Лекция 17

ҚАЗАҚСТАННЫҢ АШЫҚ УНИВЕРСИТЕТІ

ПСИХОЛОГИЯ ИНТЕРНЕТА

Конфиденциальность в интернете

В настоящее время интернет, который является протоколом для соединения устройств по общедоступным линиям связи, является самой глобальной угрозой конфиденциальности частной жизни, с которой когда-либо сталкивалось человечество.

Интернет, конечно, существенно облегчает обмен информацией, однако передаваемая информация, системы связи, по которым она передается, ежесекундно подвергаются риску взлома, кражи данных или другого ущерба. Поскольку интернет является общедоступной сетью, любой пользователь имеет возможность использовать его для любой цели, и, к сожалению, часто злоумышленники и мошенники активно этим пользуются.

Люди охотно отдают конфиденциальную информацию в интернете не только о себе, но и о других людях. Физическое расстояние, а также повышенное восприятие анонимности во многих интернет-сайтах способствуют развитию поведения, которое заставляет думать, что мы больше не заботимся о конфиденциальности в онлайне.

В 2007 году, например, социальная сеть Facebook запустила то, что пользователи назвали «жутким» сервисом, который отслеживал их действия на сторонних сайтах, а затем передавал информацию своим друзьям. Facebook отказался от этой практики, но затем, в 2010 году, компания решила настроить параметры конфиденциальности пользователей по умолчанию «все», что означает, что каждый может просматривать сайт пользователя, а не просто «друзей». Facebook продолжает вызывать возмущение и судебные процессы в отношении конфиденциальности личной информации.

Тем не менее люди продолжают отправлять сообщения. И они поддерживают «дружественных» людей, о которых мало что знают. Студент Университета штата Миссури сделал эксперимент, который показал, как люди готовы добавлять «друзей». Он написал компьютерную программу, которая генерировала запросы, чтобы добавить его в качестве друга, и отправил его 250 000 людям. Почти треть из них согласилась с просьбой, хотя они и понятия не имели, кто он такой. Многие пользователи Facebook обнаружили, что это эксперимент, и они отправили ему ненавистные и непристойные сообщения. Однако результаты эксперимента иллюстрируют, как многие люди могут раздувать список своих «друзей».

Парадокс конфиденциальности заключается в том, что люди говорят, что они обеспокоены данной проблемой; в то же время у них нет знаний о том, как настроить параметры своей конфиденциальности. Люди раскрывают подробную личную информацию большому количеству других людей. Действительно, «совместное использование» является ключевым компонентом Web 2.0, а разработка программных средств для его облегчения – большой бизнес.

В одном из исследований, например, среди опрошенных студентов колледжей, выяснилось, что только около половины сказали, что они ограничили свой профиль, чтобы «только друзья» могли видеть детали, которые часто включают в себя личную и конфиденциальную информацию. На первый взгляд, это выглядит умным шагом. Но подумайте, сколько пользователей Facebook добавили «друзей» в свою сеть, о которых они мало что знают. Что продемонстрировал эксперимент в университете Миссури.

Что объясняет этот парадокс? Одна из возможностей заключается в том, что люди действительно не знают, как управлять своей конфиденциальностью в интернете, хотя большинство заявляет, что у них есть хотя бы некоторые знания. Настройки конфиденциальности становятся все более сложными, и компании постоянно меняют политику. Сама политика утомительна для чтения, ее трудно интерпретировать и тем более применять.

Фактически, одно исследование подтвердило, что люди считают, что другие более уязвимы к рискам конфиденциальности, чем они сами. Опрос национальной выборки в Корее содержал два ключевых вопроса. Одним из них был такой: «Насколько вероятно, что вы стали жертвой неправильного использования личной онлайн-информации?» В целом, люди более оптимистично относились к своим собственным рискам по сравнению с рисками, которые, по их мнению, принимали другие, особенно если другие были подростками.

Третья возможность объяснить парадокс заключается в том, что социальная сеть представляет собой особенно опасную онлайн-среду для обеспечения конфиденциальности, как психологически, так и технологически. Люди воображают, что они ограничены аудиторией, которую они пригласили, то есть их «друзьями». Они могут раскрывать общие факты о себе, но считают свою страничку в социальной сети частным кругом и чувствуют себя свободнее, чтобы

делиться более конфиденциальной информацией. Это имеет основополагающее значение для развития и поддержания отношений. Но по мере роста сети человека растет риск нарушения конфиденциальности.

