ИНФОРМАЦИОННЫЙ МАТЕРИАЛ К ЦИФРОВОМУ ДИКТАНТУ ПО ПЕРСОНАЛЬНЫМ ДАННЫМ

Часть 1. Основы правового регулирования в сфере персональных данных

Некоторое время назад Виктория устроилась на работу в модный сетевой бутик по продаже современной одежды. До трудоустройства она не знала, что такое персональные данные, в чем их смысл, какую они имеют важность и как их можно (и нужно) защищать. Иногда она слышала по телевизору или по радио истории про утечку чьих-то персональных данных, но не придавала этому значения.

Однако после трудоустройства ей пришлось не единожды столкнуться с проблемами, связанными с персональными данными. В первый же рабочий день к Виктории в магазин пришла разгневанная клиентка, которая недавно совершила покупку, в связи с чем ей была оформлена бонусная карта. Никаких документов при выдаче карты она не подписывала, только сообщила продавцу свои ФИО и номер телефона. Через некоторое время клиентке стали приходить назойливые адресные сообщения на почту и по смс от магазина о поступлении новых товаров и акциях. Данная информация клиентку не интересовала, а избавиться от назойливой рекламы она не смогла, смс приходили каждый день, причем с разных номеров. В итоге клиентка стала требовать связать ее с директором и угрожала судом за использование ее персональных данных без ее на то согласия. После консультации с юристом директор магазина лично встретился с клиенткой, много извинялся, и пообещал очень большую скидку, лишь бы успокоить её. Глядя на ситуацию, Виктория задалась вопросами: «Как такое могло произойти? Как обезопасить себя от подобного? И почему директор так переживал, чтобы не было обращения в суд?».

Ответы Виктория смогла найти в правовых справочниках, изучив основные положения законодательства в сфере персональных данных.

В настоящее время в Российской Федерации вопросы, связанные с защитой прав и свобод граждан при обработке персональных данных, в том числе и защиты прав на неприкосновенность частной жизни, личную и семейную тайну регулируются:

- Конституцией Российской Федерации от 12.12.1993;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Гражданским кодексом Российской Федерации от 30.11.1994 № 51-ФЗ;

- Трудовым кодексом Российской Федерации от 30.12.2001 № 197-ФЗ;
- Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Конституция Российской Федерации гарантирует каждому гражданину право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки. Сбор, хранение, использование и распространение информации о частной жизни человека не допускаются без его согласия согласно статье 23 и части 1 статьи Конституции РФ.

Центральное место в системе российского законодательства в области персональных данных занимает Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – «Закон о персональных данных»), основанный на конституционных положениях, гарантирующих защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

Во исполнение отдельных положений Закона о персональных данных был принят ряд подзаконных нормативных правовых актов. Кроме этого, в соответствии с указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» персональные данные относятся к категории конфиденциальной информации как сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность.

Какие данные считаются персональными?

В соответствии с пунктом 1 статьи 3 Закона о персональных данных под **персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).**

Среди персональных данных можно выделить следующие категории персональных данных:

1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных): ФИО, дата рождения, место рождения, адрес, телефон, семейное положение, социальное положение, имущественное положение, образование, профессия, занимаемая должность, стаж работы, доходы, иная информация;

2. Специальные категории персональных данных: расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья; состояние интимной жизни.

Обработка специальных категорий персональных данных допускается только в специально предусмотренных частью 2 статьи 10 Закона о персональных данных случаях.

3. Биометрические персональные данные – это сведения, характеризующие физиологические и биологические особенности человека, на основе которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Биометрические персональные данные будут являться таковыми при наличии условий:

- они признаны таковыми в силу положений нормативных правовых актов;
- они характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность;
- они используются оператором для установления личности субъекта персональных данных.

К биометрическим персональным данным относятся физиологические параметры (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и др.) и иные физиологические или биологические характеристики человека, в том числе его изображения (фотография и видеозапись).

