вета глав государств СНГ от 10 декабря 2010 года. URL: http://base.spinform.ru/show_doc.fwx?rgn=32926

17. Про оголошення Угод про співробітництво між МВС України та МВС інших держав: наказ МВС України від 06.05.1992, № 241. Архів ГУНП України в Донецькій області. Ф. 20, д. 3, т. 6, арк. 49–66.

18. Про оголошення документів про міжнародне співробітництво між МВС України та МВС інших держав: наказ МВС України від 09 черв. 1992 р., № 420. Архів ГУНП України в Донецькій області. Ф. 20, д. 3, т. 12, арк. 51.

19. Про оголошення Угоди про співробітництво між МВС України та Федеральним міністром Австрійської Республіки у боротьбі з незаконним оборотом наркотиків та організованою злочинністю: наказ МВС України від 30 вер. 1992 р., № 564. Архів ГУНП України в Донецькій області. Ф. 20, д. 3, т.17, арк. 37–40.

20. Про оголошення Протоколу зустрічі представників МВС України та МВС Республіки Італія: наказ МВС України від 24 бер. 1993 р., № 155. Архів ГУНП України в Донецькій області. Ф.20, д. 3. т. 3, арк. 201–204.

21. Угода між Україною та Європейським поліцейським офісом про стратегічне співробітництво від 04 груд. 2009 р. URL: http://zakon.rada.gov.ua/laws/show/984_001-16

22. Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про стратегічне співробітництво: Закон України від 05 жовт. 2010 р., № 2576-VI. URL: http://zakon. rada. gov. ua/go/2576-17

ИНФОРМАЦИЯ ОБ АВТОРЕ

Барановский Александр Витальевич – адвокат, аспирант кафедры общеправовых дисциплин Донецкого юридического института МВД Украины

INFORMATION ABOUT AUTHOR

Baranovskiy Aleksandr Vitalyevich – Lawyer, Postgraduate Student of the Department of General Legal Disciplines of the Donetsk Law Institute of the Ministry of Internal Affairs of Ukraine

ezoz@ukr.net

УДК 343.982.4

СРЕДСТВА БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ КАК СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДОКУМЕНТОВ, УДОСТОВЕРЯЮЩИХ ЛИЧНОСТЬ

Ирина БЕЛОУС,
заведующий отделом
Киевского научно-исследовательского института судебных экспертиз
Министерства юстиции Украины

АННОТАЦИЯ

В статье проводится теоретическое исследование, направленное на изучение перспектив использования биометрических технологий для усовершенствования системы безопасности документов, а также обеспечения достоверной и быстрой идентификации личности. Осуществляется анализ научной, технической и юридической литературы, посвящённой проблемам защиты документов, удостоверяющих личность, а также использования для этого биометрических технологий. Раскрываются этапы процесса биометрической идентификации и основные понятия, связанные с ним. На основе проведённого исследования делается вывод о том, что использование биометрических технологий обеспечивает достоверную идентификацию и верификацию владельцев документов, удостоверяющих личность, а также является эффективным средством защиты документов от подделки.

Ключевые слова: национальная безопасность, биометрические технологии, идентификация, верификация, документ, удостоверяющий личность.

BIOMETRIC IDENTIFICATION AND VERIFICATION MEASURES AS THE MODERN TECHNOLOGIES OF PROTECTION OF IDENTIFICATION DOCUMENTS

Irina BELOUS,
Head of the Department of the Kiev Scientific Research Institute
of Forensic Expertise of the Ministry of Justice of Ukraine

SUMMARY

The article presents a theoretical study aimed at exploring the prospects for the use of biometric technologies for improving the security of documents, as well as ensuring reliable and rapid identity. The analysis of scientific and technical literature dealing with the protection of identity documents and the use of biometric technologies. The stages of the biometric identification process and the basic concepts associated with it are revealed. Based on the study, it is concluded that the use of biometric technologies provides for the reliable identification and verification of identity holders, as well as effective means of protecting documents against forgery.

Key words: national security, biometric technologies, identification, verification, identity document.

Постановка проблемы. Угроза для безопасности стран и их граждан, связанная с международным терроризмом, незаконной иммиграцией и торговлей людьми, а также другими транснациональными преступлениями подняла проблему усовершенствования защиты документов, удостоверяющих личность, на новый уровень.

