5Лазарев В.В. Общая теория права и государства: учебник / В.В. Лазарев. — 3-е изд., перераб. и доп. - М.: Юристь, 2001. - 620 с.

6Сильченко Н.В. Роль и место понятия «типология» в понятийном аппарате общей теории государства и права // Право и правотворчество: вопросы теории. - М.: Изд-во ИГиП АН СССР, 1982. - С. 55-63.

7Рожкова Л.П. Принципы и методы типологии государства и права / Л.П. Рожкова. - Саратов: Изд-во Сарат. гос. ун-та, 1984. - 144 с.

8Каган М.С. Системное рассмотрение основных способов группировки // Философские и социологические исследования. - Л., 1977. – 129 с.

9Сапарғалиев Ғ.С., Ибраева А.С. Мемлекет және құқық теориясы: оқулық. – Алматы: Фолиант баспасы, 2011. – 360 б.

10 Бекин А.В. Тип современного Российского государства и права. - Краснодар, 2009. - 233 с.

11 Жоламан Қ.Д. Мемлекет және құқық теориясы:. – Алматы: Нұр-пресс, 2005. – 295 б.

12 Лазарев В.В. Теория государства и права: учебник для вузов / В.В. Лазарев, / С.В. Липень. - 2-е изд., испр. и доп. - М.: Спарк, 2000. - 511 с.

13 Головистикова А.Н. Проблемы теории государства и права: учебник / Н.Головистикова, Ю.А. Дмитриев. - М.: Эксмо, 2005. - 320 с.

14 Чиркин В.Е. Современное государство. - М.: Междунар. отношения, 2001. — 416 с.

15 Синенко Ю.С. Типология государства: автореф. дис. ... канд. юрид. наук. -Москва, 2007. – 25 с.

*Толеубек А.А.*
*студент-магистрант Высшей школы права, по специальности международное право, Университета MNU, г. Астана*

## НЕКОТОРЫЕ АСПЕКТЫ СБОРА, ОБРАБОТКИ И СРОКОВ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОНТЕКСТЕ ПЕРСПЕКТИВ ИМПЛЕМЕНТАЦИИ ТРЕБОВАНИЙ GDPR В ЗАКОНОДАТЕЛЬСТВО КАЗАХСТАНА

**Аннотация:** Одним из основных прав человека и гражданина, закрепленных в Конституции Республики Казахстан и международных правовых документах, является право на уважение частной жизни. Данная статья посвящена сравнительно правовому анализу двух законодательных актов, регулирующих защиту персональных данных в Европейском союзе и Республике Казахстан, а именно рассматриваются аспекты сбора, обработки и сроков хранения персональных данных в контексте планируемой имплементации требований GDPR в законодательства Казахстана. Проводится анализ, текущий ситуации, связанной с защитой персональных данных в ЕС и РК, а также предлагаются рекомендации по улучшению законодательных актов.

***Ключевые слова:*** *персональные данные; сроки хранения персональных данных; сбор и обработка персональных данных; регламент GDPR; закон РК «О персональных данных и их защите»; право на частную жизнь; права человека; право на защиту персональных данных.*

В современной эпохе цифровые технологии продолжают свое развитие, играя ключевую роль в модернизации экономики, образа жизни людей, научных исследований, образования, здравоохранения, государственного управления и многих других областях. Например, цифровые технологии улучшают бизнес-процессы, расширяют доступ в сеть и коммуникационные возможности, предоставляют онлайн-образование, а также развивают телемедицину и электронные медицинские карты в сфере здравоохранения. Кроме того, цифровые технологии способствуют цифровизации государственных сервисов и развитию электронного правительства. Однако с развитием цифровой эпохи возрастает важность проблемы защиты персональных данных. Каждый год объем личной информации,

собираемой, обрабатываемой и хранимой организациями и государственными учреждениями, увеличивается в геометрической прогрессии. Этот рост вызывает серьезные тревоги во многих странах по поводу обеспечения безопасности миллионов людей от незаконного использования их личных данных в преступных или недобросовестных целях.