Отпечатки пальцев человека являются биометрическими персональными данными (дактилоскопической информацией), обработка которых осуществляется только в случаях, установленных Федеральным законом от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации», которым четко определены виды и порядок проведения дактилоскопической регистрации. Обработка указанных данных в иных случаях действующим законодательством не предусмотрена.

Не относятся к биометрическим персональным данным:

- данные, полученные при сканировании паспорта оператором персональных данных для подтверждения осуществления определенных действий конкретным лицом (например, заключение договора на оказание услуг, в том числе банковских, медицинских и т.п.), т.е. без проведения процедур идентификации (установления личности);
- данные, полученные при осуществлении ксерокопирования документа, удостоверяющего личность;
- фотографическое изображение, содержащееся в личном деле работника;
- подпись лица, наличие которой в различных договорных отношениях является обязательным требованием, и почерк, в том

числе анализируемый уполномоченными органами в рамках почерковедческой экспертизы;

- рентгеновские или флюорографические снимки, характеризующие физиологические и биологические особенности человека и находящиеся в истории болезни (медицинской карте) пациента (не имеет значения, бумажной или электронной), поскольку они не используются оператором (медицинским учреждением) для установления личности пациента;
- материалы видеосъемки в публичных местах и на охраняемой территории.

4. Общедоступные персональные данные - это сведения, доступные неограниченному кругу лиц, информация из открытых справочников, к которой доступ имеет любой желающий, в частности из таких общедоступных источников персональных данных как справочники и адресные книги.

Согласно части 1 статьи 6 Закона о персональных данных одним из правовых оснований обработки персональных данных является наличие согласия субъекта персональных данных на обработку его персональных данных. Каждый субъект персональных данных самостоятельно принимает решение о предоставлении своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных может быть дано, если иное не установлено федеральным законом в любой позволяющей подтвердить факт его получения форме, в том числе в письменной форме, с использованием электронной подписи, акцептирования публичной оферты, получения на мобильный телефон и (или) электронную почту уникальной последовательности символов и иными способами и формами.

Закон о персональных данных предусматривает возможность дачи согласия в случае недееспособности субъекта персональных данных законным представителем субъекта персональных данных, в том числе законными представителями несовершеннолетнего являются его родители, а законным представителем лица, лишенного дееспособности, выступает его опекун.

Документами, подтверждающими законность представительства, могут являться свидетельство о рождении, акт о назначении опекуном, а в случае добровольного представительства надлежащим образом оформленная доверенность в простой письменной форме.

Обработка биометрических персональных данных несовершеннолетних в силу их недееспособности, в том числе с согласия в письменной форме законного представителя субъекта персональных данных на обработку его биометрических персональных данных, не допускается, за исключением случаев, предусмотренных частью 2 статьи 11 Закона о персональных данных.

Уполномоченным органом по защите персональных данных в России является Роскомнадзор (https://rkn.gov.ru/). По фактам нарушения

обработки персональных данных гражданин может обратиться в территориальное управление Роскомнадзора.

Часть 2. Обработка персональных данных

Нашей героине захотелось получше разобраться в вопросах защиты персональных данных еще и по причине произошедших с ней накануне событий. Однажды Виктории нужно было поменять сим-карту – старая не подошла к новому смартфону. Поскольку фирменный отдел оператора сотовой связи был далеко от ее дома, Виктория решила зайти в ближайший магазин сотовой связи, где виднелся логотип нужного оператора.

На месте ей предложили новый тариф, но для этого нужно было заполнить несколько бумаг, на одной из которых было написано «Согласие на обработку персональных данных». Так как Виктория очень торопилась, читать было особо некогда, она подписала все бумаги, не заглядывая в текст. На тот момент для нее это было не важно, главное, что номер не поменялся.