Конфиденциальность является важным элементом открытого информационного пространства интернета. Пренебрежение правом человека на конфиденциальность, а точнее, его правом контроля за составом и степенью распространения персональной информации, приводит к потере пользовательского доверия, усилению контроля и как следствие к уменьшению инновативности, интенсивности и объема информационного обмена.

Поэтому очень важно поддерживать этот сложный баланс между конфиденциальностью и открытостью, удобством пользования и утечкой частной информации. В какой-то степени об этом могут позаботиться сами пользователи через установки браузера или социальной сети. Например, блокирование заголовка Referer в запросе или запрет приема cookie от сайтов третьих сторон. Однако эти меры часто малоэффективны. Допустим, отказаться от использования cookie посещаемого сайта сегодня практически невозможно без существенной потери функциональности.

Существенный вклад в решение этой проблемы могут внести создатели самих сайтов и социальных сетей. Например, минимизируя количество информации, передаваемой третьим сторонам, или информируя пользователей о степени открытости их данных в социальной сети. И делать это, не дожидаясь судебного процесса, как это произошло с услугой Facebook под названием Beacon, на которую были автоматически подписаны все пользователя сети в ноябре 2007 года.

Благодаря Beacon друзья пользователей получали оповещения о деятельности последних на некоторый других сайтах, например, о покупке билетов в кино на сайте Fandango (http://www.fandango.com). Дело закончилось двумя годами спустя полным прекращением услуги и созданием Facebook-фонда для работ в области онлайн-конфиденциальности стоимостью 9,5 миллионов долларов.

Знание и открытое обсуждение этих проблем – уже шаг к их решению. И проблемы действительно решаются: пользователи получают больший контроль в социальных сетях, браузеры заботятся о нашей безопасности и конфиденциальности. Потому что несмотря ни на что, люди хотят обмениваться информацией со своими друзьями, знакомыми, а иногда и со всем миром.

Десятилетие лет назад совершение онлайн-платежа считалось делом рискованным и делалось с большой осторожностью. Использование реальных имен в социальном общении в сети было немыслимо, а анонимность деятельности в интернете считалась почти абсолютной.

Социальные сети радикально изменили ситуацию. В них мы хотим общаться не с незнакомцами или виртуальными персонажами, а с людьми, которых мы знаем или хотим познакомиться. Это предполагает, что наш образ в сети достаточно правдив. Мы обмениваемся со своими друзьями, знакомыми, а зачастую и со всем миром, вполне правдивой информацией о своем возрасте, интересах, местонахождении, текущих заботах, да практически обо всем!

Например, недавно я прочитал в газете о сайте Blippy, позволяющем обмениваться информацией о сделанный покупках. Некий Марк оповещает весь мир о том, что он приобрел кейс для iPad за $ 41, потратил $ 24 в ресторане X и $ 6450 в клинике пластической хирургии во Флориде на операцию носа. Уникальный случай? Похоже, что нет. Сайты и стоящие за ними социальные сети для обмена самой разнообразной каждодневной информацией растут, как грибы после дождя, и пользуются огромной популярностью.

На первый взгляд, публикация в интернете пусть даже персональной, но довольно безобидной информации, например, о любимых занятиях, собственной фотографии или номера школы, которую вы закончили, не представляет опасности. Однако сайт PleaseRobMe.com наглядно показал, как информация из социальных сетей может быть использована совсем не в безобидных целях. Этот сайт использовал доступную в сетях информацию для обнаружения пустующих квартир, хозяева которых проводили время вдали от дома.

Другим аспектом является то, что область распространения вашей личной информации может оказаться гораздо больше, чем вы думаете. Она зачастую не ограничена узким кругом друзей и знакомых, и, более того, почти всегда выходит за рамки вашей социальной сети. Это, в свою очередь, может существенно ограничить ваши возможности оставаться анонимным в случаях, когда вы этого хотите.

В 1993 году в одном журнале была опубликована карикатура, изображающая двух собак, сидящих перед дисплеем компьютера, одна из которых говорит другой: «В интернете никто не знает, что ты собака». Сегодняшняя реальность существенно отличается от этой картины.

Давайте рассмотрим эту проблему более подробно. Начнем с вопроса, насколько конфиденциально пользование интернетом вообще? На первый взгляд, использование интернета весьма анонимно. Конечно, веб-сайт, который вы посетили, знает IP-адрес вашего компьютера, но что из того? Отдельный сайт и обезличенный адрес. Вроде бы нет повода для беспокойства.