Ввиду того, что несовершенная система защиты документов, удостоверяющих личность, в течение многих лет способствовала формированию большого количества способов их фальсификации, наступила необходимость разработки новых стандартов безопасности.

Актуальность темы. Для обеспечения международной и национальной безопасности с целью противодействия подделке, мошенничеству и неправомерному использованию персональных данных

владельцев документов, удостоверяющих личность, каждое государство постоянно осуществляет мероприятия, связанные с совершенствованием степени защиты их бланков в соответствии с современными требованиями их безопасности.

Основной целью обеспечения безопасности при удостоверении личности является достоверная идентификация личности, или аутентификация – подтверждение того, что человек является тем, за кого себя выдаёт.

Поэтому перспективным направлением для усовершенствования системы безопасности документов и обеспечения достоверной и быстрой идентификации личности на сегодняшний день является использование биометрических технологий.

Целью и задачей статьи является анализ теоретических и практических вопросов введения для обеспечения защиты документов, удостоверяющих личность, биометрических технологий, а также оценки их эффективности для проведения достоверной идентификации.

Состояние исследования. В последние годы проблемам биометрии и использованию её технологий для защиты документов, удостоверяющих личность, уделяется особое внимание в технической литературе. Это работы таких исследователей, как: Б.В. Аристархова, В.С. Барсукова, В.И. Волчихина, А.А. Гинца, А.В. Зайцева, А.И. Иванова, А.Ф. Стеблевой, И.Н. Спиридонова, М.А. Хебайши и др. В юридической литературе широко освещены вопросы идентификации человека по отдельным биометрическим данным – отпечаткам пальцев и внешним признакам. Метод идентификации человека на основании дактилоскопической информации был описан ещё в 1895 году известным английским учёным-антропологом Ф. Гальтоном. Метод идентификации личности по узорам сетчатки глаза впервые предложен в 1924 г. венским криминалистом доктором Тюркелем. Среди современных учёных-криминалистов следует отметить работы: Г.А. Беляевой, В.К. Башкатова, Е.В. Давыдова, Р.Е. Деминой, А.И. Железнякова, А.М. Зинина, Н.А. Иванова, В.Е. Ляпичева, Н.П. Майлис, Т.Ф. Моисеевой, И.Г. Маландина, С.Л. Мельника. В Украине вопросам криминалистического исследования документов, удостоверяющих личность, в разное время уделяли внимание: Р.С. Бєлкин, А.И. Винберг, О.В. Воробей, А.В. Ищенко, О.Л. Кобилянський, В.К. Лисиченко, Д.Я. Мирський, С.Д. Павленко, В.М. Палий, Л.Л. Патык, О.О. Сахарова, Є.В. Стариков, М.Я. Сегай, Л.В. Тальянчук, Л.О. Чередниченко, Т.Б. Черткова, Е.В. Шведова, О.Р. Шляхов, Л.П. Щербаковская, В.Ю. Шепитько. Однако вопросы обеспечения защиты документов, удостоверяющих личность, на основе использования биометрических технологий следует отнести к числу недостаточно изученных.

Изложение основного материала. Прежде всего следует обратиться к предпосылкам введения биометрических технологий в систему защиты документов, удостоверяющих личность.

Особо острым вопрос национальной безопасности и необходимости разработки новых стандартов безопасности документов, удостоверяющих личность, стал после трагических событий 11 сентября 2001 в Соединённых Штатах Америки. Учреждённый Комитет Совета Безопасности ООН своей резолюцией 1373 (2001) от 28 сентября 2001 года «О борьбе с терроризмом» постановил, что государства должны «предотвращать передвижение террористов или террористических групп с помощью эффективного пограничного контроля и контроля за выдачей документов, удостоверяющих личность, и проездных документов, а также с помощью мер предупреждения фальсификации, подделки или незаконного использования документов, удостоверяющих личность, и проездных документов» [1].

Международным сообществом функции унификации, разработки регламентов и новых стандартов документов, удостоверяющих личность, были возложены на Международную организацию гражданской авиации (ІКАО).

С учётом этого консультативная группа авиатранспортного комитета Совета ИКАО (TAG/MRTD) по новым техническим технологиям приступила к проведению оценки различных вариантов для обеспечения максимально возможного уровня безопасности использования документов, удостоверяющих личность.

На заседании Европейского Совета, которое состоялось в городе Салоники 19 и 20 июня 2003 года, было принято решение о необходимости выработать в пределах Европейского Союза последовательный подход, касающийся идентификаторов или биометрических данных для документов граждан из третьих стран, паспортов граждан Союза и систем информации (VIS и SIS II).

