ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ
AL-FARABI KAZAKH NATIONAL UNIVERSITY

ЭКОНОМИКА ЖӘНЕ БИЗНЕС ЖОҒАРЫ МЕКТЕБІ
ВЫСШАЯ ШКОЛА ЭКОНОМИКИ И БИЗНЕСА
HIGHER SCHOOL OF ECONOMICS AND BUSINESS

ХАЛЫҚАРАЛЫҚ ҚАТЫНАСТАР ФАКУЛЬТЕТІ
ФАКУЛЬТЕТ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ
DEPARTMENT OF INTERNATIONAL RELATIONS

«ФАРАБИ ӘЛЕМІ»

атты студенттер мен жас ғалымдардың халықаралық ғылыми конференция МАТЕРИАЛДАРЫ

Алматы, Қазақстан, 6-8 сәуір 2022 жыл

МАТЕРИАЛЫ

международной научной конференции студентов и молодых ученых «ФАРАБИ ӘЛЕМІ»

Алматы, Казахстан, 6-8 апреля 2022 года

MATERIALS

International Scientific Conference of Students and Young Scientists «FARABI ALEMI»

Almaty, Kazakhstan, April 6-8, 2022

Алматы, 2022

ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ
AL-FARABI KAZAKH NATIONAL UNIVERSITY

ХАЛЫҚАРАЛЫҚ ҚАТЫНАСТАР ФАКУЛЬТЕТІ
ФАКУЛЬТЕТ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ
DEPARTMENT OF INTERNATIONAL RELATIONS

«ФАРАБИ ӘЛЕМІ»

атты студенттер мен жас ғалымдардың халықаралық ғылыми конференция
МАТЕРИАЛДАРЫ
Алматы, Қазақстан, 2022 жылдың 6-8 сәуірі

МАТЕРИАЛЫ
международной конференции студентов и молодых учёных
«ФАРАБИ ӘЛЕМІ»
Алматы, Казахстан, 6-8 апреля 2022 года

MATERIALS
International Scientific Conference of Students and Young Scientists
«FARABI ALEMI»
Almaty, Kazakhstan, April 6-8, 2022

Алматы
«Қазақ университеті»
2022

В течение недели оба оценочных раунда были проведены на достаточно высоком уровне в которых приняли участие как уполномоченные лица центральных государственных органов, так и представители неправительственных организации и другие заинтересованные стороны.

Одним из первых рассмотренных вопросов ГРЕКО была фундаментальная основа противодействия коррупции в Казахстане, включающее в себя антикоррупционное законодательство страны и эффективность ее реализации, функциональные компетенции государственных органов, институтов развития, правовых норм защиты источников информации и другие вопросы.

Следует отметить, что для проведения данного мероприятия Казахстан проделал достаточно большой путь, в результате которой 15 октября 2019 года в Страсбурге было подписано Соглашение между Республикой Казахстан и Советом Европы в отношении привилегий и иммунитетов представителей Группы государств против коррупции и членов оценочных групп. Законом Республики Казахстан от 30 декабря 2019 года №299-VI данное Соглашение было ратифицировано, таким образом Республика Казахстан официально стала 50 страной-участницей этого объединения.

Как отметил исполнительный секретарь ГРЕКО г-н Джанлука Эспозито, «Подписание Казахстаном Соглашения с ГРЕКО является очень важным событием, приближающим Казахстан на шаг ближе к тому, чтобы стать полноценным членом ГРЕКО, одной из самых развитых антикоррупционных организации в мире».

Сотрудничество Казахстана с ГРЕКО демонстрирует приверженность страны фундаментальным принципам Совета Европы и намерения совершенствовать свои национальные антикоррупционные меры. При этом стратегической задачей Казахстана является ратификация Конвенции «Об уголовной ответственности за коррупцию», которая позволит компетентным органам страны на другом правовом уровне развивать сотрудничество по широкому кругу вопросов, включающие в себя оказание правовой помощи, экстрадиции преступников и возврата похищенных активов из-за рубежа.

Достижение стратегических целей позволит Казахстану на международном уровне обеспечить собственную экономическую и национальную безопасность, поскольку ГРЕКО фокусируется на целостности государственного сектора, а ее члены соглашаются на процесс общей оценки и на коллективное давление в целях совершенствования их способности бороться с коррупцией.

