-and-digital-regulatory-spaces-towards-new-european-approach (дата обращения: 19.09.2020).

2. *Лавлинский Н. Е.* Применение систем веб-аналитики для исследования поведения пользователей сайта // Научные труды Вольного экономического общества России. 2014. URL: https://cyberleninka.ru/article/n/primenenie-sistem-veb-analitikidlya-issledovaniya-povedeniyapolzovateley-sayta (дата обращения: 19.09.2020).

3. Cabalhi J. Facebook User's Data Security and Awareness: A Literature Review // Journal of Academic Research. 2018.С. 1–9. (Дата обращения: 20.09.2020).

4. Amirali S. HOnions: Exposing Snooping Tor HSDirs // IEEE Conference on Communications and Network Security. 2016. URL: https://www.ccs.neu.edu/home/amirali/publications/HOnion_CNS_2016.pdf (дата обращения: 20.09.2020).

5. Report Freedom House. Freedom on the net 2019. Freedom House, 2019. URL: https://www.freedomonthenet.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf (дата обращения: 20.09.2020).

6. Digital Insecurity: As Billions of Products Connect to the Internet, Concerned Americans Prioritize Security and Privacy When Getting Them Repaired, Study Finds. Security Innovation Center, 2018. URL: https://www.prnewswire.com/news/security-innovation-center/ (дата обращения: 20.09.2020).

7. *Hugh K. Do* data breaches cause stress? // Modern Law Magazine Issue. 2019. № 46. С 50–51.

8. Data protection as a service market–growth, trends, and forecast (2020–2025). Mordor Intelligence, 2019. URL: https://www.mordorintelligence.com/industry-reports/data-protection-as-a-service-market (дата обращения: 20.09.2020).