ЗАКОНЫ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК ЭЛЕМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ПРИМЕНЕНИЕ

Нематова Сабина Зафаровна
студентка 3-курса ТГЮУ

Аннотация: *Данная статья рассматривает вопросы о регулировании защиты персональных данных, проводится анализ понятии о персональных данных. Также, определены законы и нормативно правовые акты, регламентирующие правоотношения в сфере персональных данных, на международном и государственном уровне.*

Ключевые слова: *персональные данные; защит; правовое регулирование; защита персональных данных.*

Развитие цифровых технологий является несомненным катализатором глобального прогресса. В то же время глобальная цифровизация, интернет, мобильная связь, компьютерные технологии и потенциал науки и техники в этой области неизбежно влекут за собой новые риски и угрозы. Обеспечение информационной безопасности и защита персональных данных стали в последние годы одной из ключевых задач не только в глобальном масштабе, но и для всех государств и организаций. На международном уровне система защиты персональных данных отражена в принципе неприкосновенности частной жизни. Этот принцип содержится в Международном пакте о гражданских и политических правах (статья 17), согласно которому никто не должен подвергаться произвольному или незаконному вмешательству в неприкосновенность его жилища или тайну его сообщений, или незаконному посягательству на его честь и репутацию. В зарубежном законодательстве существует два основных подхода к определению персональных данных. Во-первых, некоторые страны, такие как Нидерланды, Швеция и Новая Зеландия, определяют всю информацию о человеке как персональные данные. Во-вторых, некоторые страны установили определенные критерии отнесения информации к этой категории и детально их определяют (например, Великобритания). В то же время наилучшим вариантом регулирования считается такой, при котором тщательно определены и закреплены в законодательстве два фундаментальных информационных права и свободы, чтобы соблюдался баланс: право на доступ к информации, затрагивающей интересы отдельных лиц, и право на ограничение доступа третьих лиц к информации о себе.

Европейский союз (ЕС) разработал и принял правила защиты персональных данных, закрепленные в Общем регламенте по защите данных (GDPR). На основании этого документа были значительно расширены права

субъектов персональных данных, а также существенно увеличены обязательства операторов и штрафы за их невыполнение. Определение персональных данных в самом GDPR содержит следующее. "Любая информация об идентифицированном или поддающемся идентификации физическом лице ("субъекте данных"). Идентифицируемое физическое лицо - это лицо, которое может быть прямо или косвенно идентифицировано, в частности, путем ссылки на идентификатор, такой как фамилия, идентификационный номер, данные о местонахождении или онлайн-идентификатор, или путем ссылки на одну или несколько физических, физиологических, генетических, психических, экономических, культурных, социальных, экономических, культурных или культурных характеристик этого лица".

Во время распространения новой коронавирусной инфекции COVID-19 произошли глобальные изменения в социальной жизни людей. Например, многие работодатели были вынуждены переводить сотрудников на дистанционные формы работы, чтобы сохранить стабильность своей деятельности, а учебные заведения создали возможности для дистанционного обучения. Особый характер такой работы предполагает наличие надежных каналов связи и достаточных материальных ресурсов для осуществления переходного процесса при условии повышенной информационной безопасности в части защиты персональных данных. Многие сотрудники работают из дома на своих личных ноутбуках или компьютерах, размывая границы между корпоративными и личными устройствами, а также между корпоративными и личными данными, что априори снижает уровень защиты информации. В то же время почти все организации сталкиваются с попытками как намеренной (сотрудники вступают в сговор со злоумышленниками), так и непреднамеренной "утечки" информации в периоды удаленной работы. Например, в связи с решением руководства оптимизировать штат во время тяжелой пандемии сотрудник получает письмо от отдела кадров компании, якобы содержащее информацию об увольнении, и переходит по ссылке на зараженный файл, прикрепленный к письму, или на сайт, похищающий персональные данные. В некоторых случаях работнику предлагали узнать больше информации. От таких писем пострадали работники, чьи личные данные попали к третьим лицам, а также компании, подвергшиеся локальному или сетевому заражению. По данным Льва Матвеева, в первом полугодии 2020 года в разных регионах страны было зафиксировано 72 случая утечки персональных данных лиц, зараженных или подозреваемых в заражении вирусом COVID-19. Также был зафиксирован случай взлома базы данных с результатами анализов пациентов онкологической клиники, за расшифровку которой мошенники потребовали выкуп в размере 80 000 рублей. Защита персональных данных является

первоочередной задачей, и необходимо принять меры по предотвращению их хищения. Успешное решение этих задач невозможно без сочетания мер и методов защиты информации.

