Мария Макушева — о трансформации открытости для НЕЗЫГАРЬ

В дискуссиях профессионалов в сфере цифровой безопасности можно отметить две линии — «меньше прозрачности» и «меньше анонимности». Они определяют контуры цифрового мира, в котором нам предстоит жить в ближайшем будущем.

Сегодня часто проблематизируется безграмотность пользователя различных сервисов, с одной стороны, и доступность пассивного следа — со смартфонов, телевизоров, умной техники — с другой. Корпорации собирают слишком много данных, значительно больше, чем государство. И это само по себе может вызывать тревоги (особенно, если корпорации иностранные).

Но важно также, что данные могут быть скомпрометированы. Вот один из множества вопросов из практики специалистов: каким образом человек, не прописанный в районе, был добавлен в районный чат, где впоследствии распространялись материалы в поддержку кандидата на выборах? (Ответ — через утечку данных сервиса по заказу продуктов).

Доверие к корпорациям подорвано случаями утечек данных и скандалами с кражей средств с личных счетов. Никто не может гарантировать, что инфраструктура компаний достаточно защищена. В качестве защиты здесь предлагается собирать, хранить, распространять меньше. А также ограничивать использование иностранных сервисов, например, Google-аналитики, на государственных сайтах.

С другой стороны, информационная безопасность для государства и корпораций — одна из сфер, которая интенсивно растет под лозунгом «больше прозрачности и контроля».

«Средства защиты данных выходят на новый уровень, внедряются

технологии на основе искусственного интеллекта, которые перемалывают огромные массивы данных, а человек принимает ключевые решения. Появляется синергия от взаимодействия машины и человека, которая меняет не только процессы по защите данных, но и поведение самого офицера безопасности», — утверждает Александр Клевцов, руководитель по развитию продукта компании InfoWatch.

Последние годы отмечены интенсивной цифровой трансформацией преступности. Число киберпреступлений поступательно растет (кроме последнего года). Более 90% из них — это социальная инженерия, введение в заблуждение человека человеком. Но увеличивается и число не зависящих от пользователей утечек данных. И цифровой след — это помощник в раскрытии киберпреступлений. Увеличение сбора данных, хранения, усложнение алгоритмов обработки — средства борьбы. А средства анонимизации — угроза. Государство требует, чтобы в ключевых сферах не было закрытости.

Также и корпорации все больше озабочены охраной цифрового контура от угроз извне и изнутри. Служба безопасности хочет знать, если значимые данные копируются или пересылаются, если сотрудник в корпоративной переписке ведет себя деструктивно по отношению к коллегам и компании, если сотрудник использует корпоративные ресурсы для личных целей. Поэтому уже сейчас человек оказывается на рабочем месте под пристальным наблюдением, и это тенденция будет расти.

На сегодня же открытость для различных потребительских сервисов значительно выше, чем для государства и для работодателя. И эту ситуацию явно хотят перевернуть. Намечается два ключевых тренда: снижение прозрачности для «чужих» и повышение — для «своих».

Однако последнее вызывает немало тревог у граждан/сотрудников. Пользователь легко делится данными с сервисами, потому как не видит риска и ответственности. В случае государства или работодателя на основе данных принимаются административные

решения. Ощущение контроля, даже «слежки» здесь более персонифицированное, последствия более понятны на бытовом уровне. Вокруг сбора данных много негативных стереотипов. Поэтому в этой сфере будут крайне важны исследования и поиск новых подходов к коммуникациям, способов говорить с человеком о безопасности так, чтобы он не чувствовал себя беззащитным объектом наблюдения.

НЕЗЫГАРЬ