В результате, национальные и международные законы и стандарты обработки персональных данных стали ключевыми аспектами защиты человеческих прав и приватности в цифровой эре. Соответствующие механизмы контроля и защиты в настоящее время интегрированы в современный правовой порядок, направленный на обеспечение безопасности личных данных граждан. В условиях стремительного развития информационных технологий концепция защиты частной жизни выросла в ключевой аспект прав человека.

Институт защиты персональных данных, зародившийся в XIX веке, активно регулирует обработку личной информации, включая биометрические данные, хранящиеся в удостоверяющих личность документах, используемых в государственном управлении. В Казахстане эти принципы также отражены в законодательстве, где «Комитет по информации и коммуникациям» играет ключевую роль в защите персональных данных, обеспечивая их законность и конфиденциальность. Тем не менее, внедрение подобных систем вызывает споры, в связи с принципами конституционной неприкосновенности частной жизни.

**Основные источники права**

Регламент Европейского Парламента и Совета Европейского Союза 2016/679 был принят 27 апреля 2016 года и вступил в силу 25 мая 2018 года. Этот правовой акт, также известный как Общий Регламент о защите персональных данных (GDPR), является ключевым нормативным документом, регулирующим обработку персональных данных физических лиц в рамках Европейского союза и Европейского экономического пространства. Извините за предыдущие ошибки, и спасибо за ваше терпение.

Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года регулирует сбор, обработку и защиту персональных данных в Казахстане, устанавливая правила для субъектов данных, операторов и уполномоченного органа. Этот закон направлен на обеспечение прав и свобод граждан в контексте обработки их персональных данных.

Конституция Республики Казахстан — основной закон Казахстана. Действующая Конституция Республики Казахстан была принята на всенародном референдуме 30 августа 1995 года. Конституция утверждает человека, его жизнь и права как высшую ценность государства, что включает защиту персональных данных как составной части прав и свобод граждан (ст.1). Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства (ст.18).

Международный Пакт о гражданских и политических правах был ратифицирован 28 ноября 2005 году Казахстаном. Статья 17. 1. определяет основные положения, связанные с правом на частную жизнь. Персональные данные в контексте этого Пакта тесно связаны с правом на неприкосновенность частной жизни, что подчеркивает важность защиты личной информации.

**Сравнительный анализ правовых норм в области персональных данных.**

**Сходство основных положений GDPR и законодательства Республики Казахстан по защите персональных данных.**

Анализ двух основных нормативных актов, регулирующих защиту персональных данных, позволяет выявить их сходство в ряде ключевых принципов. Одним из таких принципов является минимизация данных, которая закреплена в статье 5 GDPR. Этот принцип обязывает ограничивать объем собираемых персональных данных строго рамками, необходимыми для достижения четко определенных и конкретных целей обработки. Это означает, что контролеры данных обязаны тщательно оценивать объем собираемой информации, исключая любые данные, которые не являются критически важными для заявленных целей. Данный подход направлен на минимизацию рисков избыточного сбора,

обработки и хранения персональных данных, что, в свою очередь, способствует защите конфиденциальности субъектов данных.

Аналогичные требования закреплены в законодательстве Республики Казахстан. В частности, статья 7, пункт 8, Закона «О персональных данных и их защите» устанавливает, что сбор и обработка персональных данных допускаются исключительно в пределах, необходимых для достижения заявленных целей. Это положение подчеркивает важность соответствия объема собираемых данных целям обработки и исключает возможность использования персональной информации в неоправданно широких или нецелевых масштабах. Законодательство Казахстана также требует документального фиксирования целей обработки данных, что позволяет дополнительно контролировать соблюдение принципа минимизации.

