Основы защиты персональных данных

ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Персональные данные - это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. Различные фрагменты информации, собранные вместе, и приводящие к идентификации конкретного лица, также представляют собой персональные данные. Трудно точно сказать, какая именно информация о человеке входит в такое понятие персональных данных (**ПДн**). Обращаясь к законодательству разных стран в области хранения и обработки **ПДн**, нельзя найти точного определения что является персональными данными. Но можно точно сказать, если по совокупности личной информации мы можем определить конкретного человека, мы имеем дело с персональными данными.

Под такое определение попадает множество личных данных, которые как по отдельности, так и в совокупности, могут указать на конкретного человека.

Основы защиты персональных данных

Таким образом персональными данными являются:

- Имя, отчество и фамилия
- Номер стационарного или мобильного телефона
- Место рождения и дата рождения
- Домашний адрес
- Адрес электронной почты (name.surname@company.com)
- Паспортные данные
- IP адрес и cookie-файлы

- Информация о болезнях
- Фото и видео файлы
- Аккаунты в социальных сетях
- ИНН

Это лишь малая часть личной информации, по которой можно точно определить нужного человека. Несанкционированная, неосторожная и не имеющая должной зашиты обработка персональных данных может причинить большой вред физическим лицам и компаниям. Целью защиты персональных данных является не просто защита персональных данных человека, а защита основных прав и свобод людей, связанных с этими данными. Надежно защищая персональные данные, можно гарантировать, что права и свободы человека не нарушаются. Например, неправильная обработка персональных данных может привести к ситуации, когда человек упускает возможность трудоустройства или, что еще хуже, теряет текущую работу. Несоблюдение правил защиты персональных данных может привести к еще более жестким ситуациям, когда можно снять все деньги с банковского счета человека или даже создать опасную для жизни ситуацию, манипулируя медицинской информацией.

Исходя из этого можно сказать, что любая компания, собирающая подобную информацию, должна обеспечить надежную защиту для хранения и обработки персональных данных. В России законодательной основой защиты ПДн является федеральный закон **№152-ФЗ "О персональных данных"**. В этом законе говорится, что любая организация, физическое или юридическое лицо, которое осуществляет обработку персональных данных является оператором персональных данных и несёт уголовную, административную и гражданскую ответственность за нарушение требований хранения и обработки персональных данных. В Европе защита персональных данных регулируется "Общим регламентом по защите персональных данных" (GDPR). За обработку и сохранность данных согласно GDPR отвечает контроллер данных. За нарушение норм GDPR предусмотрены штрафы в размерах до $20 млн. или до 4% оборота компании.

КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для определения методов и способов защиты персональных данных их можно разделить на несколько категорий:

- Особо охраняемы данные. К этой категории относятся данные, раскрытие которых может повлиять на конфиденциальность личности и в результате привести к дискриминации. Исчерпывающего перечня таких данных не существует, однако, данные, относящиеся к следующей информации, стали широко рассматриваться как конфиденциальные: политические взгляды, религиозные взгляды, физическое и ментальное здоровье, сексуальная ориентация, расовая и этническая принадлежность, генетические данные и т.п.
- Биометрические данные. К таким данных относят физиологические или поведенческие признаки физического лица. Такие данные позволяют однозначно идентифицировать человека. Можно отнести к таким ПДн отпечатки пальцев, изображение человеческого лица, сетчатку глаза, запись голоса.

- Общие данные. Все данные, относящиеся к человеку, которые он сам разместил в открытом доступе или же прямо или косвенно к нему относящиеся. К таким данным можно отнести страницу в социальных сетях или список редакции журнала.
- Обезличенные или не относящиеся к остальным категориям данные.

Для разных категорий данных требуется обеспечение разной степени защиты. Особо охраняемы данные требуют максимальной защиты, так как нарушение требований защиты или утечка персональных данных может привести к значительному ущербу для субъекта персональных данных. Обезличенные же данные требуют лишь минимальной защиты, так как это не приведет к негативным последствиям для субъекта ПДн при утечки персональных данных.