Согласно решению Европейского Совета, в паспорт или проездной документ должны быть интегрированы биометрические идентификаторы для установления надёжной связи между законным владельцем паспорта и собственно документом. Гармонизация элементов защиты и интеграция биометрических идентификаторов является значительным шагом в направлении использования новых элементов в перспективе дальнейших разработок на европейском уровне, что делает более безопасными проездные документы и устанавливает более надёжную связь между идентификационным документом и его владельцем с целью значительного содействия защите документа от мошеннического использования.

Паспорта и проездные документы должны содержать носитель информации с высоким уровнем защиты, на котором будет размещаться фотография лица. Государства-члены добавляют два отпечатка пальцев, сохранённые в функционально совместимом формате. Данные обеспечиваются защитой, а носитель информации обеспечивается достаточной ёмкостью и пригодностью гарантировать целостность, аутентичность и конфиденциальность данных [2].

В 2003 году Группа TAG/MRTD официально представила ИКАО рекомендацию, которая была принята и одобрена в качестве рабочего плана ИКАО.

Согласно данным рекомендациям было принято решении о том, что:

– всеобщим биометрическим параметром должно быть изображение лица в виде фотографии с высоким разрешением, хранящейся на бесконтактной интегральной микросхеме, отвечающей стандарту ИСО/МЭК 14443;

– вспомогательными биометрическими параметрами, хранящимися в виде изображений, будут отпечаток пальца и узор радужной оболочки глаза;

– биометрические параметры, дубликат данных машиносчитываемой зоны и целый ряд других данных должны храниться на бесконтактной интегральной схеме в соответствии с логической структурой данных и предохранятся от несанкционированного изменения путём использования специально приспособленной инфраструктуры открытых ключей (PKI).

На основании решения Европейского Совета были приняты рекомендации, которые предусматривали:

– выбор технологии распознавания черт лица для использования во всём мире с целью машинного подтверждения личности;

– использование бесконтактной интегральной микросхемы с минимальным объёмом памяти 32 Кбайт как средства хранения электронных данных, в том числе и биометрических, в проездном документе;

– программирование интегральных схем с использованием команд, которые прописаны в установленной логической структуре данных (ЛСД);

– использование изменяемой схемы инфраструктуры открытых ключей (PKI) для применения электронно-цифровых подписей с целью защиты электронных данных от несанкционированного изменения.

В 2004 году был разработан Регламент Совета (ЕС) №2252 / 2004 от 13 декабря «О введении стандартов для элементов защиты и биометрических элементов, включённых в паспорта и проездные документы, выданные государствами-членами». Данный регламент устанавливает минимальные уровни защиты, которым должны соответствовать выданные государствами-членами паспорта и проездные документы, а также является обязательным во всех его составляющих и имеет прямое применение на территории государств-членов в соответствии с Договором об основании Европейского сообщества [2].

Более подробно стоит раскрыть процесс биометрической идентификации и основные понятия, связанные с ним.

Биометрическая идентификация – это способ распознавания человека по физиологическим или поведенческим критериям, который используется для авторизации и аутентификации личности. В процессе биометрической идентификации уникальность личности определяется посредством измерения определённых физических и поведенческих свойств и получения образца измерений (называемого также «живой образец») в стандартном формате данных. Этот образец сравнивается с эталоном (также называемым подписью), который получен измерением тех же параметров, признан уникальным идентификатором личности и сохранен в базе данных. Близкое сходство образца и эталона означает подтверждение подлинности личности. Основное внимание в этом процессе уделяется небольшому числу физических характеристик, по уникальности которых можно идентифицировать личность.

В контексте биометрической идентификации употребляются следующие термины: «верифицировать», т.е. производить проверку на совпадение «один к одному» между представленными биометрическими данными, полученными от владельца машиносчитываемого документа в настоящий момент, и биометрическим шаблоном, созданным при занесении владельца в систему;

«идентифицировать», т.е. производить поиск по принципу «один ко многим», сопоставляя представленные биометрические данные с коллекцией шаблонов, представляющих всех субъектов, занесённых в систему. При выполнении функции идентификации биометрические параметры могут использоваться для повышения качества проверки анкетных данных в рамках процесса рассмотрения заявлений о выдаче паспорта, визы или иного проездного документа. При выполнении функции верификации они могут использоваться для установления точного соответствия между документом и лицом, предъявляющим его [3].