Второе сходство заключается в требовании прозрачности процесса обработки данных. Прозрачность обработки персональных данных является одним из ключевых принципов, закрепленных как в GDPR, так и в законодательстве Республики Казахстан. GDPR, в статье 5, предусматривает, что обработка данных должна осуществляться с учетом принципа прозрачности. Это означает, что субъекты данных имеют право быть полностью информированными о том, как и с какой целью обрабатываются их персональные данные. В частности, субъектам должны быть предоставлены четкие и доступные сведения о целях обработки, правовом основании, категориях собираемых данных, сроках хранения и лицах, которым данные могут быть переданы. Также предусмотрено, что информация должна быть представлена в простой и понятной форме, исключающей возможность неоднозначного толкования.

Законодательство Республики Казахстан закрепляет аналогичный подход в статье 7 Закона «О персональных данных и их защите». Данный акт требует, чтобы субъекты персональных данных были своевременно и полно проинформированы о факте и целях обработки их данных. Цели обработки должны быть заранее определены и документально зафиксированы, а информация о них должна быть доступна субъекту данных в понятной форме. Более того, закон Казахстана дополнительно обязывает контролеров данных обеспечить соблюдение прав субъектов, включая право на получение информации о передаче их данных третьим лицам и право на исправление, блокировку или уничтожение данных, если обработка ведется с нарушением закона.

Следующим сходством является требование получения согласия субъекта данных, которое играет ключевую роль в обоих нормативных актах, регулирующих защиту персональных данных. Согласно GDPR, обработка данных возможна только при наличии законного основания, одним из которых является явное согласие субъекта данных. Этот принцип закреплен в статье 6 GDPR, а более детально его требования раскрыты в статье 7, где указано, что согласие должно быть добровольным, конкретным, информированным и недвусмысленным. Это означает, что субъект данных должен быть четко проинформирован о целях обработки, а его согласие выражено в явной форме, например, путем подписания документа или подтверждения в электронном виде. Также важно, что субъект данных имеет право отозвать свое согласие в любой момент, и этот отзыв должен быть столь же простым, как и предоставление согласия.

В законодательстве Республики Казахстан аналогичные требования к согласию субъекта данных содержатся в статье 8 Закона «О персональных данных и их защите». Здесь указано, что обработка персональных данных допускается только с согласия субъекта данных, за исключением случаев, предусмотренных законом. Согласие может быть выражено как в письменной, так и в иной форме, позволяющей зафиксировать факт его предоставления. Также законодательство Казахстана уточняет, что субъект данных имеет право отозвать свое согласие, если иное не предусмотрено законодательными актами.

Последним, но не менее важным сходством является регулирование сроков хранения персональных данных, которое занимает значительное место в обоих нормативных актах, направленных на их защиту. В соответствии с GDPR, принцип ограничения сроков хранения

данных закреплен в статье 5, где указано, что персональные данные должны храниться только до тех пор, пока это необходимо для достижения целей, ради которых они обрабатываются. После достижения этих целей данные подлежат удалению или анонимизации, если иное не предусмотрено законодательством. GDPR также подчеркивает, что контролеры данных обязаны устанавливать четкие временные рамки для хранения данных, а также регулярно пересматривать их актуальность, чтобы избежать избыточного накопления.

В законодательстве Республики Казахстан аналогичные положения содержатся в статье 7, пункте 8, и статье 24, пункте 1, Закона «О персональных данных и их защите». В них указано, что персональные данные могут храниться только в течение срока, необходимого для достижения целей обработки. После достижения этих целей данные должны быть уничтожены, если иное не предусмотрено законодательством. Кроме того, казахстанское законодательство обращает внимание на необходимость учета срока хранения в рамках соответствующих договоров, соглашений или других документов, регулирующих обработку данных.