СПОСОБЫ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Любая организация, которая хранит или обрабатывает любую персональную информацию пользователей и использует ее в личных целях является оператором ПДн и должен надежно их защищать, чтобы соответствовать законодательству нашей страны. Для работы организации необходимые данные клиентов должны быть доступны для многих сотрудников с нескольких устройств, поэтому должны быть обеспеченна легкая доступность и возможность легкого доступа. Решением этой проблемы может послужить локальное хранилище или различные облачные решения. Для защиты персональных данных согласно закону №152-ФЗ "О персональных данных" выделяется несколько технических мер, например шифрование. Существует три основных подхода для хранения шифрованных совместно используемых персональных данных:

- Локальное хранение зашифрованных данных. В этом случае данные шифруются и уже зашифрованные данные сохраняются на локальных серверах.
- Облачное хранилище с шифрованием на стороне сервера и при передаче. Шифрование данных осуществляет поставщик облачного хранилища, который шифрует и хранит персональные данные пользователей, а также соответствующий ключ шифрования и расшифровки в безопасном месте. По вашему запросу провайдер может расшифровать данные по вашему запросу. Такие услуги предлагают практически все облачные провайдеры, такие как Яндекс, Google, Dropbox, Microsoft и другие.
- Облачное хранилище с сквозным шифрованием. В этом случае данные шифруются на вашей стороне, а хранение осуществляется на облаке. Преимущество такого способа хранения в том, что вы единственный, кто обладает ключом для расшифровки данных и никто другой, даже поставщик облачных услуг.

Для того понять преимущества и недостатки каждого решения для хранения и шифрования проведем риск-анализ и выясним актуальности и вероятность успеха некоторых атак, направленных на кражу и повторное использование персональных данных пользователей.

ЛОКАЛЬНОЕ ХРАНЕНИЕ ЗАШИФРОВАННЫХ ДАННЫХ

Способ локально хранения является достаточно простым и безопасным только в том случае, если сервер, хранящий ПДн и ключ для расшифрования достаточно защищен. Однако реализовать высокий уровень защиты для небольших и средних организаций достаточно проблематично, так как хранение персональных данных не основная их деятельность. Даже наличие достаточной технической защиты и использование безопасных программ обычно недостаточно. Профессиональные целенаправленные атаки могут полностью обойти все средства защиты используя фишинг и социальную инженерию. Это может произойти, например, если сотрудник компании откроет безобидное вложение ил пройдет по ссылке в письме, которая была подделана злоумышленником. Далее вредоносное программное обеспечение, установленное на любую машину, получает доступ к локальной сети и, использовав уязвимости некоторых программных компонентов, получает доступ к конфиденциальным файлам, в которых может храниться ключ для расшифровки базы ПДн. Кроме того, вредоносные программы могут считывать нажатия клавиш, когда вы вводите пароль для расшифровки вашей базы данных. Даже компании, которые вкладывают значительные средства в безопасность данных подвержены таким угрозам.

ОБЛАЧНОЕ ХРАНИЛИЩЕ С ШИФРОВАНИЕ НА СТОРОНЕ СЕРВЕРА

Оператор персональных данных доверяет шифрование ПДн клиентов провайдеру облачного хранилища, передавая данные в облако по защищенному каналу. Провайдер шифрует данные и сохраняет их вместе с ключом шифрования и расшифровки в безопасном месте. Всякий раз, когда оператору ПДн необходимы данные, поставщик облачных услуг расшифровывает их и отправляет расшифрованные данные по к оператору ПДн по защищенному каналу. Для внешнего злоумышленника получение доступа к серверу провайдера, на котором хранятся зашифрованные данные, может быть технически более сложным, чем при использовании локального сервера. Это объясняется тем, что хранение данных является их основной деятельностью, поэтому провайдеры облачных хранилищ более подготовлены к таким атакам и используют более комплексную защиту. Тем не менее, вероятность успешной атаки вероятна даже в этом случае. Реальная разница заключается в мотивации злоумышленника. Если он знает, что поставщик хранит ключ дешифровки данных или незашифрованные данные, то злоумышленник может быть гораздо более мотивированным, при нападении на него. Наконец, внутренние злоумышленники включают самого облачного провайдера, а также его сотрудников, которые могут легко получить ключ для расшифровки данных. Хотя у поставщика облачных услуг нет стимула пользоваться файлами и базами данных клиентов из-за потенциальных юридических последствий и потери репутации, однако несправедливо уволенный или финансово мотивированный сотрудник может это осуществить.