Биометрическая идентификация позволяет надёжно устанавливать личность человека путём быстрого сравнения по принципу «человек –документ» или по принципу «человек – база данных» [4 с. 165].

Существующие в настоящее время технологии биометрической идентификации делятся на две группы: статические и динамические.

Статические технологии основаны на анализе неизменных физиологических характеристик человека. В число этих характеристик входят: отпечатки пальцев, форма и геометрия лица, форма и строение черепа, сетчатка глаза, радужная оболочка глаза, геометрия ладони, кисти руки или пальца, термография лица, термография руки, рисунок вен на ладони или пальцев руки, ДНК, запах тела, форма уха.

Динамические методы идентификации основываются на анализе поведенческих характеристик личности – особенностей, присущих каждому человеку в процессе воспроизведения какого-либо действия. Динамические методы существенно уступают статическим в точности и эффективности и, как правило, используются в качестве вспомогательных. В качестве идентификаторов используются: динамика подписи, динамика клавиатурного набора, голос, движение губ, походка, особенности выполнения рукописных объектов.

Применение всех биометрических технологий включает четыре основных этапа:

1) регистрация идентификатора – сведения о физиологической или поведенческой характеристике преобразуются в форму, доступную компьютерным технологиям, и вносятся в память биометрической системы;

2) выделение – из вновь предъявленного идентификатора выделяются уникальные признаки, анализируемые системой;

3) сравнение – сопоставляются сведения о вновь предъявленном и ранее зарегистрированном идентификаторе;

4) решение – выносится заключение о том, совпадают или не совпадают вновь предъявленный и ранее зарегистрированный идентификатор. Заключение о совпадении/несовпадении идентификаторов может затем транслироваться другим системам контроля, которые далее действуют на основе полученной информации.

Сравнение биометрических идентификаторов может осуществляться в двух режимах. При идентификации сравнение идёт в режиме «один ко многим» (1:N): вновь предъявленный идентификатор сравнивается со всеми ранее зарегистрированными. Можно сказать, что в режиме идентификации биометрическая система ищет ответ на вопрос: «Кто Вы?», анализируя весь перечень идентификаторов, сведения о которых были зарегистрированы ранее. При верификации сравниваются сведения о двух конкретных идентификаторах (режим «один к одному», или 1:1). Примером служит сравнение сведений о вновь предъявленном идентификаторе со сведениями, записанными в память специальной карты, при этом, разумеется, необходимо предъявлять и биометрический идентификатор, и карточку. В данном случае формируется ответ на вопрос: «Вы действительно тот, за кого себя выдаёте?»

Системы, действующие в режиме верификации, как правило, являются полностью автоматическими (т.е. принимают решение без участия человека). Системы, действующие в режиме идентификации, также могут быть автоматизированными (формируется перечень возможных «кандидатов» на совпадение с вновь предъявленным идентификатором,

расположенных по мере убывания вероятности совпадения, и окончательное решение принимает оператор системы). Для ускорения распознавания пользователю может быть предложено применение дополнительного идентификатора. В этом случае в режиме идентификации производится сравнение не со всем списком, а только с его частью, выделяемой в соответствии с введённым дополнительным идентификатором [5].

При всём многообразии биометрических методов на практике в основном используются три: распознавание по отпечатку пальца, по изображению лица (двухмерному или трехмерному – 2D- или 3D-фото) и по радужной оболочке глаза. Однако любой из них основан на сопоставлении данных идентифицируемого объекта и биометрического эталона. Такое сопоставление невозможно без записи и сохранения биометрической информации. Основными инструментами автоматизированного биометрического метода являются сканер для измерения биометрической характеристики и алгоритм, позволяющий сравнить её с предварительно зарегистрированной той же характеристикой (так называемым биометрическим шаблоном). «Биометрический шаблон» является автоматически закодированным представлением черты, созданной программно-реализованным алгоритмом; он позволяет производить сравнения (проверки на совпадение) с определённой степенью уверенности в том, что отдельно записанные черты идентифицируют (или не идентифицируют) одного и того же человека [3].

Процесс биометрической идентификации владельца документа, удостоверяющего личность, состоит из следующих этапов:

1) Установление подлинности личности – несомненное удостоверение подлинности личности зарегистрированного пользователя.

