

Verbraucherzentrale Berlin e. V.
Hardenbergplatz 2
10623 Berlin
Тел.: (030) 214 85-224
Факс: (030) 211 72 01
mail@verbraucherzentrale-berlin.de
www.verbraucherzentrale-berlin.de

Результаты семинара «Да — защите данных»

«Мигранты и защита прав потребителей на электронном рынке»

13.06.2014 г.

Второй семинар проекта «Мигранты и защита прав потребителей на электронном рынке» был посвящен теме защиты данных и был проведен 13 июня 2014 г. в помещении Общества защиты прав потребителей. В мероприятии приняли участие 26 человек. Участниками были 13 гостей из Парламента, учреждений федерального правительства и земли. Также мероприятие посетили шесть представителей из русских мигрантских обществ и таких объединений, как Федеральный союз изгнанных, Молодежная миграционная служба (представительство Шёнеберг), Международная конфедерация (представительство Марцан-Хеллерсдорф), Молодежный и семейный центр «Шалаш» и Центр интеграции Вох 66.

Ева Белль, председатель Общества защиты прав потребителей, открыла семинар приветствием, в котором она подчеркнула важность защиты данных мигрантов. Она обратила внимание на новый проект закона, который в будущем предоставит обществам защиты прав потребителей право на подачу жалоб против нарушений защиты данных интернет-компаниями.

В своей приветственной речи Сабина Тёпфер-Катав, заместитель министра защиты прав потребителей, представила результаты потребительского мониторинга в Берлине за 2013 год, который показал огромный дефицит потребительского образования у мигрантов турецкого и русского происхождения. Многие потребители недостаточно информированы о значении защиты данных. Она выразила желание, что при использовании высокоразвитых информационных и коммуникационных технологий потребители должны лучше осознавать важность защиты данных. Предварительная выборка данных пользователей в интернете такими фирмами как Google обеспечивает составление профилей и соответствующую им рекламу. Этими данными интересуются не только компании, но и криминальные структуры. По этой причине на первое место должен быть поставлен вопрос не только защиты данных, но и защиты прав потребителей. Заместитель министра завершила свое приветствие требованием к Европейскому Союзу создать единые и высокие стандарты и правила в отношении защиты данных и информировать об этом людей.

Доктор Гюнтер Хёрман, председатель Общества защиты прав потребителей Гамбурга, описал различные сферы деятельности обществ защиты прав потребителей в течение последних пяти лет, которые постепенно стали соответствовать потребностям потребителей. Хёрман подчеркнул возрастающее значение персональных данных в современном информационном и коммуникационном обществе. Сохранение телефонных и интернет-данных и доступ к ним без ведома пользователей вызывают чувство постоянного контроля частной жизни. Фирмы получают возможность создавать первостепенные и монопольные позиции на рынке благодаря умелой обработке данных и тем самым склонять потребителя к использованию их предложений (в качестве примеров можно привести Google и Facebook). Он указал на решение Европейского суда (И-йю Джи Эйч EuGH) относительно Директивы ЕС о хранении пользовательских данных. И-йю Джи Эйч EuGH в апреле 2014 г. отменил Директиву ЕС о хранении пользовательских данных, так как она нарушала основные права. Хёрман подчеркнул значение защиты данных как неотъемлемого условия не только для защиты демократии, но и для защиты прав потребителей.

Доктор Чичек Бацик, руководитель проекта «Мигранты и защита прав потребителей на электронном рынке», подчеркнула особую роль мигрантов и деятельность Общества защиты прав потребителей Берлина для этой целевой группы. Наряду с консультациями юристов на турецком языке, Общество защиты прав потребителей Берлина в настоящий момент приняло на работу русскоязычного юриста, который также проводит ежемесячные консультации на месте в Марцане и Лихтенберге на русском и немецком языках. Далее Бацик рассказала об обучении в рамках существующего с 2012 года проекта «Обучение кураторов для защиты прав потребителей, направленной на целевую группу».

Бацик подчеркнула, что мигранты согласно потребительскому мониторингу в Берлине за 2013 год представляют собой особенно ранимую потребительскую группу и имеют большую потребность в просвещении в сфере интернета и телекоммуникаций. Большая часть (56 % мигрантов турецкого происхождения и 47 % русскоговорящих) использует интернет для получения информации. Как и большинство немецкого населения, мигранты также используют интернет для покупок и банковских операций. Более трети турецко- и русскоговорящих пользователей, согласно мониторингу, уже сталкивались с проблемами в области электронной торговли и получают в сравнении с немецкими потребителями вдвое большие счета за смартфоны. В связи с этим Бацик подчеркнула особое значение данного проекта. В то время как 85 % немцев согласно потребительскому мониторингу в Берлине за 2013 год осознанно решают, какие (персональные) данные могут использоваться в программах и приложениях, лишь 45 % мигрантов турецкого происхождения и 37 % русскоязычных обращают внимание на защиту своих данных.

