ЛЕТНЯЯ ШКОЛА
по управлению интернетом

Ольга Исаева

Как Интернет изменил информационную приватность?

С появлением Интернета и Всемирной паутины (World Wide Web) доступ к информации стал значительно проще, равно как упростился доступ и к персональной информации пользователей. Сегодня значительная часть населения, имеющего доступ в Интернет, осуществляет такой доступ не только (или не столько) посредством стационарных компьютеров: все чаще для целей получения информации используются смартфоны и мобильный интернет. Пользователи устанавливают на свои устройства различные приложения, в которые вводят персональную информацию: мессенджеры[1] и социальные сети[2], банковские приложения[3], приложения магазинов[4] и проч. Чем активнее Интернет проникает в повседневную жизнь, тем больше возникает рисков нарушения приватности. В связи с этим вопрос усиления мер защиты приватности, а равно ответственности (за их несоблюдение) всё чаще поднимается как на национальном[5], так и на региональном[6] уровнях.

Разговор об изменении информационной приватности нельзя вести без предварительного краткого анализа, как именно вхождение Интернета в нашу повседневность изменило жизнь, поэтому дальнейшее изложение будет построено на логике «изменение – влияние на приватность – оценка».

Прежде всего, следует отметить, что согласно исследованию, проведенному компанией Avast совместно с YouGov, на сегодняшний день Интернет все чаще используется для общения (как следует из результатов опроса, в котором приняли участие более тысячи респондентов из России старше 18 лет, использование социальных сетей является второй, а общение в мессенджерах – третьей по популярности онлайн-активностями среди пользователей)[7]. Социальные сети, мессенджеры, электронная почта – все эти средства позволяют осуществлять мгновенный обмен информацией на расстоянии с сохранением ощущения живого общения и нахождения собеседника поблизости. Современная коммуникация в режиме онлайн предоставляет возможность обмена не только текстовыми сообщениями, но также документами, файлами различного формата (аудио, видео, фото и проч.), что значительно упрощает не только бизнес-процессы (для которых, в силу особого значения скорости обмена информацией

---

[1] См. например: WhatsApp Messenger // Google Play. URL: https://play.google.com/store/apps/details?id=com.whatsapp&hl=ru&gl=US
[2] См. например: TikTok // Google Play. URL: https://play.google.com/store/apps/details?id=com.zhiliaoapp.musically&hl=ru&gl=US
[3] См. например: Тинькофф онлайн банк // Google Play. URL: https://play.google.com/store/apps/details?id=com.idamob.tinkoff.android&hl=ru&gl=US
[4] См. например: SHEIN Модный онлайн шопинг // Google Play. URL: https://play.google.com/store/apps/details?id=com.zzkko&hl=ru&gl=US
[5] См. Штрафы за утечку данных в России // TADVISER. Государство. Бизнес. Технологии. URL: https://www.tadviser.ru/index.php/Статья:Штрафы_за_утечку_данных_в_России
[6] См. В Европе вступил в силу закон о защите персональных данных. Как его выполнить? // D-RUSSIA.RU. URL: https://d-russia.ru/v-evrope-vstupil-v-silu-zakon-o-zashhite-personalnyh-dannyh-kak-ego-vypolnit.html
[7] См. об этом, например: Для чего россияне используют интернет // ИКС Медиа. URL: https://www.iksmedia.ru/news/5871446-Dlya-chego-rossiyane-ispolzuyut-Int.html

для совершения тех или иных операций, подобная возможность имеет особенное значение), но и жизнь любого рядового пользователя. Обмен информацией доступен вне зависимости от часового пояса, региона и даже страны – находящиеся вдали друг от друга люди могут свободно поддерживать общение, даже если не могут часто видеться. Вместе с тем в созданных условиях все большую опасность представляют возможные утечки, и в данном контексте необходимо отметить два аспекта.

Во-первых, стать доступными третьим лицам могут сами передаваемые сообщения. В подобных случаях можно говорить о нарушении права на тайну переписки. Безусловно, подобные нарушения были возможны и во времена «голубиной почты», однако при взломе систем злоумышленники, как правило, получают доступ к переписке (ко всем перепискам) в целом, а не к единственному сообщению. Иными словами, за счет все большей популярности онлайн-инструментов при повседневном общении возрастают риски нарушения неприкосновенности частной жизни, попытаться минимизировать которые можно установкой отдельного пароля для каждого сервиса (что, однако, не гарантирует защиту от взлома) или, например, самостоятельной оценкой, что можно отправить сообщением, а что будет лучше сообщить / передать иным способом.