Важно понимать, что эффективное применение законов о защите безопасности требует не только знания нормативной базы, но и ее практического использования в реальных сценариях. Организации и государственные учреждения должны уделять должное внимание соблюдению законов, внедрению соответствующих политик и процедур, а также обучению персонала по вопросам информационной безопасности. Только путем совместных усилий общества, законодателей и бизнес-сообщества можно обеспечить надежную защиту информации, повысить осведомленность о киберугрозах и действенно противодействовать потенциальным угрозам для информационной безопасности. Внедрение современных технологий, обучение персонала и постоянное совершенствование правовых норм являются важными шагами на пути к обеспечению безопасного цифрового окружения для всех участников общества.

МЕЖДУНАРОДНОЕ ЗАКОНОДАТЕЛЬСТВО

Оставаясь верной своей репутации первопроходца в области защиты прав личности, Калифорния стала первым штатом, принявшим закон, обязывающий компании защищать конфиденциальность персональных данных потребителей. Но Калифорния больше не одинока. Колорадо, Коннектикут, Юта и Вирджиния приняли аналогичные законы, которые вступили в силу в 2023 году. Во Флориде, Монтане, Орегоне и Техасе новые законы о защите персональных данных вступят в силу в 2024 году. В штатах Делавэр, Айова, Нью-Джерси и Теннесси приняты законы, которые дают компаниям время до 2025 года соблюдать их. Закон штата Индиана о защите персональных данных вступает в силу в 2026 году. Для компаний, имеющих клиентов по всей территории США, эта сложная сеть законов о защите персональных данных создает юридические и операционные проблемы. Для компаний, чьи субъекты данных находятся за пределами США, ситуация становится еще сложнее. Общие правила Европейского союза по защите данных (GDPR) несколько шире и несколько уже государственных законов о конфиденциальности данных. Бразилия, Великобритания, Австралия, Объединенные Арабские Эмираты и Сингапур в основном придерживаются системы Европейского союза по защите персональных данных.

Калифорнийский закон о защите прав потребителей (CCPA) является первым законом о конфиденциальности в Соединенных Штатах, регулирующим сбор, управление и продажу личной информации пользователей веб-сайтов. Он предоставляет несколько прав на конфиденциальность для потребителей Калифорнии. Предприятия, регулируемые CCPA, будут иметь ряд обязательств

перед этими потребителями, включая раскрытие информации, Общий регламент по защите данных (GDPR), подобный потребительским правам субъекта данных (DSR), "отказ" для определенных передач данных и требование "согласие" для несовершеннолетних. CCPA применяется только к компаниям, которые занимаются бизнесом в Калифорнии и удовлетворяют одному или нескольким из следующих: (1) иметь валовой годовой доход более $ 25 млн, или (2) получить более 50% своего годового дохода от продажи Калифорнии личной информации потребителя, или (3) купить, продать или поделиться личной информацией более чем 50 000 калифорнийских потребителей ежегодно. CCPA вступил в силу 1 января 2020 года. Принудительное применение генеральным прокурором Калифорнии (AG) началось 1 июля 2020 года. Калифорнийская группа доступности применяет CCPA и имеет право выдавать штрафы за несоответствие. CCPA также предоставляет частное право на действия, которое ограничивается нарушениями данных. В соответствии с этим правом убытки могут составлять от 100 до 750 долларов США за каждый инцидент на потребителя. Кроме того, Генеральный прокурор Калифорнии может обеспечить выполнение CCPA в полной мере, наложив гражданско-правовые санкции в размере не более 2 500 долларов США за нарушение и 7 500 долларов США за преднамеренное нарушение закона.