Как было отмечено выше, на проведенных в сентябре прошлого года раундах мониторинга, со стороны ГРЕКО было изучено антикоррупционное законодательство страны на предмет соответствия европейским стандартам и эффективность проводимой антикоррупционной политики в целом. По результатам данного аудита ГРЕКО в настоящее время вырабатываются индивидуальные рекомендации для Казахстана. Однако, изучая международный опыт ГРЕКО по мониторингу антикоррупционной политики других государств, можно предположить, что их универсальные требования, так или иначе, войдут в основу соответствующей рекомендации и для Казахстана.

В данном случае, к этим рекомендациям относятся прежде всего проведение государством всестороннего исследования проблем коррупции для выявления системных рисков как в государственном, так и в частном секторе.

При этом очевидно будут рекомендованы комплекс мероприятий, направленные на принятие необходимых законодательных и практических мер для усиления независимости судебной системы, функциональной автономии правоохранительных органов, непосредственно отвечающих за противодействие коррупции с целью их правовой защиты от неправомерного вмешательства в их деятельность.

Также, не без внимания останется вопрос проработки и принятия законодательных мер, усиливающих прозрачность деятельности государственного аппарата и вовлечения в его орбиту представителей общественности для проведения консультации по тем или иным вопросам с целью консолидированного принятия решения.

Исходя из специфики требований Совета Европы, следует полагать, что одним из краеугольных аспектов для Казахстана станет вопрос совершенствования действующего законодательства страны, направленной на реформирование системы предупреждения и выявления конфликта интересов.

Проблемы коррупции в сфере государственных закупок, скорее всего, будут вновь подняты для принятия по ним дополнительных эффективных законодательных мер, включая усиление контроля государства при регистрации юридических лиц с созданием реестра конечных бенефициаров. Кроме того, вполне возможна имплементация международной практики введения законодательных ограничений на занятие руководящих должностей в юридических лицах, осужденных за тяжкие коррупционные преступления. Здесь же следует акцентировать внимание на вопрос уголовной ответственности юридических лиц за коррупционные правонарушения и принятия по ним соответствующих санкции.

Ответственность государственных служащих и приравненных к ним лиц за совершение коррупционных правонарушений также будет отнесен к центральным вопросам рекомендации ГРЕКО. Здесь непременно будут затронуты вопросы ежегодной декларации активов, положения о их раскрытии и применения санкции в отношении лиц, намеренно скрывших от учета материальные активы и имущества. Совершенствование конкурсных процедур отбора и продвижения на государственной службе на принципах меритократии также не останется без внимания.

Таким образом, подводя итоги следует отметить, что визит мониторинговой группы ГРЕКО в Казахстан действительно носит исторический характер, поскольку после завершения всех мониторинговых процедур, уполномоченные органы страны начнут работу по совершенствованию антикоррупционного законодательства на совершенно другом правовом уровне, с учетом международных конвенции, передового опыта европейских государств и 20 основных принципов борьбы с коррупцией.

ФОРМА КОНТРОЛЯ, ЗАЩИТЫ И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЛОКАЛЬНЫХ НОРМАТИВНЫХ АКТАХ В РЕСПУБЛИКЕ КАЗАХСТАН

Бисалиев Марлен
PhD докторант 1-го курса специальности «Международное право»
КазНУ им. Аль-Фараби
Научный руководитель: д.ю.н., профессор Шакиров К.Н.

Введение

Для того, чтобы получить доступ ко многим услугам и преимуществам общества, пользователям и работникам все чаще требуется предоставлять данные о персональной информации. Однако, неверное обращение или нарушение регламента процесса обработки персональных данных нередко ведут к растущему беспокойству по данному вопросу среди населения, да и общества в целом.

Обеспокоенность по поводу рисков нарушения конфиденциальности при обработке персональных данных, примером которой может служить потеря двух дисков с подробной информацией о пособиях на 25 миллионов детей правительством Соединенного Королевства, становится все более распространенной [1], и пользователи ищут более эффективные способы контролировать свои личные данные, которые используются другими индивидами, домохозяйствами, организациями и государственными учреждениями.