Однако многие, если не большинство посещаемых веб-сайтов используют те или иные технологии для отслеживания посетителей. Даже если это и не портал с пользовательским именем и паролем, всякий раз, когда вы заходите на сайт (а сегодня это почти синоним работы в интернете), происходит «утечка» частной информации о посетителе сайта, то есть о вас. Например, популярными технологиями являются встроенные «жучки» в виде изображений в 1 пиксель, cookies или приложения JavaScript.

Утечка частной информации также происходит не только на самом веб-сайте, который вы посетили, но также и на сайтах третьих сторон. Эти сайты часто, хотя и неочевидно, присутствуют на просматриваемой веб-странице, например, в виде рекламных фрагментов. Типичным сценарием является размещение рекламных объявлений рекламными провайдерами, например Google's Adsense, Yahoo!, по договоренности с владельцем сайта. Обычно эти фрагменты существуют в виде компонентов JavaScript или просто графической картинки. Отображение страницы современного информационного веб-сайта включает десяток обращений за различными элементами, в том числе и к сайтам третьих сторон. Стоит отметить, что это происходит независимо, кликнул ли пользователь на баннер или нет.

В январе 2014 года в журнале Forbes кибержурналист Джозеф Стейнберг опубликовал список связанных с интернетом приборов, которые «шпионят» за нами буквально в наших домах. Это интернет вещей.

Интернет вещей (англ. Internet of Things, IoT) – концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой. Она рассматривает организацию таких сетей, как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Интернет вещей находится только в начале своего пути, но уже развивается с огромной скоростью, и все вводимые новшества добавляют серьёзные проблемы, связанные с информационной безопасностью. Новостной веб-сайт Business Insider опубликовал в 2013 году исследование, которое показало, что сомнение в безопасности является для опрошенных наибольшей проблемой при внедрении технологий интернета вещей. В их числе телевизоры, кухонная техника, камеры. Очень ненадёжна компьютерная система автомобилей, которая контролирует тормоза, двигатель, замки, капот, вентиляцию и приборную панель; эти части системы наиболее уязвимы для злоумышленников при попытках получения доступа к бортовой сети. Также атака может быть произведена удалённо по интернету. Хакерами была продемонстрирована возможность дистанционного управления электрокардиостимуляторами. Позднее они научились получать доступ к инсулиновым помпам и имплантируемым кардиодефибрилляторам.

Компания Hewlett Packard провела масштабное исследование в 2015 году, в котором сообщается, что 70% устройств IoT имеют уязвимости в безопасности своих паролей, существуют проблемы с шифрованием данных и с разрешением доступа, и 50 % приложений для мобильных устройств не обмениваются данными.

Лаборатория Касперского – компания, специализирующаяся на производстве программного обеспечения для защиты информации, провела испытания на объектах, подключенных к интернету вещей, и обнаружила, что видеоняни могут быть взломаны для перехвата видео, и кофемашины, которые передают информацию в незашифрованном виде, могут сохранять пароль сети WiFi, к которой были подсоединены.

Безопасность интернета вещей стала одним из важнейших аспектов новых технологий. Возможно, покажется, что не существует риска для данных, которые передаются и хранятся такими системами, они не являются уязвимыми, но реальность такова, что устройства,

которые не имеют должной защиты, подвергаются атакам, будучи заведомо заражёнными вредоносным кодом для создания ботнета.

Как же сохранить собственную интернет-конфиденциальность и обезопасить себя в интернете? VPN может решить многие вопросы кибербезопасности и максимизировать интернет-конфиденциальность как компаний, так и частных лиц.

Используя VPN, вы подключаетесь к защищенной сети, имеете свободный доступ к нужным вам веб-сайтам или социальным сетям. Неважно, почему вы до сих пор не использовали возможности VPN для обеспечения собственной безопасности, важно, что вы это можете сделать прямо сейчас. Услуги VPN стали финансово доступными любому пользователю сети, что гарантирует высокий уровень индивидуальной кибербезопасности и конфиденциальности. Подписка на VPN обычно обходится пользователю всего в несколько долларов в месяц, она обеспечивают неограниченный доступ к интернету, конфиденциальность и защиту всех интернет-подключений, предотвращает утрату личных данных вашей семьи.

Возможности обмена информацией в интернете сегодня поистине безграничны и продолжают стремительно развиваться. Социальные сети создали невиданную доселе степень информационной связности между людьми в глобальном масштабе. Интернет превратился в динамичную социальную среду, объединяющую сотни тысяч миллионов людей. Как сказал основатель Facebook Марк Цукерберг, миссией компании является сделать мир более открытым и связанным.