Вторым законом о защите персональных данных в мировом уровне, как было упомянуто выше, является «Европейский союза по защите данных» (GDPR). GDPR - это закон ЕС, содержащий обязательные правила о том, как организации и компании должны использовать персональные данные в соответствии с принципами добросовестности. Обработка данных означает сбор, структурирование, систематизацию, использование, хранение, совместное использование, раскрытие, удаление и уничтожение данных. Каждая организация, обрабатывающая персональные данные (а это любая организация, имеющая сотрудников и клиентов), должна гарантировать, что используемые ею персональные данные соответствуют требованиям GDPR. Персональные данные - это ценность, двух мнений быть не может. Данные позволяют разрабатывать бизнес-модели, лучше понимать своих клиентов, проводить эффективные маркетинговые кампании и развивать свои продукты и услуги. Но, как и в случае со многими другими активами, необходимо ответственное использование, основанное на общих правилах. Последние несколько лет мы были свидетелями громких сообщений о взломах персональных данных и скандалах, связанных с Facebook, eBay, Equifax и Uber. Личная информация сотен миллионов людей (номера социального страхования, адреса, кредитные рейтинги и т.д.) была скомпрометирована. В GDPR не только четко указано, что персональные данные принадлежат частному лицу, но и предусмотрены

значительные штрафы для компаний, не соблюдающих правила. В Европе конфиденциальность и защита данных считаются жизненно важными составляющими устойчивой демократии. GDPR разработан для защиты этих требований и представляет собой усовершенствованную версию предыдущей директивы ЕС о защите данных.

В основе всех законов о защите персональных данных лежит обязательство определенных компаний, которые собирают персональные данные, сохранять конфиденциальность этих данных и позволять потребителям контролировать, кто имеет доступ к этим данным. Законы штатов в Соединенных Штатах обычно определяют персональные данные как любую информацию, которая может обоснованно идентифицировать – прямо или косвенно – физическое лицо или домохозяйство. Общий регламент ЕС, напротив, применяется только к информации, которая может идентифицировать физическое лицо.

В целом персональные данные включают:

- Имя
- Дата рождения
- Домашний почтовый адрес
- Номер домашнего телефона
- Личный адрес электронной почты
- Номер мобильного телефона
- Рабочий адрес
- Рабочий номер телефона
- Рабочий адрес электронной почты
- Файлы cookie и информация для отслеживания
- IP-адрес физического лица или семьи

Конфиденциальные персональные данные - это часть персональных данных. Законы штата о защите персональных данных предусматривают дополнительную защиту “конфиденциальных персональных данных”. В зависимости от штата, “конфиденциальные персональные данные” могут включать в себя:

- Номер социального страхования
- Номер паспорта
- Номер водительского удостоверения
- Точные данные о геолокации
- Биометрические данные
- Медицинские данные (известные в США как защищенная медицинская информация или PHI)
- Генетические данные
- Раса
- Этническое происхождение

- Сексуальная ориентация
- Гендерная идентичность
- Религиозная принадлежность
- Членство в профсоюзе
- Политическая принадлежность
- Иммиграционный статус или гражданство

Биометрические данные включают, например, отпечаток большого пальца или данные распознавания лиц для разблокировки телефона или открытия системы безопасности. Что касается конкретных штатов, то в законодательстве Калифорнии содержится самое широкое определение конфиденциальных персональных данных, поскольку оно включает все вышеперечисленные категории, а также информацию о дебетовом, кредитном или банковском счете в сочетании с кодом безопасности или паролем для этой учетной записи. Калифорнийский закон о защите прав потребителей (CCPA) с поправками, внесенными в него Калифорнийским законом о правах на неприкосновенность частной жизни (CPRA), послужил образцом для других законов штата о защите частной жизни. Большинство штатов последовали примеру Калифорнии, хотя есть и исключения, связанные с обработкой определенных типов персональных данных. Закон штата Техас о конфиденциальности и безопасности данных (TDPSA) специально исключает информацию о сексуальной активности или сексуальной ориентации человека из определения конфиденциальных персональных данных. Закон штата Айова о защите персональных данных – The Iowa Act, касающийся данных потребителей, – не включает членство в профсоюзах или политическую принадлежность в определение конфиденциальных персональных данных. То же самое относится к Теннесси в соответствии с Законом о защите информации штата Теннесси.

ЗАКОНОДАТЕЛЬСТВО УЗБЕКИСТАНА

В Узбекистане было принято два новых нормативно-правовых акта в области защиты персональных данных, которые вступают в силу 7 января 2023 года. Новые нормативные документы устанавливают новые требования, касающиеся уровней защиты персональных данных при их обработке, хранения биометрических и генетических данных на материальных носителях, хранения биометрических и генетических данных вне баз персональных данных. Закон Республики Узбекистан от 02.07.2019 г. №ЗРУ-547 «О персональных данных», Постановление Кабинета Министров Республики Узбекистан от 05.10.2022 г. № 570 «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных».