Характер ответов на эту проблем варьируется от таких технологических мер, как шифрование, до средств правовой защиты и изменения деловой практики. Этот характер в значительной степени определяется концепцией конфиденциальности, встречающейся в

литературе. Концепцию создают формирующие контексты, которые ограничивают способы понимания проблемы и, следовательно, доступные методы для ее решения.

В последние годы растет понимание того, что предоставление пользователям контроля над своими личными данными является важным аспектом для поддержания доверия к кибер-среде.

В этом тезисе используются такие понятия как «согласие» (англ. — consent) и, что немаловажно, отзыв данного «согласия» как основы для нового понимания контроля над персональными данными. Это понимание открывает возможности для повышения доверия к субъектам предпринимательства, трудовой деятельности и государственного надзора, решая некоторые из основных существующих проблем информационной конфиденциальности.

Теоретическое обоснование

Среди положений нормативных правовых актов, содержащих общепризнанные нормы и принципы международного права, определяющие права и принципы регулирования отношений в киберсреде, следует назвать в первую очередь нормы статьи 19 Всеобщей декларации прав человека 1948 года [2], а также нормы статьи 19 и статьи 20 Международного пакта о гражданских и политических правах 1966 года [3]. Становится проблематично контролировать данные, когда они распределены в разных структурных подразделениях и субъектах исследовательской и предпринимательской деятельности: медицинские данные пациента находятся в информационных системах медицинского учреждения, исследовательские системы в другом структурном подразделении или даже в другой стране.

Многие ученые считают, что право на неприкосновенность частной жизни имеет внутреннюю ценность как право человека, что неразрывно связано с сущностью человека. Например, Лукас Интрона рассматривает гипотетический случай полностью прозрачного общества (то есть отсутствия конфиденциальности) [4]. Однако, концепция и манифест такого общества были описаны в работе Питера Лудлоу только в 2001 году [5]. В работе отмечалось, что такое общество берет свое начало еще с 1990-х годов о неком «кибер-государстве».

Анализируя характеристики источников международного права в сфере кибербезопасности, отдельные ученые полагают, что речь о праве кибербезопасности как о самостоятельном институте международного информационного права, а объекты защиты (персональные данные) должны обеспечиваться не только нормативными правовыми актами, но и техническими и управленческими методами [6].

Контроль или форма контроля в контексте данной статьи рассматривается как что-то, что происходит в начале процесса раскрытия информации, а контроль конфиденциальности рассматривается исключительно с точки зрения ограничения того, какие личные данные становятся доступными для других. Однако, на практике это довольно частичное представление о том, как личные данные раскрываются и передаются другим лицам.

Субъекты сети Интернет все чаще регистрируются в различных онлайн-сервисах и раскрывают данные о себе (фамилия, имя, адрес электронной почты и проч.). Эти данные затем хранятся в частных и государственных базах данных в течение значительного периода времени и могут быть переданы другим структурным подразделениям предприятий или выбранным сторонним организациям, в том числе и государственным.

Согласие на обработку персональных данных, вероятно, является наиболее важным механизмом, существующим в настоящее время для определения того, как и когда эти данные могут быть использованы. Понятие информированного согласия возникло в контексте медицинских исследований и разработки Нюрнбергского кодекса 1947 года, который четко установил право отказаться от медицинских исследований на любой стадии, фактически аннулируя любое данное или подразумеваемое согласие согласно статье 9 кодекса [7].

Как было продемонстрировано выше, хотя широко понимается, что контроль играет важную роль в отношении вопросов конфиденциальности и согласия, концептуализация контроля обычно ограничена. То есть во многих исследованиях контроль рассматривается как нечто большее, чем принципы справедливой обработки информации: уведомление, выбор и доступ в сочетании, в лучшем случае, с возможностью выбора или выхода из маркетинговых списков. Хотя это и понятно, учитывая системы на базе мэйнфреймов, существовавшие в 1950-х и 1960-х годах, это становится несколько ограниченным, учитывая диапазон и гибкость современных компьютерных систем, в которых все чаще выходят на первый план понятия ориентированности на пользователя. Пользователи все чаще могут создавать свою собственную нормативную среду и управлять ею [8]. Например, они могут платить за использование инструментов без шпионского программного обеспечения вместо использования бесплатных пакетов, управляемых шпионским программным обеспечением [9], и таким же образом ожидают большего контроля над тем, как используются их личные данные.

