Персональные данные – это любая информация о человеке, которая связана с ним, позволяет идентифицировать его в полной мере, получить иные сведения о нем, совершать какие-либо посягательства на тайну его личной жизни или на имущество.

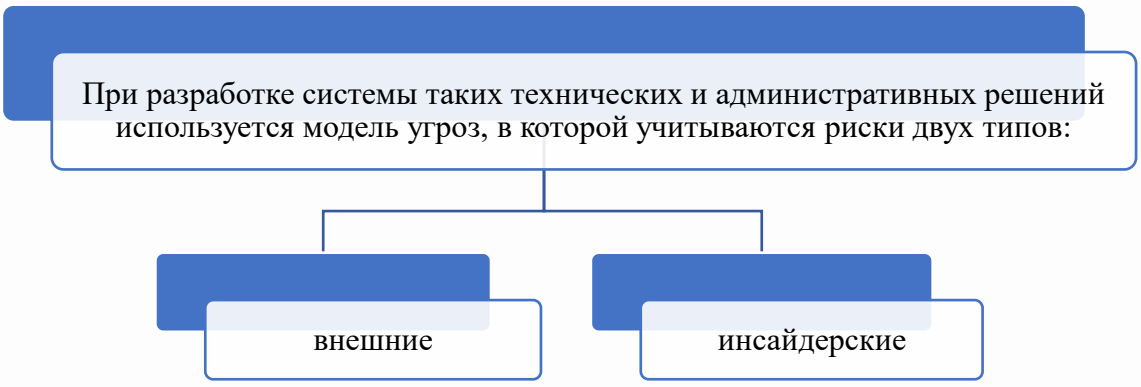
В группе риска утраты важной информации при проведении обработки персональных данных оказываются многие люди, среди них:

- граждане, пользующиеся банковскими картами;
- граждане, получающие медицинские услуги;
- владельцы пенсионных накоплений;
- вкладчики банков;
- владельцы недвижимости

Это не исчерпывающий перечень, пострадать от утечки персональных данных могут и многие другие. Поэтому государство выстроило систему защиты персональных данных. В ее основу лег Федеральный закон от 27.07.2006 № 152-ФЗ «О защите персональных данных», систему технических мер регламентируют правительство, ФСТЭК, ФСБ.

Причины утечек

Любая организация, которая в своей деятельности обрабатывает персональные данные, обязана предпринять комплекс организационных и технических мер, направленных на их защиту. Перечень этих мер и способов регламентируется для каждой группы данных.



Первый тип угроз, представляющих собой неправомерное проникновение в защищенный информационный периметр организации-оператора, – хакерские атаки.

Второй тип угроз реализуются наиболее часто. Гражданин предоставляет сведения о себе во множестве случаев в медицинском учреждении, в туристическом

агентстве, в котором для оформлении визы, он практически полностью раскрывает сведения о своем финансовом статусе. Согласие на обработку персональных данных зачастую не подписывается. Таким образом, паспортные данные, сведения о недвижимости, доходах, операциях по банковской карте оказываются в незащищенном виде в компьютере, на котором может не быть даже антивирусной защиты.

В этом случае доступ к ним становится возможным:

- при прямом проникновении недобросовестного сотрудника агентства в компьютер или к материальным носителям информации;
- при размещении их в облачных сетях, иногда на множестве серверов, зачастую расположенных не в России. Законодательство требует обязательного хранения персональных данных внутри страны, но эти требования выполняют не все операторы, зачастую даже не знающие о существовании такой обязанности;
- при хищении ноутбука или портфеля сотрудника компании, в котором находится интересующая злоумышленника информация.

Частые случаи, появляющиеся в судебной практике, в которых штрафуются или наказываются иным образом врачи или сотрудники банковских учреждений, допустившие утечку сведений, например, паспортных данных, говорят о существовании проблемы и ее серьезности.

Последствия утечек

Последствия утечек могут оказаться серьезными и для владельцев данных, и для операторов. Для первой группы существуют многочисленные риски стать жертвой злоумышленников.

Они могут пострадать:

- от разглашения любой информации, имеющей отношение к личности;
- от шантажа;
- от неправомерного списания средств с банковской карты;
- от вмешательства в личную жизнь.

Минимальным риском станет неправомерная передача сведений, например, адреса электронной почты, каким-либо компаниям, которые начнут преследовать их обладателя рекламными объявлениями. Но даже это дает возможность возбудить дело и о неправомерной рекламе, и об утечке данных и приведет к штрафам, налагаемым на операторов, если источник утечки или спама удастся достоверно установить.

Операторы, в свою очередь, допустившие утечку персональных данных, понесут ответственность:

- гражданскую, в виде взыскания в судебном порядке понесенных гражданами убытков и морального вреда;
- административную, в виде наложения штрафа, приостановления или запрета деятельности, связанной с обработкой персональных данных;
- уголовную, в случае неправомерного распространения ПДн, причинившего существенный ущерб и передаче информации в правоохранительные органы.

Как избежать негативных последствий от утечек данных

Меры по защите информации требуют не только исполнения операторами обязанностей, установленных законом, но и **осмотрительности от субъектов персональных данных**. От первых потребуется максимально внимательно относиться к соблюдению требований закона, постановлений правительства РФ и нормативных актов ФСТЭК России, которыми определяется необходимый уровень технических средств, призванных защитить персональные данные от утечки.

Это такие меры, как:

- установка межсетевых экранов, затрудняющих проникновение к массивам информации;
- внедрение системы идентификации и аутентификации сотрудников, имеющих к ним доступ;
- фиксация в журналах учета всех действий специалистов, осуществляющих обработку данных, позволяющая понять, что конкретно они делали с охраняемыми законом сведениями;
- установка средств антивирусной защиты;
- использование средств криптографической защиты для шифрования данных при хранении и передаче;
- применение способов и мер, которые могут предотвратить утечку данных по физическим каналам, например, путем фотографирования экрана компьютера, снятия звуковой информации, перехвата

Все эти меры защиты от утечек данных требуют существенных средств, но они внедрены в большинстве государственных учреждений и крупных компаниях. В зоне риска продолжают оставаться небольшие фирмы, чаще работающие на рынке оказания услуг гражданам. Они далеко не всегда попадают в перечень проверок Роскомнадзора, так как не считают необходимым действием регистрацию в качестве операторов. Даже если это будет произведено, создание системы технической защиты информационных баз персональных данных является затратным мероприятием, которое не все могут себе позволить. **Именно это требует проявления осмотрительности от граждан при выборе поставщика услуг и взаимодействиях с ним.**

Среди таких правил:

- не передавать персональные данные компаниям, не зарегистрированным в качестве операторов;
- осторожнее относиться к любым платежам в сети Интернет;
- всегда изучать текст согласия на обработку персональных данных, определяя, какими способами она производится, каковы цели обработки, возможность передачи сведений третьим лицам и в каких случаях.

Соблюдение осторожности и операторами, и гражданами позволит минимизировать риски. Всегда нужно помнить, что полностью возместить материальный и моральный ущерб у гражданина не получится.