Штрафы не помогут, нужно закрывать сервисы для «пробивки»: доцент МАИ Пётр Ухов — о наказании за утечки персональных данных

24 сентября 2024

Фото: Пресс-служба МАИ / Личный архив

Депутаты Госдумы выступили с инициативой существенного увеличения штрафов за утечки персональных данных и уголовного наказания за неправомерное использование конфиденциальной информации о гражданах России. Предполагается, что санкции могут накладываться на любую организацию и ответственных лиц, которые нарушат закон. Но есть нюанс.

Несмотря на ранее введённую ответственность за сливы личных данных, процесс не прекращается. Более того — число мошеннических схем и взломов растёт, а уровень безопасности снижается. С чем это может быть связано? Есть ли верный способ обезопасить себя и близких? Своим мнением поделился замначальника управления «IT-Центр» МАИ, кандидат технических наук, доцент Пётр Ухов.

Пётр Александрович, ситуация с обеспечением конфиденциальности оставляет желать лучшего. Как вы считаете, мы сами виноваты в том, что везде оставляем «следы»?

На самом деле это очень интересный вопрос. Персональные данные — это любая информация, которая позволяет идентифицировать вас как конкретного субъекта. Как бы вы не старались сохранить её сегодня, что-то всё равно окажется в общем доступе. Мы привыкли пользоваться социальными сетями, маркетплейсами, которые значительно облегчают нам жизнь, всевозможными услугами, запись на которые осуществляется через

сеть — везде так или иначе мы оставляем свои данные. Даже если речь идёт только о фамилии, имени и отчестве, телефоне или адресе электронной почты. В некоторых случаях этого уже достаточно, чтобы узнать о вас если не всё, то очень многое.

Отвечая на ваш вопрос более обстоятельно, отмечу, что человек в этой ситуации — сам источник своих проблем. Если вы решились где-нибудь оставить не только свои ФИО, но и паспортные данные, значит, это потенциально может привести к проблемам. На вас могут оформить кредит или микрозайм. Цифровой мир слишком быстро приучил нас к хорошему: в обмен на персональные данные мы получаем комфортный сервис и прочие удобства, от которых вряд ли сможем отказаться.

Это проблема глобального масштаба? В России, за рубежом — ситуация с обеспечением безопасности одинакова?

Да. Везде происходит одно и то же. А всё потому, что принципы хранения информации везде плюс-минус одинаковы. Наши персональные данные сохраняются в базах данных, часто на облачных сервисах. Хорошо, если в зашифрованном виде и с соблюдением требований кибербезопасности, но, к сожалению это не всегда так. В большей степени это определяется культурой безопасной разработки владельца такого сервиса и политиками безопасности при обмене данными внутри микросервисной архитектуры — именно так сейчас строятся многие системы, приложения и сервисы.

Кто и как может украсть персональные данные и любую другую засекреченную информацию? Это командная работа или заинтересованный человек запросто справится в одиночку?

Чтобы украсть данные, иногда достаточно просто хорошо разбираться в программировании, веб-сервисах и системах на базе Linux. Кроме этого, часто маленькие организации и физические лица хранят важные документы в тех же Google-таблицах или «Яндекс»-документах. Данные сервисы предоставляют возможность персонального доступа, но многие из-за удобства просто открывают документы «по ссылке». В этом случае всё может быть просмотрено и украдено.

Мы должны понимать, что вне зависимости от введения или невведения штрафов утечки были, есть и будут. Потому что во всех системах хранения информации есть уязвимости — их просто нужно вовремя устранять. В целом это борьба ресурсов: чем больше вы вложите во взлом системы, тем больше вероятность, что вы её взломаете; чем больше вы вложите в защиту, тем надёжнее она будет. Но и в одном, и в другом случае 100-процентных гарантий не существует.

Если бороться со сливами при помощи штрафов не получится, то что нам тогда поможет защитить себя?