Беспокойства к требованиям обработки персональных данных могут возникнуть по разным причинам. Они могут быть вызваны изменениями на рынке, например, когда компания, на которую пользователи ранее дали свое согласие, выкупается конкурентом или когда компания решает переместить свой центр обработки данных за границу. Беспокойства также могут быть вызваны повышением осведомленности о рисках защиты данных после громких утечек данных. Они также могут быть вызваны раскрытием неожиданных подробностей о вторичном использовании данных, например, когда медицинская исследовательская компания обнаруживает, что она использует медицинские данные для исследований, финансируемых фармацевтическими компаниями. Изменения в согласии могут произойти после получения нежелательных / неожиданных маркетинговых материалов (нежелательной почты и спама) или просто по прихоти пользователя (субъекта).

Дискуссия

Существуют проблемы с обеспечением того, чтобы предпочтения в отношении предоставления и отзыва согласия владельцев персональной информации были связаны с личными данными, к которым они относятся, как в пределах так и за пределами организации. В частности, это касается отмены права на использование определенных элементов персональных данных для определенных целей. Например, отмена права на использование медицинских данных в исследовательских целях определенной организацией требует, чтобы предпочтение отзыва было связано с медицинскими данными, включая подробную информацию о том, какие организации могут либо не могут их использовать, а также обеспечение того, что, если данные будут переданы третьей стороне, эти предпочтения могут оставаться за ней.

«Липкие политики» (англ. — sticky policies) представляют собой один из подходов к улучшению контроля владельцев над своими данными. При таком подходе к данным прикрепляются машиночитаемые политики. Их называют «липкими», поскольку они перемещаются вместе с данными, поскольку данные перемещаются по нескольким информационным системам. Например, если информационная система передает медицинские данные пациента из больницы в исследовательское учреждение, а затем в исследовательскую группу, информация может быть в форме, в которой определенные атрибуты, такие как медицинские результаты или персональная информация, должны быть зашифрованы в части возможности идентификации пациента и его места жительства.

Использование криптографически поддерживаемых «липких политик» и стандартов совместимости изучается как возможные решения проблем обмена данных между предприятиями, поскольку предпочтения в отношении отзыва согласия могут изменяться со временем, и тем не менее в рамках любого крупного предприятия использование и расположение данных, вероятно, будет рассредоточено по нескольким, распределенные

системы. Следовательно, контроль возникает и для отзыва, но контроль в этом контексте — это инженерная концепция, а не желательный атрибут.

Таким образом, вопросы качества контроля обработки персональных данных выходят на первый план, поскольку возможно предложить и реализовать различные формы контроля отзыва согласия с разной степенью и глубиной проверяемости. Как следствие, контроль становится многогранным и организации могут выбирать из ряда различных уровней отзыва, привязанных к степени обновления системы, в котором они работают. Точно так же, как при разработке программного обеспечения используется модель зрелости возможностей (англ. — Capability Maturity Model) для оценки зрелости процессов при разработке программного обеспечения, где субъекты могут выбрать взаимодействие с теми организациями, чей «уровень зрелости» является высоким на рынке.

Возвращаясь к законодательству Республики Казахстан, Закон РК от 21 мая 2013 года № 94-V «О персональных данных» устанавливает, что в компетенцию Уполномоченного органа входит, в том числе, рассмотрение обращений субъектов персональных данных (их законных представителей), принятие мер по привлечению нарушителей к ответственности, право требовать от владельцев, операторов и третьих лиц разъяснений, блокирование или уничтожение неточных или незаконно полученных личных данных. В Законе введено новое понятие: «служба защиты персональных данных». Посредством этой услуги будет обеспечиваться информационное взаимодействие между владельцами и / или операторами по обработке персональных данных. Это позволит организации предоставить (отозвать) согласие на сбор, обработку и / или передачу персональных данных третьим лицам. То есть такая услуга станет новой формой предоставления (отзыва) согласия в дополнение к тем формам, которые были предоставлены ранее.