Таким образом, анализ основных положений GDPR и законодательства Республики Казахстан в области защиты персональных данных показывает их значительное сходство в подходах к регулированию обработки данных. Оба акта подчеркивают важность принципов минимизации, прозрачности, получения согласия субъектов данных и ограничения сроков хранения. Эти общие принципы направлены на обеспечение баланса между эффективной обработкой данных и защитой прав субъектов, способствуя укреплению их доверия к обработчикам данных. Несмотря на определенные различия в деталях, законодательство Казахстана демонстрирует стремление следовать международным стандартам в области защиты персональных данных, что подтверждает его современность и соответствие глобальным трендам.

**Нерегулируемые положения, связанные с защитой персональных данных в РК и ЕС.**

**Отсутствия сроков хранения.**

В законодательстве о защите персональных данных Республики Казахстан и в GDPR существует общий недочет – отсутствие четких временных рамок для хранения информации. Неоднозначность в определении сроков хранения персональных данных может привести к разночтениям и различным интерпретациям правил организациями и контролирующими органами. Это может создать неопределенность в понимании требований и нормативов, что потенциально повлияет на охрану данных и их удаление.

В общем, как в GDPR, так и в казахстанском законе утверждаются общие принципы, требующие хранения персональных данных только в течение того периода, который необходим для целей обработки данных. В случае GDPR существует прецедентная практика, компенсирующая неопределенность законодательства. В свою очередь, отечественная система работает иначе, и этот неопределенный статус нормативов затрудняет и ухудшает правоприменительную практику и создает сложности при определении оптимальных периодов хранения данных.

К примеру, дело «Google против Испании» ярко иллюстрирует аспекты, связанные с сроками хранения данных. В 2014 году Марио Костеха Гонсалес обратился с запросом к Google о удалении информации из поисковой выдачи, касающейся его финансовых трудностей. Конфликт, возникший вокруг этого случая, связан с несовершенством правовых механизмов обеспечения безопасности обработки персональных данных в интернете. Судебное решение по данному делу подчеркнуло, что граждане ЕС имеют право требовать удаления своих персональных данных из поисковых систем, если эти данные устарели или перестали быть актуальными. Важно отметить, что дело «Google против Испании» выразило особое внимание к соблюдению принципов сроков хранения, предусмотренных в GDPR, вынесением решения в пользу гражданина ЕС - Марио Костеха Гонсалеса, предоставив право требовать удаления устаревших или неактуальных персональных данных из

поисковых систем. Также данный прецедент обязал поисковые сервисы, такие как «Google», соблюдать установленные сроки хранения данных, подчеркивая важность соблюдения GDPR в отношении обработки и хранения персональных данных.[1]

Также данная проблема хорошо освещается в деле «Гохран против Соединенного Королевства». Заявитель был задержан за вождение в нетрезвом виде в Северной Ирландии. В этот день у властей были взяты его биометрические данные, включая отпечатки пальцев и образец ДНК. Заявитель потребовал уничтожения или возврата своих данных, что было отклонено. Высший суд Северной Ирландии и Верховный суд Великобритании признали вмешательство в права заявителя, но считали это оправданным и соразмерным, поскольку вождение автомобиля с избыточным потреблением алкоголя является серьезным преступлением. По данному решению ЕСПЧ отметил, что долгосрочное хранение биометрических данных после задержания было несоразмерным и нарушало стандарты, установленные в Конвенции о защите прав человека и основных свобод.[2] Решение выражает важность соблюдения принципов демократии, обеспечения контроля и возможности обжалования решений при сборе и хранении подобных данных. Оно указывает на необходимость справедливого баланса между интересами государства и правами частных лиц в контексте минорных правонарушений. Решение ЕСПЧ представляет собой важный прецедент, укрепляющий права граждан в сфере сбора, сроков хранения и использования их биометрических данных в контексте уголовных дел.