Однако спустя несколько дней данная сыграла злую шутку – у нашей героини подозрительно быстро закончились деньги на балансе, а на телефон постоянно стали приходить рекламные смс от различных торговых сетей, в которых она даже ни разу не была. Более того, через две недели в своем почтовом ящике Виктория обнаружила адресованный ей конверт с предварительно одобренной неименной кредитной картой с лимитом, который превышал её совокупный доход за полгода.

Виктория начала выяснять, в чем была причина данных событий, и все привело к оператору сотовой связи. После повторного обращения в салон выяснилось, что, подписав бумаги, она лично дала свое согласие на подключение платных сервисов в тарифе, прием рекламных информационных сообщений от третьих лиц – партнеров мобильного оператора, и согласие на выпуск неименной моментальной кредитной карты от банка-партнера салона связи.

После этого Виктория решила наконец выяснить, как защититься от подобного произвола, и отправилась изучать законодательство по обработке персональных данных, после чего она узнала, кто такие операторы персональных данных, какие требования к ним предъявляет государство и какие права есть у граждан - субъектов персональных данных.

В соответствии с пунктом 3 статьи 3 Закона о персональных данных обработка персональных данных – это любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Таким образом, законодательством перечень действий по обработке персональных данных не

ограничен и не исключает возможности обработки персональных данных любыми способами.

Обработка персональных данных должна соответствовать определенным целям, а обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается.

Основополагающими началами обработки персональных данных являются заложенные в Законе о персональных данных принципы обработки персональных данных:

- обработка персональных данных на законной и справедливой основе;
- ограничение обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопустимость обработки персональных данных, несовместимой с целями сбора персональных данных;
- обработка персональных данных, которые отвечают целям их обработки;
- соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- исключение обработки персональных данных, являющихся избыточными по отношению к заявленным целям их обработки и др.

Выделяют несколько способов обработки персональных данных:

- автоматизированная обработка персональных данных − обработка персональных данных с помощью средств вычислительной техники;
- неавтоматизированная обработка персональных данных – обработка персональных данных, осуществляемая при непосредственном участии человека;
- смешенная обработка персональных данных.

Статьей 16 Закона о персональных данных установлены права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных, в частности запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением следующих случаев: при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных. В частности, примерами могут стать следующие ситуации:

● по результатам автоматизированной обработки данных выявлено, что у работника недостаточный уровень квалификации, то на этом основании уволить его как несоответствующего занимаемой должности нельзя;

● по результатам автоматизированной обработки данных выявлено, что работник не зашел на территорию организации, то на этом основании привлечь его к ответственности нельзя.

Данное положение нашло также отражение в статье 86 Трудового кодекса Российской Федерации, согласно которой при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

Оператор непосредственно определяет порядок получения согласия субъекта персональных данных для обработки его персональных данных.

Письменная форма согласия должна включать в себя цель обработки персональных данных, а согласие субъекта персональных данных на обработку его персональных данных может включать в себя только одну цель обработки персональных данных. Указанная норма является императивной и не подлежит расширенному толкованию. При обработке персональных данных субъекта в случаях, требующих составления письменной формы согласия в соответствии с ч. 4 ст. 9 Закона о персональных данных, указанное согласие составляется отдельно для каждой из целей обработки персональных данных.

Согласно пункту 2 статьи 9 Закона о персональных данных согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В то же время необходимо отметить, что требования по обработке персональных данных не распространяются на отношения, возникающие:

1. при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2. организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда РФ и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3. обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Также положениями 2-11 части 1 Закона о персональных данных предусмотрены 10 случаев, при наступлении которых обработка персональных данных допускается без согласия субъекта персональных данных, к которым относится, в том числе следующие:

обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов

государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем и в других случаях.

Персональные данные в Интернете:

Персональные данные, которые могут быть собраны оператором через сайт, условно можно разделить на две группы.

1. Персональные данные, которые вы передаете сами, заполняя формы обратной связи на сайте: Ф.И.О., адрес, номер телефона, e-mail.

