РОЦИТ

СЕРИЯ УЧЕБНЫХ ПОСОБИЙ ПО ЦИФРОВОЙ ГРАМОТНОСТИ

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

цифровой диктант.рф

ПРИ ПОДДЕРЖКЕ

ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Проект реализован с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

СЕРИЯ УЧЕБНЫХ ПОСОБИЙ ПО ЦИФРОВОЙ ГРАМОТНОСТИ

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Огромная доля информации, размещенной в интернете, подпадает под определение «персональные данные». И, наверное, сейчас только ленивый не слышал, что «персональные данные» — это очень важно для жизни и для безопасности. Однако главный вопрос, исходящий из этого, все еще стоит на повестке дня: как именно мы можем контролировать свои персональные данные, чтобы наконец ощутить себя в этой самой безопасности?

КАКИЕ ДАННЫЕ СЧИТАЮТСЯ ПЕРСОНАЛЬНЫМИ?

Для начала надо разобраться в том, какая информация относится к персональным данным пользователя. «Персональные данные» — это прямая транслитерация английского термина personal data, что также значит **«данные о личности»**, **«информация о персоне»**. В связи с этим сразу возникает вопрос: что именно считается «информацией о личности»? Только анкетные данные или что-то еще? Долгое время и в России, и на Западе персональными данными считали исключительно анкетные данные, и под это понимание писали законы и директивы, например, старый Модельный закон СНГ «О персональных данных». Но с возросшим числом скандалов вокруг вмешательства в личную жизнь, это определение пересмотрели, причем весьма радикально.

В настоящее время в России действуют нормы Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — закон о персональных данных).

В соответствии с указанным законом персональными данными считается любая информация, на основе которой можно прямо или косвенно определить конкретное физическое лицо.

GDPR: ОБЩИЙ РЕГЛАМЕНТ О ЗАЩИТЕ ДАННЫХ

На международной арене также остро стоит проблема незащищенности персональных данных, поскольку во всемирной сети хранится множество информации, имеющей прямое отношение к указанной категории. Так,

например, в мае 2018 г. в Евросоюзе вступил в силу Общий регламент о защите данных (General Data Protection Regulation, GDPR), описывающий правила защиты данных для граждан ЕС. Согласно GDPR физические лица вне зависимости от гражданства имеют право на защиту своих персональных данных, находясь на территории любой из стран Евросоюза

НОРМЫ GDPR ПРИМЕНИМЫ В 3-Х СЛУЧАЯХ:

1

Если компания осуществляет свою деятельность на территории стран, входящих в состав Евросоюза, посредством филиала, аффилированной компании, компании-партнера, привлеченного агента или представителя, и благодаря их деятельности получает и обрабатывает персональные данные.

2

Если компания продает товары или оказывает услуги физическим лицам, находящимся на территории ЕС, и в рамках этой деятельности получает и обрабатывает персональные данные.

3

Если компания отслеживает активность или поведение физических лиц, находящихся на территории ЕС на момент мониторинга. К отслеживаемым данным можно отнести, например, использование cookie-файлов, сбор данных геолокации, видеонаблюдение, регулярный контроль данных о здоровье

В эпоху интернета это право особенно актуально. Информация в интернете легко копируется и распространяется на различных площадках, в результате чего контролировать ее становится очень сложно. Дополнительная сложность связана с социальными сетями, где зачастую пользователи сами активно раскрывают информацию о себе, не задумываясь о том, что эта информация может быть легко использована против них.

Впрочем, по-прежнему актуальны и ситуации, когда информацию выкладывает в интернет и распространяет не сам человек, а кто-то другой – например, в случаях киберунижения. Надо сказать, что неконтролируемый оборот персональных данных опасен не только для нервов, но и для кошелька – широко раскрытые подробности о личной жизни нередко дают преступникам «ключ» к банковским счетам, а также дают возможности для того, чтобы спланировать кражи и грабежи.

С точки зрения законодателя (сначала европейского, потом российского), для требования прекратить оборот персональных данных неважно, выложил ли человек информацию о себе сам или ее опубликовали другие. Общедоступность персональных данных значима в тех случаях, когда надо решить, следует ли спрашивать разрешения субъекта персональных данных на перепост. Однако если речь заходит об удалении информации, значимо лишь одно: можно ли однозначно идентифицировать персону на основе спорных данных или нет.

Право на контроль за персональными данными не абсолютно. Международный законодатель предусматривает определенные исключения – например, в строго определенных правоохранительных целях или при оказании отдельных госуслуг. Однако для расширительной трактовки этих исключений государством присутствуют ограничения – например, обработка персональных данных должна соответствовать цели, заявленной при сборе.

ЗАКОН О “ПРАВЕ НА ЗАБВЕНИЕ”

«Право на достоверную информацию», или «Право на забвение» — это неофициальное название реального правового механизма, который позволяет убирать из поисковых выдач ссылки на контент, унижающий достоинство конкретно определяемого человека. В России этот правовой механизм обычно называют «Закон о достоверной информации», однако с персданными его почему-то не связали: оно присутствует только в Федеральном законе «Об информации». При этом, в силу отсутствия реальных наказаний для поисковиков, на практике «право на забвение» в России пока не сильно работает.