Резюмируя, хочется отметить, что представленная неопределенность в установлении сроков хранения персональных данных в законодательстве Республики Казахстан может стать источником разногласий и разночтений между организациями и контролирующими органами. Эти разногласия, в свою очередь, могут оказать влияние на безопасность хранения и удаление данных. В случае с Европейским союзом данная неопределенность в установлении временных рамок является менее критичной проблемой, поскольку в ЕС развита прецедентная практика, которая может частично устранить нечеткость законодательства, связанные с его интерпретацией, и снизить потенциальные негативные последствия.

**Отсутствие «нормы» в сроках хранения**

Страны Европейского союза имеют возможность адаптировать регламент GDPR под свои национальные законы. Так, например, Германия, в качестве члена ЕС, обязана внедрять и следовать GDPR, но также она может видоизменять и внедрять некую конкретику для более лучшей адаптации регламента GDPR в национальное законодательство. Тем самым, Германия внедрив определенные национальные адаптации в пределах общего регламента установила сроки хранения данных, разделив их по категориям и специфике отрасли. Такие сроки могут меняться в зависимости от обстоятельств и требований отрасли, что предоставляет более конкретные и гибкие правила. Так, например, банковские и бухгалтерские документы могут храниться до 10 лет, деловые письма до 6 лет, медицинские записи от 10 до 30 лет, трудовые документы могут храниться после окончания рабочих отношений до 6 лет.[3]

Возможность стран-участниц адаптировать регламент GDPR под себя представляет собой гибкость в реализации стандартов в соответствии с особенностями своего национального законодательства. Это может включать в себя уточнения или дополнения к общим правилам, чтобы лучше соответствовать местным условиям, культуре и законодательным особенностям страны. Такие адаптации позволяют балансировать общеевропейские стандарты с уникальными потребностями каждой страны. В свою очередь, отсутствие конкретных указаний в казахстанском законе относительно сроков хранения персональных данных может создать неопределенность для организаций при определении оптимальных сроков хранения данных и вызвать споры.

**Неэффективность политики конфиденциальности**

Политика конфиденциальности неразрывно связана с аспектами сбора, обработки и сроков хранения персональных данных, поскольку определяет правила и обязательства,

которые организации, компании, носители информации и операторы должны соблюдать при работе с персональными данными. Она предназначена для того, чтобы защитить права и конфиденциальность индивида, а также для предотвращения неправомерного использования данных, путем установления стандартов и обязательств. Политика конфиденциальности обеспечивает честное, законное и безопасное обращение с личной информацией. В целом, она служит гарантией, что персональные данные будут использоваться в соответствии с законом и с уважением к правам каждого человека.

Несмотря на вышеперечисленное, персональные данные, такие как местоположение, интересы, и даже личные фотографии, становятся легкодоступными в виртуальном пространстве. Это создает среду, где злоумышленники могут злоупотреблять чувствительной информацией для мошенничества, фишинга и других видов кибератак. Интернет может хранить на вашем компьютере невидимые файлы, называемые «cookie», чтобы отслеживать вашу активность. Эти файлы позволяют владельцам сайтов собирать вашу информацию, а также анализировать содержимое вашего компьютера, что соответственно нарушает право пользователей на частную жизнь и приватность. [4]

В целом, опираясь на законодательные акты можно определить, что нарушение безопасности персональных данных определяется как «событие, приводящее к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению или доступу к передаваемым, хранимым или обрабатываемым персональным данным».[5] Это подразумевает, что угроза безопасности предшествует посягательству на данные, вызывая негативные события.