В этом случае объем переданных персональных данных вы можете определить сами. Согласие на обработку таких данных обычно можно предоставить путем:

проставления галочки в специальном окне («Я даю свое согласите на обработку персональных данных» ☑);

принятия условий публичной оферты, опубликованной на сайте; обычно оплата товара означает согласие с условиями.

2. Персональные данные, которые оператор собирает без предоставления вами информации.

В основном это файлы «куки» (cookie) – небольшие текстовые файлы со служебной информацией с сайта (сведения о программном обеспечении, которым вы пользуетесь, IP вашего компьютера, информация о вашем браузере).

Ваше согласие на обработку этих персональных данных оператор получает, если вы остаетесь на сайте после того, как появилось всплывающее окно с информацией примерно следующего содержания: «Продолжая использовать настоящий сайт, вы даете согласие на обработку файлов cookie в целях функционирования сайта. Если вы против обработки ваших данных, незамедлительно покиньте сайт».

Владелец сайта вправе обрабатывать ваши персональные данные только в тех целях, которые были указаны при получении вашего согласия, чаще это направление вам рекламных материалов. Файлы «куки» обычно используются для сбора статистики и информации о предпочтениях пользователя.

Часть 3. Защита персональных данных

Дело в том, что это не единственная история, произошедшая с Викторией и ее персональными данными. Однажды ей понадобилось срочно перевести деньги, когда она была в гостях у подруги. Лимит интернета на смартфоне закончился, и она решила зайти с компьютера подруги в свой интернет-банк для того, чтобы сделать перевод средств из личного кабинета. Виктория по привычке ввела в поисковике название банка, перешла по первой ссылке в поисковике, после чего открылся сайт нужного банка. Она ввела свой логин и пароль, но сайт выдал сообщение о том, что данные неверны, а личный кабинет заблокирован, а для восстановления доступа и оперативной разблокировки личного кабинета нужно ввести свои персональные данные – паспорт, СНИЛС, и номер телефона, после чего в специальном окне ввести код из смс, который придет на телефон. Ничего не подозревая, Виктория ввела запрошенную информацию, ведь сайт был полностью похож на официальный сайт ее банка. Однако, через некоторое время после отправки кода из смс, начали поступать сообщения о переводах с ее банковского счета и списаниях денежных средств. К счастью, Виктория смогла оперативно дозвониться на «горячую линию» своего банка (Виктория знала, что бесплатный номер телефона всегда можно найти на банковской карте), чтобы заблокировать операции по переводу денег.

Оказалось, что компьютер подруги был заражен вирусами, которые подменяли реальные адреса сайтов банков, и вместо этого открывали поддельные сайты злоумышленников (которые были точной копией официальных сайтов крупных банков), и вымогали учетные данные пользователей, после чего средства клиентов списывались на счета мошенников.

После этой истории наша героиня сделала несколько выводов – теперь у нее на домашнем ПК установлен лицензионный антивирус, она его регулярно обновляет и запускает проверку на вирусы. Кроме того, теперь она всегда проверяет адреса интернет-страниц сайтов и пользуется сохраненными ранее закладками, а не заходит по первой ссылке из «поисковика».

Важно знать! Фишинг – это метод мошенничества, позволяющий обмануть пользователя и заставить его раскрыть свой пароль, номер кредитной карты и другую конфиденциальную информацию, в том числе персональные данные! Большое количество случаев фишинга происходит при работе в сети Интернет, а особенно при работе с электронной почтой, поэтому очень важно соблюдать следующие правила:

1. Всегда проверять адрес сайта. Официальные сайты крупных организаций, таких как банки и государственные ресурсы имеют сертификат

безопасности, который виден в адресной строке браузера, а адрес сайта начинается с «https://».

1. При работе с почтой не переходить по ссылкам и не открывать вложения от незнакомых вам отправителей (всегда проверять адрес отправителя!).