Остановившись на целях проекта, Бацик рассказала о различных мероприятиях, запланированных для просвещения турецко- и русскоязычных потребителей в области электронного рынка:

Просвещение целевой группы о правах потребителей, предложениях и консультациях на электронном рынке, исследование ситуации на рынке телекоммуникаций с помощью контроля и семинаров, разработка информации в области телекоммуникаций и интернета, учет жалоб целевой группы и передача информации для грамотного обращения с телекоммуникационными услугами, интернетом и защитой данных. В двух запланированных исследованиях рынка в фокусе находились телефонные тарифы в Турцию и тарифы в Российскую Федерацию, причем в центре внимания находилось исследование и оценка стоимости, услуг и методов ведения дел операторов телефонной сети. Центральным звеном проекта стала последующая обработка информации на темы электронного рынка для целевых групп. Бацкич упомянула, что информация для целевых групп будет предоставляться на немецком языке, а также в виде кратких изложений/информационных стендов на турецком и/или русском языках. В заключение она проинформировала о результате стартового семинара.

Кристиан Далер, специалист по информатике службы Берлинского уполномоченного органа по защите данных и информационной безопасности рассказал об основах безопасного использования беспроводных локальных сетей и смартфонов и просветил участников касательно информационных «следах» пользователей в интернете. Прежде всего, Далер объяснил, почему важно всегда использовать закодированные беспроводные сети при интернет-серфинге. Так как общественные учреждения, кафе или магазины не всегда предлагают закодированное соединение с интернетом, таких соединений нужно избегать. В частности, при незакодированных интернет-соединениях нужно избегать услуг электронной торговли. Исключениями являются безопасные соединения VPN (виртуальная частная сеть) и IPsec (безопасный протокол IP). По возможности лучше использовать соединения WPA и WPA2 (Wi-Fi Protected Access) благодаря их безопасности. Подключение к сети WPS (Wi-Fi Protected Setup) довольно удобно, но частично небезопасно: После включения компьютера, когда в течение 1–2 минут устанавливается автоматическое интернет-соединение, PIN-коды могут быть перехвачены.

Дальнейшим условием для безопасного серфинга в интернете является использование трудно угадываемых и по возможности не настроенных предварительно паролей для сетей Wireless LAN, которые при необходимости можно конфигурировать и управлять ими с помощью специального программного обеспечения. Деактивация удаленной конфигурации роутера после подключения к сети также способствует защищенной передаче данных.

В заключение Далер разъяснил некоторые настройки безопасности для смартфонов, такие как использование пароля во избежание несанкционированного доступа к аппарату и сохраненным на нем данным, контроль при загрузке и использовании бесплатных приложений и контроль при подтверждении доступа к собственным данным. Кроме того, необходимо осторожнее обращаться с функцией определения местонахождения некоторых приложений, так как для пользователей могут создаваться также профили передвижения. Перед использованием незнакомых приложений важно разыскать информацию о них. В настоящее время проверенные приложения в фирменных магазинах являются более безопасными. В частности, приложения для Android часто не проверяются. С помощью загруженных приложений можно получить доступ к личным данным пользователей. Зачастую неясно, кто получает данные пользователей, и как они используются. Например, полученные в играх данные могут использоваться в рекламных целях, поэтому при игре лучше отключать Wireless LAN.

Во второй части своего доклада Далер разъяснил, какие данные пользователей передаются при запросе интернет-сайтов. На основе переданных данных о типе браузера, настройках экрана, операционной системе, информации о разрешении экрана и глубине цвета можно, к примеру, определить, через какое устройство происходит обращение к данному вебсайту. О зависимости продажных цен от устройства средства массовой информации уже сообщали в связи с устройствами фирмы Apple.

Еще одна возможность использовать вебсайты для персонализации и распознавания данных связана с файлами Cookie. Файлы Cookie — это небольшие текстовые файлы с информацией о посещаемых вебсайтах, которые через эти вебсайты сбрасываются на компьютер пользователя, чтобы потом получить возможность его идентифицировать. Позже с помощью так называемых отслеживаемых файлов Cookie со стороны поисковых машин может отслеживаться история отдельных пользователей и перепродаваться партнерским вебсайтам для разработки направленных предложений. Кроме того, онлайн-магазинами сохраняются прежние заказы и просмотренные продукты пользователя, чтобы целенаправленно предлагать ему дополнительные подходящие товары. Такого рода доступ к данным можно минимизировать с помощью отключения некоторых функций браузеров, таких как Flash и JavaScript, а также Add-Ons (небольшие расширения браузера), таких как NoScript и AddBlock-Plus. Далер подчеркнул повышенную безопасность при серфинге в режиме инкогнито и продемонстрировал эту настройку в браузере.

Кроме того, Далер проинформировал о праве на информационное правовое определение согласно §§ 33–35 Федерального закона о защите данных (BDSG), в рамках которого пользователи могут требовать информацию как о сохраненных данных, так и об исправлении, блокировке и удалении данных. В заключение он сообщил о так называемых списках робинзонов (www.robinsonliste.de), предлагающих защиту от нежелательных рекламных рассылок и телефонных звонков.