В Законе также введено новое понятие «добровольное киберстрахование». Целью добровольного киберстрахования является компенсация имущественного ущерба, причиненного субъекту, собственнику, оператору и / или третьему лицу, в соответствии с законодательством о страховании и страховой деятельности. Виды, условия и порядок добровольного киберстрахования будут определены соглашением сторон.

Закон прямо устанавливает, что расходы, связанные с уничтожением персональных данных из общедоступных источников, будут нести владелец, оператор и / или третье лицо. Если уничтожение персональных данных из общедоступных источников является следствием отзыва согласия пользователя, то размер затрат, а также лица, которым будут при необходимости возмещены такие расходы, будут определены в судебном порядке.

Более того, 17 июля 2020 года вступила в силу поправка в статью 9 о «Сборе, обработке персональных данных без согласия субъекта». Она устанавливает, что сбор и обработка персональных данных будет осуществляться без согласия субъекта или его законного представителя в случае получения персональных данных органами государственных доходов для целей налогового администрирования и (или) для контроля информации от физических лиц и юридических лиц в соответствии с законами Республики Казахстан.

В качестве примера, возможно запрашивать данные в следующей форме:

1. Объем (перечень обрабатываемых персональных данных): фамилия, имя, отчество, пол, дата рождения, место рождения.

2. Цель обработки персональных данных с указанием ссылки на локальные, национальные и международные нормативные правовые акты (при необходимости):

1) обеспечение исполнения действующего законодательства и нормативных правовых актов РК;
2) передача данных в соответствии с положения государственного органа;
3) анализ интересов субъекта персональных данных;
4) взаимодействие с субъектом персональных данных;
5) осуществление аудио или видеозаписей в соответствии с субъектом деятельности;
6) идентификации личности субъекта.

3. Способы обработки персональных данных: сбор, запись, хранение, передача, обезличивание, шифрование, удаление, уничтожение.

4. Подпись (факт), подтверждающее согласие.

Права человека могут быть реализованы только в том случае, если это лицо идентифицируемо. Если запрос отправляется по почте, ответ должен быть отправлен заказным письмом, чтобы гарантировать, что отправитель запроса будет идентифицирован после получения письма с ответом.

Тогда остается проблема учета документов и согласий по данной форме для средних и крупных субъектов предпринимательства. Разумеется, такие данные возможно формализовать, а процесс информатизировать. Такой способ позволит ответственному работнику более эффективно управлять и обеспечивать надлежащую документацию в области защиты и обработки персональных данных в соответствии с локальными и национальными нормативными правовым актами.

В случае ненадлежащего использования, согласие пользователя может быть отозвано и оспорено в соответствии с действующим законодательством Республики Казахстан. В соответствии с законом о нормативных правовых актах, будет учитываться их иерархия.

Заключение

Правила предоставления и отзыва согласия пользователя предназначены для использования вместе с политикой безопасности и конфиденциальности предприятия. Тем самым они единообразно фиксируют предпочтения пользователей в их соблюдении. Они предназначены для согласования требований предприятий и требований пользователей, позволяя, с одной стороны, предприятиям определять, какой контроль предоставляется пользователям, а с другой – пользователям определять, что происходит с их личными данными и как они обрабатываются.

Согласно статье 11 Трудового кодекса Республики Казахстан от 23 ноября 2015 года № 414-V, работодатель издает акты в пределах своей компетенции в соответствии с настоящим кодексом и иными нормативными правовыми актами Республики Казахстан, трудовым договором, соглашениями, коллективным договором. Таким, образом, разработка, издание и контроль данного акта не противоречит трудовому законодательству, а более того, является дополнительным документом, который защищает права работодателя и позволяет в дальнейшем избежать трудовых споров и претензий со стороны работника организации.

Также возникают проблемы у «обработчика» персональных данных. В случае судебных разбирательств, обработчику будет крайне сложно доказать законность и назначения обработки персональных данных. Таким образом, разработки и обеспечение локальных нормативных актов организации крайне важна по следующим причинам:

- приведение в соответствие с национальным законодательством;
- разрешение при судебных разбирательствах;
- в процессе взаимодействия с государственными надзорными органами.