ОБЛАЧНОЕ ХРАНИЛИЩЕ С ШИФРОВАНИЕ НА СТОРОНЕ КЛИЕНТА

Данный способ хранения ПДн сочетает в себе преимущества локального хранения и облачного хранения с шифрование на стороне провайдера. Только оператор ПДн знает ключ для расшифровки, но данные безопасно хранятся у поставщика. Даже в случае, если злоумышленник каким-то образом получит копию зашифрованной базы данных с ПДн клиентов, то он не извлечет никакой личной информации. Практическую пользу от таких данных злоумышленник получит только в случае их успешного расшифрования, а для этого требуется ключ дешифровки. Если размер ключа равен 256 бит и является полностью случайным, вероятность того, что злоумышленник угадает ключ ничтожно мала. Таким образом, можно с уверенностью сказать, что ни один злоумышленник не имеет шанса угадать ключ. До тех пор, пока данные не могут быть расшифрованы, они не представляют ценности и не принесут ущерба субъектам ПДн.

Однако, если ваш ключ расшифровки генерируется не случайно или совпадает с вашим паролем, злоумышленник может подобрать нужный ключ и расшифровать базы с персональными данными. Так же, алгоритм шифрования, используемый оператором ПДн или провайдером облачного хранилища, может быть уязвим для некоторых атак. Например, злоумышленник может использовать конструктивные недостатки схемы шифрования. Этого довольно маловероятно, если используются рекомендуемые и стандартизированные алгоритмы шифрования. Еще однин способ взлома схемы шифрования заключается в использовании недостатков реализации в некоторых программных компонентах, использующихся в схеме шифрования. Недостатки реализации неизбежны до тех пор. Для лучшей реализации защиты персональных данных необходимо оператору ПДн и провайдеру облачных услуг использовать рекомендуемые средства криптографической защиты информации (**СКЗИ**), а также регулярно обновлять программные компоненты.

Таким образом, проанализировав каждый способ хранения можно сделать выводы о возможных угрозах, уязвимостях и путях утечки персональных данных в выбранном способе хранения. В приведенной ниже таблицы приведены в соответствие способы хранения и вероятности утечки ПДн, что позволяет сделать выбор наилучшего способа хранения базы персональных данных.

Таблица Актуальность и вероятность успеха атаки на ПДн

Таблица Актуальность и вероятность успеха атаки на ПДн

Исходя из данных таблицы, можно сделать вывод о том, что облачное хранилище со сквозным шифрованием обладает наибольшей степенью защиты и наименьшей вероятностью утечки данных. Это происходит главным образом потому, что провайдер не имеет доступа к ключам для расшифрования данных, и поэтому злоумышленник не так сильно замотивирован. Даже если он получит доступ к данным, они не буду иметь ценности в зашифрованном виде. Еще одна причина для использование облачного хранилища вместо локального повышенная

безопасность. Поставщик облачных услуг имеет гораздо более защищенную от угроз сервера. Это улучшает доступность и целостность персональных данных, что является главными принципами информационной безопасности.

КАТЕГОРИИ УГРОЗ

Под угрозой персональных данных можно считать случаи, при которых возникает вероятность потери или раскрытия личной информации субъекта персональных данных. Угрозой является лицо или организация, которые стремятся получить, изменить данные или другие активы ИС (информационной системы) незаконно, без разрешения владельца и часто без ведома владельца. Уязвимостью является возможность для угроз получить доступ к индивидуальным или организационным активам. Например, когда человек покупает что-то в интернете, он предоставляет данные кредитной карты, когда эти данные передаются через Интернет, они уязвимы для угроз. Защитная мера - это некоторая мера, которую отдельные лица или организации принимают для предотвращения угрозы неправомерного получения актива. Наконец, целью угрозы является актив, который желателен для угрозы. Угроза безопасности - это вызов конфиденциальности, целостности и доступности информационных систем, возникающих от одного из трех источников:

- Человеческих ошибок
- Компьютерных преступлений
- Стихийных бедствий

Человеческие ошибки включают неумышленные и случайные действия, представляющие угрозу **ИСПДн**, вызванные работниками организации. Действия сотрудников в выполнении процедур или их отсутствие могут привести к отказу в обслуживании. Например, сотрудники могут непреднамеренно отключить веб-сервер или шлюзовой корпоративный маршрутизатор, запустив интенсивное вычислительное приложение. Неосведомленность или халатность сотрудников организации или компании может поставить под угрозу конфиденциальность данных и безопасность компонентов сети организации. Открыв фишинговое электронное сообщение или заразив корпоративный компьютер, сервер вредоносным программным обеспечением со своего личного телефона, ноутбука или просто скопировав конфиденциальную информацию на свое устройство, чтобы доделать работу дома. Фишинг одна самых популярных атак, от которой практически невозможно защитить пользователей интернета. Так же никто не может быть уверен, что сотрудник не совершит ошибку и не отправит секретную или конфиденциальную информацию по ошибочному адресу. Описанные ситуации представляют серьезную угрозу безопасности данных.