Самые громкие дела, связанные с нарушением персональных данных в результате кибератак, при отсутствии достаточных технических и организационных мер по обеспечению информационной безопасности, были рассмотрены Управлением комиссара по информации Соединенного Королевства (ICO) в отношении компаний British Airways. Так, например, случай с «British Airways», данный инцидент произошел в сентябре 2018 года. Инцидент заключался, в частности, в перенаправлении трафика пользователей с сайта British Airways на мошеннический сайт, через который мошенники собирали данные клиентов. В результате инцидента была скомпрометирована личная информация примерно 500 000 клиентов. Расследование, проведенное регулирующим органом, показало, что из-за плохой системы безопасности компании была скомпрометирована различная информация, включая данные для входа в систему, информацию о платежных картах и бронировании путешествий, а также имя и адрес. British Airways сотрудничала со следствием и улучшила свои меры безопасности, но компания была оштрафована на 204 600 000 евро за нарушение статьи 32 GDPR о безопасности обработки персональных данных.[6]

Также стоит отметить, что в законе РК «О персональных данных и их защите» закреплены только основные требования по обеспечению конфиденциальности персональных данных. Закон РК не содержит конкретных требований уведомления государственных органов или клиентов об утечках данных, за исключением случаев, когда утечка касается персональных данных ограниченного доступа или является критичной для общественных объектов информационно-коммуникационной инфраструктуры. В таких случаях собственники соответствующих объектов информируют техническую службу государства. Некоторые важные вопросы, касающиеся обеспечения конфиденциальности персональных данных, так и остаются неурегулированными. Данные утверждения можем подкрепить новостными порталами и заголовками к ним.

Так, например, в феврале 2020 году произошла утечка данных из баз генпрокуратуры РК. О том, что данные, которые находятся в базе Генеральной прокуратуры Казахстана, стали доступны для пользователей Сети, сообщили специалисты ЦАРКА на новостном журнале «zakon.kz». Согласно сообщению ЦАРКА, «утечка охватывает данные всех граждан Казахстана и иностранцев, по которым когда-либо проводилось административное делопроизводство. Система в настоящее время передает в Интернет разнообразную информацию, включая штрафы, предупреждения, адреса проживания, фотографии

нарушителей, номера автомобилей, данные из техпаспортов, информацию о владельцах имущества и многое другое. Особенно беспокойным является то, что доступ к системе позволяет не только получать данные, но и редактировать их, удалять или создавать фиктивные дела. Это создает серьезную угрозу для конфиденциальности и безопасности личной информации граждан».[7]

Рассмотрим следующий случай, Центр анализа и расследования кибератак («**ЦАРКА**») получил сообщение от анонима, который утверждал, что конфиденциальная информация «сотен тысяч пациентов» из сети клиник стала доступной публично.[8] Данные казахстанских пациентов, зарегистрированных в приложении «Damumed», были скомпрометированы. Представители Центра информационных технологий «Даму» подтвердили передачу данных третьим лицам от лица с легальным доступом в систему Damumed. Аналитики ЦАРКА считают, что утечка произошла из-за элементарной ошибки – несанкционированного доступа к медицинским документам организации.

Резюмируя хочется отметить, что регламент GDPR более эффективно работает в части в вопросе о конфиденциальности данных по сравнению с законом РК о защите персональных данных. В целом, GDPR устанавливает высокие стандарты и обеспечивает защиту прав и свобод граждан, требуя от организаций доказать адекватность принимаемых мер безопасности. Такой подход способствует повышению кибербезопасности, снижению рисков и защите конфиденциальности личной информации. Кроме того, GDPR предусматривает штрафы за нарушения, что стимулирует компании активнее следовать стандартам и регулярно улучшать свои меры безопасности. В свою очередь, в Казахстане необходимо ужесточить систему санкций за нарушение и невыполнение требований законодательства о персональных данных, поскольку ужесточение законодательства может стать серьезным стимулом для компаний и самого населения к соблюдению требований по защите персональных данных. В противном случае конфиденциальность и права человека на частную жизнь могут быть нарушены при обработке, сборе и хранении информации по вине персонала компании и самой компании, а значит, могут стать серьезным инцидентом информационной безопасности, который может привести к непоправимому ущербу и многочисленным рискам как для компании, так и для человека. А также Казахстану необходимо перенять опыт Европейского союза в информировании граждан о кибербезопасности. Сотрудничество правительства и общества в повышении осведомленности граждан о цифровых правах и защите персональных данных будет способствовать улучшению общей безопасности информационных ресурсов.