Во-вторых, в случае использования онлайн-средств общения для целей бизнеса немаловажную роль имеют, возможно, не столько сами сообщения, сколько файлы, обмен которыми осуществляется сотрудниками компании или даже партнерами по бизнесу. В случае принятия решения о возможности использования любого инструмента обмена информацией для передачи документов (особенно конфиденциальных документов) необходимо тщательно ознакомиться с политикой соответствующего сервиса, выяснить, как долго и в каком виде хранятся передаваемые пользователями документы. На основании такой информации, можно если не запретить использование тех или иных средств, то хотя бы иметь представление о том, какие средства являются менее желательными к использованию, а какие – более приоритетными.

Помимо коммуникации Интернет вошёл и в финансовую сферу: появилась возможность не только совершать покупки онлайн (данный аспект будет рассмотрен следующим), но и осуществлять любые платежи с помощью онлайн-банкинга.

С одной стороны, говоря об онлайн-банкинге, следует отметить, что потенциальную опасность утечки представляет не только сама информация о платежах, совершенных пользователям (за счет такой информации становится возможным узнать, каким образом человек тратит средства, как проводит досуг и многое другое), но также данные банковской карты и персональные данные гражданина[8], например: ФИО, паспортные данные, информация об адресе регистрации, контактный номер телефона и адрес электронной почты. Кроме того, возрастает риск доступа третьих лиц к учетной записи клиента банка. В связи с этим в настоящее время следует аккуратнее относиться к предоставляемой возможности «запомнить» карту, устанавливать только официальные банковские приложения и не допускать возможности распространения личной информации сервисами из-за халатного к ней отношения самим пользователем.

---

[8] См. например: Утечки данных из банков России // TADVISER. Государство. Бизнес. Технологии. URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных_из_банков_России

С другой стороны, даже сама возможность осуществления платежа из любой точки, безусловно, является плюсом. Для оплаты коммунальных платежей больше не обязательно каждый месяц ходить в банк и стоять в длинной очереди – достаточно отсканировать прилагаемый к квитанции QR-код, и оплата пройдёт. Для возврата долга или, напротив, предоставления средств взаймы также не нужно встречаться лично, ехать на другой конец города – можно перевести деньги онлайн, а получатель снимет их (если необходимы наличные) в ближайшем к нему банкомате. Вместе с тем в настоящее время нередки случаи мошенничества: злоумышленники получают доступ к используемым средствам онлайн-общения (обычно – социальные сети; реже – мессенджеры) и обращаются к знакомым пользователя с просьбой перечислить определенную сумму по указанным реквизитам. Подобные действия уже ни для кого не новость, но чем дальше, тем более убедительны злоумышленники: они обращаются с «просьбой», предварительно изучив переписку с тем или иным пользователем, в сообщениях используют нужную манеру общения. Иными словами, удобство использования одновременно выступает и в качестве угрозы нарушения информационной приватности.

Помимо изложенного, можно также говорить том, что Интернет сделал доступнее и сферу развлечений, за счет чего стал проще доступ к информации о предпочтениях граждан.

Фильмы, музыка, игры, программы – практически что угодно можно приобрести онлайн и скачать на свое устройство без необходимости приобретения материального носителя. Вместе с тем в погоне за экономией люди нередко прибегают к «помощи» сайтов, распространяющих нелицензионное программное обеспечение или контент, чем рискуют обречь себя на значительные проблемы: вместе с желаемым, например, фильмом (если таковой вообще в итоге будет) на устройстве может появиться вирус, который будет считывать информацию пользователя и передавать ее очередным злоумышленникам.