К категории компьютерных преступлений относятся действия сотрудников и бывших сотрудников, которые умышленно уничтожают данные или другие компоненты системы. Умышленные же действия сотрудники преднамеренно совершают для получения доступа к секретной информации или нанесения ущерба компании. Злоумышленники или компании-конкуренты могут за материальное вознаграждение получать от сотрудников компании важную и конфиденциальную

информацию. В своем большинстве это опытные сотрудники, которые могут легко уничтожить следы своих преступлений. Выявление таких сотрудников очень непростая задача. Также угрозу безопасности данных компании представляют уволенные сотрудники, которые при увольнении могут забрать всю информацию, к которой имеют доступ. В категории компьютерных преступлений угроза безопасности данных обусловлена действиями физических лиц, террористических организаций, иностранных спецслужб и криминальных формирований, реализующие ситуации в которых создаются условия, представляющие угрозу безопасности персональных данных. Также к категории компьютерных преступлений можно отнести действия злоумышленников, которые взламывают систему, авторов вирусов и червей, которые заражают компьютерные системы, а также аппаратные и программные закладки. Атаки типа "**отказ в обслуживании**" могут быть осуществлены злоумышленниками. Злоумышленник может перегрузить веб-сервер, например, миллионами поддельных запросов, которые перегрузят сервер так, что он не сможет обслуживать реальные запросы.

Природные явления и катастрофы включают пожары, наводнения, ураганы, землетрясения, цунами, лавины и другие природные явления. Проблемы этой категории включают в себя не только первоначальную потерю доступности, но и потери, возникающие в результате действий по устранению первоначальной проблемы.

Большинство угроз реализуемых с применением программных средств, осуществляются при несанкционированном или случайном доступе, в процессе которого происходит полное нарушение конфиденциальности, целостности и доступности персональных данных, т. е. копирование, изменение, уничтожение или несанкционированное распространение. Такие угрозы включают в себя:

Угрозы внедрения вредоносного программного обеспечения. Угрозы такого типа широко распространены. Реализуются при посещении непроверенных ресурсов без подтвержденного сертификата или при подключении по незащищенному протоколу связи, а также в случае использования неофициального (пиратского) программного обеспечения.

Угрозы утечки с серверов оператора ПДн. Такие угрозы обусловлены халатностью и нежеланием операторов персональных данных обеспечить необходимые меры по защите доступа к персональным данным хранящихся на серверах, а также каналов передачи. Невыполнение минимальных рекомендаций для защиты персональных данных приводит к утечкам и несанкционированному распространению информации.

Осуществляемые методами социальной инженерии угрозы. Актуальный вид угроз от которого нет надежных способов защиты. Действия злоумышленника направлены на получение от пользователей или сотрудников конфиденциальной информации или доступа к интересующим его информационным системам, хранящих персональные данные. Вероятность реализации угроз данного типа увеличивается при недостаточных мерах защиты персональных данных, а также публикации личной информации в открытых источниках.

Угрозы проникновения в операционную среду устройства с использованием прикладных программ или средств операционной системы подразделяются на:

- Угрозы непосредственного доступа. Доступ к серверу или базе данных, оставленному без присмотра и без соответствующей защиты и содержащей персональные данные, злоумышленник может осуществить непосредственно.
- Угрозы удаленного доступа. Доступ к серверу или базе данных злоумышленник может получить посредством взлома систем защиты, либо используя по умолчанию установленные данные для авторизации.

Угрозы нештатных режимов работы программных средств за счет преднамеренных изменений служебных данных, игнорирования, предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, модифицирования самих данных. Использования нелицензионного или скомпрометированного программного обеспечения создает риск реализации угроз данного типа.