И тем не менее, убрать персональные данные о себе из интернета может и подросток, и взрослый – правда, первому может понадобиться помощь родителей. Хотя, к сожалению, и не во всех случаях.

ЕСЛИ ЧЕЛОВЕК ДАВАЛ СВОЕ СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ,

то он может его и отозвать – для чего надо направить соответствующий отзыв тому, кто эти данные обрабатывает. Лучше всего в письменной форме. В течение тридцати дней оператор персональных данных обязан прекратить их обработку, а также уничтожить их или – при невозможности удаления – заблокировать. Однако удаление возможно, если данные больше не нужны для целей их обработки.

ЕСЛИ ЧЕЛОВЕК СВОЕГО СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕ ДАВАЛ И НЕ ОПУБЛИКОВАЛ ИХ В ОТКРЫТЫЙ ДОСТУП САМ,

в течение трех рабочих дней оператор обязан прекратить обработку персональных данных. А потом, если еще за десять дней не удастся «ввести обработку в правовое поле» (то есть добиться согласия субъекта), то уничтожить персональные данные.

ЕСЛИ ДАННЫЕ БЫЛИ ОПУБЛИКОВАНЫ ЧЕЛОВЕКОМ САМОСТОЯТЕЛЬНО И РАСПРОСТРАНИЛИСЬ В ИНТЕРНЕТЕ,

оператор поисковой системы в течение десяти рабочих дней с момента получения требования гражданина (физического лица, заявителя) обязан прекратить выдачу ссылок на информацию, распространяемую с нарушением законодательства Российской Федерации, являющуюся недостоверной, а также неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя. Исключение составляет информация о событиях, содержащих признаки уголовно наказуемых деяний, сроки привлечения к уголовной ответственности по которым не истекли, и информации о совершении гражданином преступления, по которому не снята или не погашена судимость. В случае отрицательного решения, принятого в отношении доводов заявителя, оператор обязан направить ему мотивированный отказ.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В России существует уполномоченный орган по защите персональных данных. А именно – Роскомнадзор. По фактам нарушения оборота персональных данных гражданин может обратиться в территориальное управление Роскомнадзора. Ведомство уделяет весьма серьезное внимание повышению осведомленности граждан в плане их прав с персональными данными, особенно детей – и для их просвещения даже запустило специальный сайт. Полномочия Роскомнадзора вплоть до проведения проверок и права блокировок прописаны законодательно.

Одним из базовых способов защитить свои персональные данные и информацию о себе в интернете, является сохранение определенной анонимности в Сети

Как правило, пользование любыми пользовательскими сервисами в интернете, в том числе и средствами коммуникации, требует регистрации, подразумевающей возможность указания ряда персональных данных (фамилия, имя, отчество, возраст, домашний адрес, телефон и т.д.). Нужно помнить, что широкое указание персональных данных не требуется. Минимум указываемых персональных данных, допустимый для большинства интернет-ресурсов – фамилия, имя и иногда дата рождения / возраст.

При этом иногда полезно в интернете пользоваться псевдонимом – особенно на неперсонифицированных сервисах. В блогах и даже в социальных сетях этот вопрос скорее стоит отнести на усмотрение пользователя. Не секрет, что многие пользователи (особенно молодежь) специально идут в те же соцсети в поисках популярности и сбора «лайков», публикуя ради этой популярности различный контент.

ТАКИМ ПОЛЬЗОВАТЕЛЯМ МОЖНО ПОРЕКОМЕНДОВАТЬ ВЕСТИ ДВА АККАУНТА:

ЗАКРЫТЫЙ

который доступен только для офлайн-друзей, под подлинным именем

ОТКРЫТЫЙ

ради того самого «набора лайков» с более свободным режимом подписок, но уже под псевдонимом

Конечно, с ростом противоправного использования технологии распознавания лиц эффективность этого совета будет сходить на нет (злоумышленник сможет «пробить» лицо с аккаунта по всей соцсети либо по краденым базам биометрических данных), но еще несколько лет такой лайфхак будет актуален.

Псевдоним позволит защитить себя, своих близких и особенно детей от нежелательной идентификации злоумышленниками и возможных последующих нежелательных действий. Однако важно осознавать, что псевдоним в интернете не является индульгенцией (то есть разрешением) на недопустимые действия под прикрытием анонимности. Особенно это важно помнить детям, в среде которых часто встречается повышенная агрессивность.

Несмотря на свободу выбора псевдонима, в этом деле должны присутствовать определенные этические ограничения. Как представляется, вряд ли следует ограничивать желание взять псевдоним по имени популярного киногероя. Однако к числу «недопустимых ходов» относятся попытки выдать себя в Интернете за лицо другого пола или возраста. Поэтому на попытки, допустим, ребенка выдать себя за взрослого в Интернете родителям надо обращать соответствующее внимание и соответствующим образом корректировать.