Я правда не уверен, что повышение штрафов хоть как-то поможет повысить уровень защиты. Речь ведь о том, что некоторые организации и физические лица просто не понимают, что такое безопасная разработка или цифровая гигиена и почему эти принципы важно соблюдать.

По моему личному мнению, в первую очередь нужно бороться с рынком сбыта персональных данных и прочей важной, конфиденциальной и тем более секретной информации. Если вы устраняете того, кто платит деньги за покупку персональных данных, устраняете посредника, которому можно заплатить, то «пищевая цепочка» просто прекращает своё существование.

Со штрафами же, по моему мнению, скорее будет обратный эффект. Утечки будут пытаться скрывать всеми силами, только чтобы не попасть под санкции: вымогателям будут платить ещё больше денег за нераскрытие украденной конфиденциальной информации, сложится ситуация, при которой пострадавшая сторона будет вынуждена вести переговоры с цифровыми преступниками, а не обращаться в компетентные органы.

Если вы думаете, что рынки сбыта находятся где-то очень далеко в секретных хакерских сетях, то вы ошибаетесь. Самая обычная «прогулка по ботам» в Telegram может закончиться хорошим уловом — большим досье на интересующего вас человека. Кстати, для этого иногда достаточно знать только ник или номер телефона субъекта.

А если мы «попросим помощи» у искусственного интеллекта, он нам поможет?

ИИ — это просто инструмент в руках специалиста или мошенника. Он целевым образом способен помочь специалисту по безопасности обнаружить незащищённые места в системе, потенциально опасные источники запросов, сомнительные учётные записи, узлы, которые могут быть скомпрометированы. Фактически всё это ИИ делает уже сейчас, но говорить о полном переложении ответственности за обеспечение безопасности на искусственный интеллект не приходится. Нет такого «сильного ИИ», который бы смог перестроить всю систему безопасности и навсегда избавить нас от цифровых террористов.

Кстати, ИИ активно эксплуатируется и мошенниками при взломе систем методами социальной инженерии. Можно подделать голос собеседника или даже сделать видеозапись и многое другое. Например, недавно всем сотрудниками МАИ писали в Telegram от имени нашего ректора или руководителей подразделений и просили выполнять различные действия — скинуть пароль от личного кабинета, отправить фото паспорта и т.д. Поэтому не стоит вести разговоров по телефону или в мессенджерах при подобном запросе, лучше сразу перезвоните коллегам или вашему руководителю — в 99,99% случаев это мошенничество.

Получается, единственный способ остаться в безопасности — минимизировать число адресатов, куда мы направляем свои данные?

Да. Говоря иначе: нам всем следует просто очень тщательно соблюдать цифровую гигиену. А выражается она вот в чём.

Во-первых, не нужно везде вбивать свои платёжные карты. И откажитесь от автоплатежей. Для надёжности используйте разовые платёжные виртуальные карты (многие банки предоставляют такую услугу): открыли их, провели транзакцию и заблокировали.

Во-вторых, тщательно проверяйте, кому отправляете свои паспортные данные. Никогда не делайте это через почту, если есть возможность. Кроме того, старайтесь лишний раз не давать снимать копии с паспорта и других документов — неизвестно, где и как они потом будут использоваться.

В-третьих, тщательно анализируйте контент, который выкладываете в сеть. Так, даже банальное фото в квартире у окна, рядом с частным домом или в какой бы то ни было другой локации поможет быстро вычислить ваше местонахождение. Про адрес проживания, думаю, говорить вообще не следует.

В-четвёртых, конечно, не стоит забывать об опасности использования VPN. Помните: бесплатные сервисы практически всегда воруют у вас информацию. Когда вам что-то предоставляют бесплатно, помните, что вы — «товар». Если вы не отключаете VPN при введении паролей, входе в банковские приложения и при проведении каких-либо финансовых операций даже в браузере, будьте готовы к тому, что скоро можете лишиться денег или какой-то важной информации, которая ранее была защищена. Помните: любой VPN — это кот в мешке. Если оператор захочет получить ваши данные, то он их обязательно получит.

Материал подготовлен при поддержке Минобрнауки России