2. Использовать «сложные» пароли – не менее 8 символов (в пароле должны быть верхний/нижний регистр + цифры + спецсимволы – ! ~#$%).

3. Никому не давать свой пароль, даже хорошо знакомым коллегам, сотрудникам из ИТ-подразделений. Сотрудники службы безопасности НИКОГДА не попросят вас сказать им свой пароль.

4. Важно помнить, что если почтовое сообщение запрашивает ваш пароль, или требует пароль взамен на получение какой-либо услуги, то не стоит вводить его. Скорее всего, это проделки злоумышленников.

7. Если Вы получили вложение или ссылку от знакомого отправителя, но нет уверенности в ее безопасности – не открывайте ссылку! Попробуйте связаться с отправителем альтернативным способом и уточнить, отправлял ли он Вам данное письмо - возможно его ящик был взломан злоумышленниками.

Угрозы безопасности персональных данных

В отношении физических лиц наиболее вероятна угроза неправомерного доступа к их персональным данным для завладения личной информацией и дальнейшего использования в корыстных и прочих противоправных целях. При возникновении угрозы со стороны злоумышленника целью, как правило, ставится нанесение финансового ущерба субъекту персональных данных. Злоумышленники могут манипулировать персональными данными с целью оказания давления на субъекта и принятие им выгодного вымогателям решения. Иностранные спецслужбы и организации могут ставить целью дестабилизацию экономической, социальной и политической жизни региона или целого государства.

Угрозы безопасности персональных данных включают в себя:

- угрозы утечки персональных данных с сервера оператора персональных данных. Угроза возникает при передаче персональных данных оператору, не заинтересованному в тщательной проработке мер защиты доступа к хранимым на его серверах персональным данным и допускающему (непреднамеренно или преднамеренно) утечки персональных данных.
- угрозы доступа (проникновения) в операционную среду устройства с использованием штатного программного обеспечения:
    1. угрозы непосредственного доступа. Злоумышленник может получить доступ к устройству или ресурсу, содержащему

персональные данные, оставленному без присмотра с недостаточной степенью защиты доступа;

2. угрозы удаленного доступа. Злоумышленник может получить доступ к устройству или ресурсу с используемыми дефолтными (по умолчанию) данными для авторизации; либо осуществить то же самое посредством взлома нестойких систем защиты.

- Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств (могут возникнуть, например, в случае использования нелицензионного программного обеспечения).
- Угрозы внедрения вредоносных программ. Такие угрозы наиболее распространены и могут возникать при посещении сомнительных ресурсов, установки нелицензионного или скомпрометированного программного обеспечения.
- Угрозы методами социальной инженерии. Данный вид угроз реализовывается злоумышленником целенаправленно в отношении пользователя и/или третьих лиц. Вероятность возникновения угрозы данного типа возрастает при публикации персональных данных в открытых источниках в цифровой среде, а также при несоблюдении достаточных мер по защите своих персональных данных.

Зная актуальные угрозы безопасности персональных данных, можно определить основные меры защиты:

Как защитить свои персональные данные в Сети:

1. Одним из базовых способов защиты своих персональных данных и информации о себе в сети Интернет является сохранение определенной анонимности.

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. Интернет-мошенники регулярно открывают различные страницы в соцсетях, чтобы выпытать полезную информацию, которую можно использовать для причинения вреда другим интернет-пользователям.

Не стоит выкладывать в Интернет фотографии паспорта и других документов в электронном виде, фотографии интимного характера, фотографии со штрих-кодами, в том числе фото билетов на любые мероприятия, а также авиабилетов, домашний адрес и номер телефона.

2. 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.

3. 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.

4. 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.

5. Регулярно выполняйте обновление антивирусного ПО и операционной системы.

6. Не используйте и не устанавливайте «взломанные» платные программы, они могут привести к утечке данных.