В соответствии со ст. 7 Закона о персональных данных, правительство Республики Узбекистан уполномочено устанавливать:

• уровни защищенности персональных данных при их обработке в зависимости от угроз безопасности;

• требования по обеспечению защиты персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

• требования к материальным носителям биометрических и генетических данных и технологиям хранения таких данных вне баз персональных данных.

Во исполнение вышеуказанных полномочий правительство приняло Постановление, в соответствии с которым утверждены два Положения:

1. Положение об определении уровней защищенности персональных данных при их обработке (далее «Положение №1»);

2. Положение о требованиях к материальным носителям биометрических и генетических данных и технологиям хранения таких данных вне баз персональных данных (далее «Положение №2»).

При этом следует отметить, что расходы, возникающие в связи с выполнением требований, предусмотренных в Положениях, осуществляются за счет собственных средств организаций, осуществляющих обработку персональных данных. Также Положение № 2 устанавливает требования к материальным носителям, содержащим биометрические и генетические данные. Прежде всего, такие материальные носители должны иметь маркировку «конфиденциально» или «для служебного пользования», а собственник и (или) оператор обязан вести учет таких материальных носителей. Положение № 2 также требует, чтобы при хранении биометрических и генетических данных в электронном виде эти данные были зашифрованы и защищены криптографическим или иным способом.

Кроме того, собственник и (или) оператор должны принимать соответствующие меры безопасности для предотвращения кражи, стирания, уничтожения, несанкционированного приобретения, изменения и бесконтрольного оставления материальных носителей, на которых записаны биометрические и генетические данные. При принятии таких мер биометрические и генетические данные должны:

• соответствовать требованиям пожарной безопасности, санитарным нормам, правилам и гигиеническим нормативам, а также быть гарантированными от затопления;

• иметь надежные средства защиты, исключающие доступ к ним посторонних лиц;

• храниться в сейфах, металлических полках или металлических стеллажах;

• храниться в помещениях, оборудованных охранной сигнализацией и устройствами видеонаблюдения, входные двери и окна которых подключены к службе охраны.

Материальный носитель должен использоваться в течение срока, установленного собственником и (или) оператором, осуществившим запись биометрических и генетических данных на материальный носитель, но не более срока эксплуатации, установленного изготовителем материального носителя. При удалении персональных данных с материальных носителей, на которых зафиксированы биометрические и генетические данные, списание этих материальных носителей не производится. Не списанные материальные носители могут быть повторно использованы для целей обработки персональных данных в будущем, за исключением материальных носителей, предназначенных для одноразового использования и пришедших в негодность. Такие материальные носители уничтожаются в установленном порядке.

Согласно Положению № 2, при хранении биометрических и генетических данных вне баз персональных данных должны соблюдаться следующие условия:

- доступ к персональным данным, хранящимся на материальном носителе, для уполномоченных лиц собственника и (или) оператора;
- использование средств электронной подписи или иных информационных технологий, позволяющих сохранять целостность и неизменность биометрических и генетических данных, записанных на материальном носителе;
- проверка наличия письменного согласия субъекта на обработку биометрических и генетических данных или иных оснований для обработки биометрических и генетических данных, предусмотренных законодательством.

Собственник и (или) оператор вправе устанавливать дополнительные требования, не противоречащие требованиям законодательства, к технологиям хранения биометрических и генетических данных вне баз персональных данных, в зависимости от методов и средств защиты таких данных в базах данных этого собственника и (или) оператора.

ЗАКЛЮЧЕНИЕ

В конце, делая выводы важно понимать, что эффективное применение законов о защите безопасности требует не только знания нормативной базы, но и ее практического использования в реальных сценариях. Организации и государственные учреждения должны уделять должное внимание соблюдению законов, внедрению соответствующих политик и процедур, а также обучению персонала по вопросам информационной безопасности. Только путем совместных усилий общества, законодателей и бизнес-сообщества можно обеспечить надежную защиту информации, повысить осведомленность о киберугрозах и действенно противодействовать потенциальным угрозам для информационной безопасности. Внедрение современных технологий, обучение персонала и постоянное совершенствование правовых норм являются важными

шагами на пути к обеспечению безопасного цифрового окружения для всех участников общества.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. https://www.gdprsummary.com/gdpr-summary/
2. ЗРУ «О персональных данных»
3. Постановление Кабинета Министров Республики Узбекистан от 05.10.2022 г. № 570 «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных».
4. https:/www.axiomlaw.com/blog/data-privacy-law
5. https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-1/viewer