Помимо большей доступности контента, доступнее стали и услуги: будь то покупка или запись к врачу – практически в каждом случае возможно получить желаемый результат без предварительного живого общения. Что касается покупок, можно и вовсе не общаться с продавцом: достаточно ознакомиться с информацией о товаре, представленной на сайте магазина. Для записи на оказание услуг также уже нередко используются средства онлайн-записи: пользователь выбирает время, указывает свои данные и единственным актом общения для него будет звонок менеджера с целью подтверждения записи (если будет). Однако и здесь возможны неприятные ситуации: фишинговые сайты или зеркала, уязвимости сервера, через который проходит запись, или (что бывает чаще) злоупотребления со стороны самих исполнителей, дополняющих политику конфиденциальности (или иной подобный документ) собственным правом на предоставление данных пользователей третьим лицам – так или иначе данные пользователя могут использоваться в целях, о которых он не был ранее осведомлен, или лицами, с которыми пользователь не взаимодействовал напрямую, его могут одолевать звонками или сообщениями, а для решения данного вопроса понадобится немало сил.

Наконец, многочисленные аккаунты в различных приложениях и на различных сайтах и ресурсах приводят к тому, что при необходимости о пользователе можно составить достаточно полный «портрет» за счет сопоставления баз различных приложений: не только как его зовут и где он живет, но также что он любит, с кем общается, какие места посещает, какие фильмы смотрит, какую музыку предпочитает и многое-многое другое. На основании любого элемента информации пользователю может поступать реклама (чаще таргетированная реклама) продукции или услуг, подходящих (или предположительно подходящих) именно ему. Следует подчеркнуть, речь не идёт о назойливых звонках или рассылках (которые, как правило, не персонифицированы и от которых все же обычно можно отказаться) – в данном контексте мы говорим о рекламных баннерах на сайтах в сети Интернет. Пользователь мог единожды сделать запрос в поисковике, а реклама искомой продукции будет преследовать его везде еще некоторое время после поиска. Более того, по мнению исследователей безопасности Томми Миска (Tommy Mysk) и Талала Хай Бакри (Talal Haj Bakry), несмотря на заявления Apple об обратном, данные аналитики устройств Apple способны напрямую связывать информацию об использовании устройства, его производительности и функциях непосредственно с конкретным пользователем[9].

Подводя итог изложенному, можно отметить, что с появлением и последующим стремительным развитием сети Интернет возникает все больше рисков нарушения информационной приватности пользователей. Персональные и личные данные, собственные фото или видео, история платежей или посещения заведений – все эти цифровые следы оставляет практически каждый, тогда как гарантии незлоупотребления информацией пользователю никто дать не может. В связи с этим лучше отдавать предпочтения проверенным ресурсам и сервисам, знакомиться с политиками конфиденциальности (а не просто ставить галочку у слов «ознакомлен(-а) и согласен(-на)»), если сервис осуществляет сбор персональных данных. Безусловно, полностью обезопасить себя никак не получится, но подобное осторожное поведение позволит хотя бы минимизировать риски утечки пользовательских персональных данных, а сам пользователь будет понимать, какие данные используются сервисами и для каких целей.

Источники:

1. В Европе вступил в силу закон о защите персональных данных. Как его выполнить? // D-RUSSIA.RU. 2018. URL: https://d-russia.ru/v-evrope-vstupil-v-silu-zakon-o-zashhite-personalnyh-dannyh-kak-ego-vypolnit.html
2. Для чего россияне используют интернет // ИКС Медиа. 2022. URL: https://www.iksmedia.ru/news/5871446-Dlya-chego-rossiyane-ispolzuyut-Int.html
3. Приложения // Google Play. URL: https://play.google.com/store/apps/
4. Утечки данных из банков России // TADVISER. Государство. Бизнес. Технологии. 2021. URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных_из_банков_России

[9] См. об этом подробнее Sami Fathi. Apple Device Analytics Contain Identifying iCloud User Data, Claim Security Researchers // MacRumors. URL: https://www.macrumors.com/2022/11/21/apple-device-analytics-identifying-user/?utm_source=ixbtcom

5. Штрафы за утечку данных в России // TADVISER. Государство. Бизнес. Технологии. 2022. URL: https://www.tadviser.ru/index.php/Статья:Штрафы_за_утечку_данных_в_России
6. Sami Fathi. Apple Device Analytics Contain Identifying iCloud User Data, Claim Security Researchers // MacRumors. 2022. URL: https://www.macrumors.com/2022/11/21/apple-device-analytics-identifying-user/?utm_source=ixbtcom