Особенно важно отметить статью 10 Гражданского процессуального кодекса Республики Казахстан от 13 октября 2015 года № 377-V — «Неприкосновенность частной жизни. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений».

Согласно пунктам 17, 18 Нормативного постановления Верховного Суда Республики Казахстан от 25 июня 2010 года № 4 «О судебной защите прав, свобод человека и гражданина в уголовном судопроизводстве», информация о частной жизни должна быть «собрана и обработана» без нарушения конституционных прав гражданина, в соответствии с Уголовным и Уголовно-процессуальным кодексом Республики Казахстан [10].

Так, по состоянию на декабрь 2021 года в Банке судебных актов [11] содержится 1 167 судебных дел по запросу «персональные данные» по гражданским делам, фабулы дел которых содержат нарушения и признаки нарушений законодательства Республики

Казахстан о персональных данных и их защите, более того, некоторые дела квалифицированы как уголовные преступления. Среднее количество процессов в год составляет 130 единиц, однако, с 2017 года тренд начинает быть отрицательным. Это может быть обусловлено усилением законодательства в области регулирования сбора и обработки персональных данных.

Список использованных источников:

1. Whitley EA (2009) Perceptions of government technology, surveillance and privacy: the UK identity cards scheme. In New Directions in Privacy and Surveillance (Neyland D and Goold B, Eds), pp 133-156, Willan, Cullompton.
2. Всеобщая декларация прав человека от 10 декабря 1948 года [Электронный ресурс]. — Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml
3. Международный пакт о гражданских и политических правах от 16 декабря 1966 года [Электронный ресурс]. — Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml
4. Introna LD (1997) Privacy and the computer: Why we need privacy in the information
2. society. Metaphilosophy 28(3), 259-275.
1. Ludlow, Peter, ed. Crypto anarchy, cyberstates, and pirate utopias. MITPress, 2001.
2. Бисалиев М.С., Шакиров К.Н. Вестник Карагандинского университета. Серия Право. 2021 (3). С. 15-25
3. The Nuremberg Code (1947) [Электронный ресурс]. Режим доступа: https://media.tghn.org/medialibrary/2011/04/BMJ_No_7070_Volume_313_The_Nuremberg_Code.pdf
4. Tsiavos P, Hosein IR and Whitley EA (2003) The footprint of regulation: How information
3. systems are affecting the sources of control in a global economy. In Organizational information
4. systems in the context of globalization (Korpela M, Montealegre R and Poulymenakou A, Eds),
5. pp 355-370, Kluwer, Athens, Greece.
1. Mlcakova A and Whitley EA (2004) Configuring peer–to–peer software: An empirical study
6. of how users react to the regulatory features of software. European Journal of Information Systems 13(2), 95-102.
1. Нормативное постановление Верховного Суда Республики Казахстан от 25 июня 2010 года № 4 «О судебной защите прав, свобод человека и гражданина в уголовном судопроизводстве». — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/P10000004S_
2. Банк судебных актов. Верховный Суд Республики Казахстан. — [Электронный ресурс]. — Режим доступа: https://sud.gov.kz/rus/court-acts

ТЕНДЕНЦИИ УНИФИКАЦИИ МЕЖДУНАРОДНОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ГЛОБАЛЬНОГО ЭКОЛОГИЧЕСКОГО УПРАВЛЕНИЯ-ГЛОБАЛЬНЫЙ ПАКТ ПО ОКРУЖАЮЩЕЙ СРЕДЕ: ПРОЕКТ МЕЖДУНАРОДНОГО СОГЛАШЕНИЯ

Фу Тин
Ph.D докторант 2-курса специальности «Международное право»
КазНУ имени аль-Фараби
Научный руководитель: доктор Ph.D., доцент Алтаева К. Ж.

Введение

Глобальные экологические проблемы нарастают день ото дня, а угрозы общественному здоровью, с которыми сталкивается человечество, становятся все более серьезными, однако международное экологическое право не может быть эффективно реализовано из-за фрагментарности. 24июня 2017г.Франция публично обнародовала текст «Управления-глобального пакта об окружающей среде (проект)» (GlobalPactfortheEnvironment, далее именуемый «Проект конвенции») в Сорбоннском