7. Будьте осторожны при подключении к общественным (открытым) сетям Wi-Fi.

Внимательно читайте соглашение о подключении, 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.

При подключении к публичным сетям Wi-Fi рекомендуется отключить функцию передачи файлов. Не стоит входить в приложения, где указаны ваши персональные данные. Особенно в банковские приложения.

Какие еще правила безопасности в цифровой среде нужно соблюдать?

1. Установить на персональный компьютер и телефон надежную антивирусную защиту. Она блокирует попытку перехода на подозрительный сайт, а также остановит вирус или банковский троян при попытке проникнуть в устройство.

2. Не переходить по подозрительным ссылкам в смс и электронных письмах.

3. Скачивать приложения только из официальных магазинов Apple Store, Microsoft Store и Google Play. В настойках телефона установить запрет на скачивание приложений из непроверенных источников.

4. В ходе установки приложений обращать внимание на запросы разрешений (например, доступ к контактам и на отправку смс).

5. Внимательно читать название сайта, на котором вводятся конфиденциальные данные. Зачастую названия сайтов-подделок от оригинальных отличаются лишь одним символом.

И не только Интернет

И, когда, казалось бы, Виктория знала уже все о защите своих персональных данных, с ней произошла следующая история:

На телефон позвонил человек, который представился сотрудником службы безопасности банка, и сообщил, что на ее счете замечены подозрительные операции. Виктория, будучи человеком опытным и образованным, не стала доверять незнакомцу и собиралась скорее закончить разговор, чтобы самостоятельно позвонить в банк и прояснить ситуацию. Однако на том конце провода убедили ее не терять времени и заблокировать карту, потому что «злоумышленники» снимут деньги быстрее, чем она наберет номер банка. Виктория доверилась незнакомцу, к тому же, что он и не собирался спрашивать у нее ни пин-код, ни CVC-код карты – только номер лицевого счета. Для «заморозки» денег потребовалось назвать незнакомцу код из push-уведомления, которое пришло ей на телефон прямо во время разговора. Также во время разговора Виктория слышала, что на телефон ей приходят смс, но не стала перебивать собеседника и прочитала сообщения, когда разговор уже закончился. Каково же было ее удивление, когда она наконец прочитала входящие смс, о том, что с ее счета в очередной раз были списаны денежные средства несколькими операциями на общую сумму 50 тысяч рублей.

Важно знать! Никогда не сообщайте ПИН-код от банковской карты, указанный на обороте банковской карты код безопасности, одноразовый пароль, смс или push-сообщения третьим лицам!

Никто, в том числе сотрудники банка, не вправе требовать от держателя карты сообщить ПИН-код или код безопасности. А одноразовый пароль вводится при совершении онлайн-покупки на странице с защищенным соединением.

Довольно часто мошенники выдают себя за сотрудников банка. Под предлогом «сбоя в базе данных», «начисления бонусов» или «подключения к социальной программе» злоумышленники просят, а иногда даже требуют сообщить им реквизиты карты, код безопасности и одноразовый пароль. Получив необходимые сведения, мошенники списывают деньги со счета. Злоумышленники могут также говорить о подозрительных операциях или покушении на счет, для предотвращения требуется сообщить ее данные либо произвести определенные действия с помощью банкомата – ЭТО ОБМАН.

Другая схема мошенничества: компенсация или социальная выплата.

Представляясь работниками различных госструктур, неизвестные сообщают, что вам якобы положена компенсация за приобретаемые ранее некачественные БАДы или лекарственные препараты, для ее получения нужно лишь оплатить пошлину или проценты. Либо сообщают, что вам положены выплаты или пособия. Для зачисления денежных средств вас просят назвать данные банковской карты – ЭТО ОБМАН.

Помните, что самый распространенный способ совершения хищений денежных средств с карт граждан – побуждение владельца карты к переводу денег путем обмана и злоупотребления доверием!