Также хочу отметить идею о том, что необходимо использовать не только правовые, но и компьютерно-технические способы защиты информации. Использование технических методов, таких как «кибертуман», для защиты конфиденциальной информации является эффективным подходом. Суть «кибертумана» заключается в разбиении секретной информации на фрагменты, которые затем распределяются по различным серверам и устройствам конечных пользователей. Этот подход увеличивает уровень безопасности, поскольку даже в случае взлома одной части данных злоумышленнику не удается получить доступ ко всей информации. Такой метод снижает риски преступных действий, усложняя доступ к конфиденциальной информации.[9]

В контексте обеих юрисдикций, а именно Республики Казахстан и Европейского Союза, можно выделить позитивные правовые инициативы, направленные на обеспечение безопасного сбора, обработки и хранения персональных данных. В процессе сравнительного анализа законодательных актов были выявлены схожие положения, различия и некоторые недостатки. Оба правовых документа подчеркивают важность ограничения периода хранения данных, получения согласия субъектов на их обработку, а также информирования субъектов о целях обработки, что соответствует принципу минимизации данных.

Тем не менее, выявлены определенные недостатки, такие как нечеткость и неопределенность сроков хранения персональных данных, отсутствие четких «норм» сроков хранения данных и неэффективность политики конфиденциальности, включая низкий

уровень санкций за нарушение. Важно также отметить, что отсутствие ежегодных отчетов от Министерства цифрового развития и аэрокосмической промышленности (МЦРИАП) мешает предоставлению ясной картины ситуации в стране по утечкам персональных данных. Эта неопределенность может затруднить предвидение и управление потенциальными проблемами и вызовами.

Введение и хранение персональных данных в цифровой среде представляют значительные вызовы, требующие усилий в сфере законодательства и регулирования. В этом контексте опыт Европейского союза может оказать влияние на модернизацию законодательства о персональных данных, так как предложение внести изменения, устанавливая нормы хранения персональных данных в зависимости от категории данных и отрасли, представляется неотъемлемым для предотвращения неконтролируемого сбора и хранения данных. Отсутствие четких норм и прозрачных политик может привести к разногласиям и недопониманиям между организациями и контролирующими органами, что усложняет процессы соблюдения законодательства. Неопределенные сроки хранения данных, в свою очередь, могут стать источником уязвимостей в системах безопасности, вызывая недостаточное внимание к обеспечению безопасности хранимой информации. Такие действия направлены на улучшение эффективности законодательства и обеспечение баланса между безопасностью и прозрачностью в сфере обработки персональных данных.

Казахстану необходимо извлечь уроки из международного опыта, особенно в сфере разработки политики конфиденциальности. На данный момент законодательство РК не регулирует аспекты, связанные с обязанностью уведомления государственных органов или клиентов о случаях утечек данных, за исключением ситуаций, когда утечка касается персональных данных с ограниченным доступом или представляет серьезную угрозу для общественных объектов. Изучение опыта Европейского союза в информировании граждан об информационной кибербезопасности представляется особенно значимым. Общественное внимание и образование играют ключевую роль в обеспечении кибербезопасности, поскольку осведомленные граждане способствуют повышению уровня защиты персональных данных. Эффективное взаимодействие правительства и общественности в области повышения осведомленности граждан о цифровых правах и защите персональных данных будет способствовать улучшению уровня безопасности данных. Помимо этого, Казахстану необходимо ужесточить систему санкций за нарушение и невыполнение требований законодательства о персональных данных, поскольку ужесточение законодательства может стать серьезным стимулом для компаний и самого населения к соблюдению требований по защите персональных данных.

**Список литературы:**

1. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»

2. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // OJ. L 119. Vol. 59. 4 May 2016. P. 1–88

3. Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (с изменениями и дополнениями по состоянию на 19.09.2022 г.)