КАК ЕЩЕ ЗАЩИТИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ:

ИСПОЛЬЗУЙТЕ СЛОЖНЫЕ ПАРОЛИ И МЕНЕДЖЕР ПАРОЛЕЙ

Не создавайте простые пароли для авторизации в социальных сетях, мессенджерах, почтовых и других онлайн-сервисах. Идеальный пароль сегодня должен быть достаточно длинным и простым для запоминания. Придумайте какую-нибудь фразу, состоящую из нескольких слов, которую сможете угадать только вы. Советуем использовать автоматический менеджер паролей, который будет создавать сложные пароли и автоматически подставлять их в нужные формы за вас. Главное: не забудьте пароль от аккаунта, к которому привязан менеджер паролей.

ИСПОЛЬЗУЙТЕ МЕССЕНДЖЕРЫ СО СКВОЗНЫМ ШИФРОВАНИЕМ

В мессенджерах со сквозным шифрованием могут иметь доступ к сообщениям только те пользователи, которые участвуют в диалоге. Ни какие-то третьи лица, ни создатели мессенджера не имеют доступа к переписке.

ИСПОЛЬЗУЙТЕ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

Самый главный совет по защите личных сетевых аккаунтов: обязательно включите двухфакторную аутентификацию везде, где только можно. Когда двухфакторная аутентификация включена, при заходе в личный аккаунт у вас запросят дополнительную информацию (SMS-код, скан пальца или лица, и т.д.), которая подтвердит, что именно вы пытаетесь воспользоваться данным аккаунтом.

НЕ ВЫКЛАДЫВАЙТЕ СЛИШКОМ МНОГО ИНФОРМАЦИИ О СЕБЕ В ИНТЕРНЕТ

Интернет-мошенники регулярно открывают различные страницы в соцсетях, чтобы выпытать полезную информацию, которую можно использовать для причинения вреда другим интернет-пользователям. Представьте, что ваш кодовый вопрос для восстановления пароля к электронной почте — имя вашего питомца. На своей странице в социальной сети вы делитесь фотографиями своего питомца и подписываете его имя. Мошенник без труда сопоставит эти данные и сможет без вашего ведома поменять пароль от адреса электронной почты, украв какие-то полезные данные.

ЧТО НЕ СЛЕДУЕТ ВЫКЛАДЫВАТЬ В ИНТЕРНЕТ, ЧТОБЫ ЗАЩИТИТЬ СВОИ ДАННЫЕ?

ФОТОГРАФИИ ПАСПОРТА И ДРУГИХ ДОКУМЕНТОВ В ОТКРЫТОМ ВИДЕ

Например, имея данные документов, мошенники могут занимать деньги у банка и зарегистрировать поддельную фирму.

ФОТОГРАФИИ СО ШТРИХКОДАМИ

В том числе фото билетов на любые мероприятия, а также авиабилетов. Другой человек может легко пройти на мероприятие по выложенному билету, обладая QR-кодом (его можно считать даже с фотографии билета в плохом качестве). Организаторы мероприятий не несут ответственности за подобные инциденты.

Если же мошенник считает штрихкод с авиабилета, он может узнать по номеру брони, когда вы улетаете и возвращаетесь, изменить дату и время вылета или даже аннулировать обратный билет

ДОМАШНИЙ АДРЕС

По онлайн-следам (например, фотографиям или статусам) можно понять, где в данный момент находится пользователь. Если злоумышленники знают еще и его адрес, то легко могут проникнуть в квартиру и ограбить ее.

НОМЕР ТЕЛЕФОНА

Если номер телефона попадает в Сеть (например, указан на странице в социальной сети), значительно увеличивается риск рекламных и спам-звонков.

БУДЬТЕ ОСТОРОЖНЫ ПРИ ПОДКЛЮЧЕНИИ К ОБЩЕСТВЕННЫМ СЕТЯМ WI-FI

Внимательно читайте соглашение и не раздавайте свои данные кому попало. В частности, при авторизации не сообщайте свою основную электронную почту и номер телефона. Например, для таких случаев, когда от вас требуется оставлять свои данные незнакомцам, лучше зарегистрировать дополнительный адрес электронной почты или купить еще одну SIM-карту. Кстати, они пригодятся и для совершения онлайн-покупок.

Также рекомендуем использовать при подключении к публичным сетям Wi-Fi VPN и отключить функцию передачи файлов, это позволит зашифровать передачу данных и никто не сможет перехватить ваши файлы и прислать вам что-то ненужное, например, вирусы.

Кроме того, не советуем входить в приложения, где указаны ваши персональные данные. Особенно в банковские приложения. Иначе вы рискуете потерять свои денежные средства

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

СЕРИЯ УЧЕБНЫХ ПОСОБИЙ ПО ЦИФРОВОЙ ГРАМОТНОСТИ

РОЦИТ