Доктор Кей Иши и Полина Роггендорф из проекта «Безопасность потребителей в интернете», Технический университет Берлина, проинформировали участников о безопасном серфинге в интернете. На примере трехмерной конструкции русскоязычного новостного вебсайта Роггендорф и Иши продемонстрировали невидимые хитрости интернета. Они упомянули, что многие процессы в интернете происходят автоматически и невидимо для пользователей. Цель невидимого интернета — сбор данных. Но все же есть программы, помогающие выяснить, какие фирмы отслеживают историю пользователей. На примере программы Ghostery Иши показал, как много и какие фирмы наблюдают за посещением открытого ими вебсайта. Это означает, что многие фирмы имеют доступ к данным пользователей и используют их в работе с файлами Cookie в рекламных целях. Число таких действующих невидимо вебсайтов при среднестатистическом серфинге может достигать 100. Настоящая опасность сбора данных состоит не в рекламе, а в нежелательном сохранении данных. Тенденция объединения информации, собранной из различных источников, непрерывно растет. Статистический учет и интерпретация собранных данных, например, проводится компанией Piwik-Analytics¹.

¹ Piwik-Analytics является альтернативой Google Analytics. Программа Open-Source служит для сбора и анализа данных посетителей вебсайтов. (Источник: <http://www.piwik-analytics.com/>)
Далее Иши объяснил, что владельцы сами решают, какие данные могут собирать

специализированные фирмы на их вебсайтах. С помощью поисковых запросов, обращений к вебсайтам и т.д. Google, например, узнает специфическую информацию о пользователях, которая за доли секунды через процесс cookie-matching, то есть сопоставление файлов Cookie, используется для анализа серфинга, и в форме аукционов Google продается рекламным фирмам. В заключение Иши дал важные советы для защиты данных при серфинге в интернете: Защита компьютера с помощью актуализации антивирусных программ, а также использование надежных паролей. Для защиты данных очень важны соответствующие настройки и функции браузера, так как, например, удаление журнала браузера и файлов Cookie, а также использование расширений браузера, например, Ghostery. Дальнейшие советы для защиты компьютера и персональных данных пользователи найдут в проектах «Безопасность потребителей в интернете» (<https://www.verbraucher-sicher-online.de/>) и «Пользователи интернета имеют права» (<https://www.surfer-haben-rechte.de/>). Кроме того, пользователи должны обращаться со своими данными как можно бережней и не передавать данные.

В открытой дискуссии принимали участие Доктор Кей Иши и Кристиан Далер. Модератором дискуссии был Юнал Зеран, руководитель проекта из Гамбурга. Доктор Тургут Алту, представитель организации по защите природы и защите прав потребителей, Союз90/Зеленые Парламента Берлина, высказался за то, что такие образовательные мероприятия должны проводиться на местах в мигрантских организациях, чтобы эта информация преподносилась также этой целевой группе. Хайке Ансорена, референт экономической защиты прав потребителей, Ведомство по вопросам юстиции и защиты прав потребителей, задала вопрос относительно «Права быть забытым» (решение Судебной палаты Европейского союза), почему Google при заявке на удаление персональных данных требует копию удостоверения личности. Далер ответил, что хотя требование копии удостоверения личности с точки зрения закона необязательно, так же как и при заключении договоров на подключение мобильного телефона, в реальности эти предпосылки не соблюдаются. Google и другие фирмы тем самым хотят идентифицировать заявителя по его удостоверению личности. Кроме того, удаление данных в Google не означает полного удаления из всемирной паутины.

Заключение

Недостаточное осознание мигрантами вопросов защиты данных, которое обнаружилась уже в ходе потребительского мониторинга в Берлине за 2013 г., было подтверждено как на стартовом семинаре проекта 14 марта 2014 г., так и на этом втором семинаре. Отзывы участников показали, как важны конкретные рекомендации по защите собственных данных и настройкам безопасности компьютера. Просвещение мигрантов по защите данных и усиление их компетентности в области медиа играют важную роль. Так как интернет в повседневной жизни мигрантов является неотъемлемым средством, а они все сильнее сталкиваются в сети с ловушками, специфическими для их целевой группы, Общество защиты прав потребителей Берлина планирует издать информационные бюллетени о защите данных для русско- и турецкоязычных мигрантов в сотрудничестве с Берлинским уполномоченным по защите данных. В этом потребительском бюллетене должны быть перечислены важные советы по защите данных. Целевая группа, кроме этого, должна быть проинформирована, почему важны настройки безопасности компьютера и смартфонов и почему рекомендована сдержанность при указании персональных данных в социальных сетях и в системах электронной торговли. Эта информация должна быть представлена также на интернет-странице Общества защиты прав потребителей.

Интерактивный форум, запланированный на ноябрь, должен, по меньшей мере, поднять вопрос защиты данных.

Отзывы участников о семинаре

«Спасибо за отличное мероприятие!»

«Хотел бы поблагодарить за приглашение на семинар по защите данных. Было очень познавательно!»

«Спасибо за приглашение! Я как можно скорее выполню настройки безопасности на моем компьютере!»