4. Kalis, S. M. (2014). Google spain sl, google inc. v. agencia espanola de proteccion de datos, mario costeja gonzalez: An entitlement to erasure and its endlenss effects. *Tul. J. Int'l & Comp. L.*, *23*, 589.

5. Application No. 45245/15, Gaughran v. The United Kingdom, Judgment of 13 February 2020.

6. Overview of the retention periods of business records. — Text: electronic // Hermann Schwelling Maschinenbau (HSM). URL: http://surl.li/pgarc

7. Tsesis, A. (2014). The right to erasure: Privacy, data brokers, and the indefinite retention of data. Wake Forest L. Rev., 49, 433.

8. The list and summary of the imposed GDPR fines. https://www.enforcementtracker.com/. Accessed 10 Sept 2020

9. Zakon.kz казахстанское интернет-издание. (2020, февраль 14). Обнаружена утечка данных из базы Генпрокуратуры РК.

10. TengriNews. (2019 июля 09). Утечка данных тысяч пациентов произошла в Казахстане.

11. Бегларян, М. Е., & Мамакаев, Х. В. (2017). Кибератаки и законодательство РФ. Право и практика, (2), стр. 49-56.

12. Martínez-Martínez, D. F. (2018). Unification of personal data protection in the European Union: Challenges and implications. Profesional de la Informacion, 27(1), 185-194.

13. Овчинникова, Е. А. (2022). Сравнительный анализ законодательства в области защиты персональных данных в Российской Федерации и Евросоюзе. Интерэкспо Гео-Сибирь, 8(2), 113-117.

14. Кудашкин, Я. В. (2019). Правовое обеспечение безопасности обработки персональных данных в сети Интернет (Doctoral dissertation, дис. канд. юрид. наук).

*Трофимчук К. А.*
*Карагандинский университет имени академика Е.А. Букетова. юридический факультет, магистрант 2 курса*
*(Научный руководитель - Ахметова Н.С., к.ю.н., профессор, Карагандинский университет имени академика Е.А. Букетова, Юридический факультет)*

## ЦИФРОВИЗАЦИЯ, КАК ПРИНЦИП ДЕБЮРОКРАТИЗАЦИИ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВЕННОГО АППАРАТА

Тема цифровизации как принципа дебюрократизации деятельности государственного аппарата в Казахстане и мире становится все более актуальной. В условиях ускоряющегося технологического прогресса и глобализации, традиционные бюрократические механизмы госуправления часто оказываются неэффективными. Цифровизация является одним из инструментов, способствующих упрощению и повышению прозрачности процессов внутри государственного аппарата.

Цифровизация, стала неотъемлемым процессом во всех сферах деятельности государства, в том числе и в судебной системе. За минувшие 9 лет реализовано достаточно большое количество цифровых проектов. Рассмотрим некоторые из них.

В Республике Казахстан с 2015 года функционирует Единый реестр досудебных расследований, информационная платформа которого позволяет в электронном формате проводить учет информации об уголовных правонарушениях и уголовных делах, а также вести досудебное расследование в электронном формате, дистанционно осуществлять ведомственный контроль и прокурорский надзор. Данная информационная система интегрирована с базой данных органов прокуратуры «Қадағалау», а также с информационной платформой судей «Төрелік», что позволяет с момента регистрации информации об уголовных правонарушениях в органах уголовного преследования проводить досудебное расследование, прокурорский надзор и судебное производство в электронном формате.

Потребность в получении быстрой и качественной судебной информации по рассмотренным делам, результатам и срокам разрешения жалоб и заявлений поступающих в суды, и по многим другим вопросам побудила Верховный Суд к разработке новой информационной системы «Төрелік» . Ее внедрение позволило обеспечить оперативный доступ к обмену информационными данными, закрепив высокой степенью надежности, и