2) Захват – получение исходного биометрического образца. Процесс занесения в биометрическую систему состоит в захвате исходного биометрического образца. Он используется для взятия биометрических образцов у каждого нового лица (потенциального владельца электронного документа) в целях создания нового шаблона для хранения. Данный процесс захвата – это автоматическое получение биометрического параметра при помощи таких устройств, как дактилоскопический сканер, сканер для фотографий, цифровая камера прямой съёмки или камера, изменяющая масштаб живого изображения радужной оболочки глаза. Для процесса захвата с помощью каждого снимающего устройства должны быть установлены определённые критерии и правила (например, обращение лицом к камере – стандартная поза при съёмке для целей распознавания черт лица; каким образом – нажатием или перекатыванием – следует снимать отпечатки пальцев; глаза должны быть полностью открыты для фиксирования радужной оболочки глаза). Полученное в результате изображение сжимается и затем сохраняется для идентификации личности в будущем.

3) Извлечение – преобразование исходных данных биометрического образца в промежуточную форму.

4) Создание шаблона – преобразование промежуточных данных в шаблон. В процессе создания шаблона сохраняются отличительные и повторяющиеся характеристики взятого биометрического образца, и он обычно осуществляется с помощью собственного программно реализованного алгоритма получения шаблона из хранимого изображения. Это позволяет формировать изображение таким образом, чтобы впоследствии его можно было сравнить с другим образцом изображения, захваченного в тот момент, когда необходимо подтверждать подлинность личности и дать сравнительную оценку степени совпадения.

Неотъемлемым элементом этого алгоритма является контроль качества, благодаря которому посредством определённого механизма оценивается качество образца. Стандарты качества должны быть максимально высокими, так как все будущие проверки будут зависеть от качества первоначально зафиксированного изображения. Если качество является неудовлетворительным, процесс захвата следует повторить.

5) Сравнение – сопоставление с информацией в хранящемся контрольном шаблоне.

В процессе идентификации используются шаблоны, полученные на основе новых образцов, и сравниваются с шаблонами зарегистрированных конечных пользователей с целью определить, был ли конечный пользователь ранее зарегистрирован в системе, если да, является ли он одним и тем же лицом [3].

В процессе верификации используются новые образцы владельца электронного документа, удостоверяющего личность, и сравниваются с ранее записанными шаблонами этого владельца с целью определить, является ли данный владелец одним и тем же лицом.

Для обеспечения более надёжной проверки лица, предъявившего документ, базовая информация, а также биометрические данные владельца документа вносятся на встроенный электронный носитель, что позволяет идентифицировать человека и делает невозможным использование документа другим лицом.

В сфере обеспечения надёжной автоматизированной идентификации личности наиболее точными и функционально совместимыми в глобальном масштабе считаются биометрическая идентификация по двухмерному изображению лица, а также отпечаткам пальцев.

Кроме высокой надёжности, в пользу этих двух способов биометрической аутентификации также свидетельствует возможность их использования практически в каждой стране. Ведь даже в случае отсутствия в той или иной стране базы данных по машиносчитываемым документам в качестве источника сравнительных образцов для верификации или идентификации их предъявителей могут выступать имеющиеся базы данных криминальной информации, в которых обычно содержатся как отпечатки пальцев, так и двухмерные изображения лица личностей, причастных к совершению правонарушений.

Особое значение в сфере применения технологий биометрической идентификации имеют соответствие и соблюдение международных стандартов: по отпечаткам пальцев – это стандарты: ICAO NTWG, NISTIR 6529 CBEFF, ISO/IEC FCD 19794-2, ISO/IEC 19794-4, ANSI/NIST-ITL 1-2000 Standard; в сфере биометрической аутентификации по двухмерным изображениям лица – ICAO NTWG та ISO/TEC FCD 19794-5.

Выводы. Вышеизложенное позволяет сделать вывод, что повышение уровня защиты документов, удостоверяющих личность, расширяет возможности для борьбы с транснациональными преступлениями и защищает общество от преступности. А использование биометрических технологий для идентификации и верификации владельцев документов, удостоверяющих личность, предоставляет неоспоримые преимущества по сравнении с другими способами. Биометрия обеспечивает наиболее надёжную и комплекс-

ную технологию из имеющихся в мире решений по аутентификации личности. Хранение биометрических идентификаторов на бесконтактной интегральной схеме как носителе информации в документах, удостоверяющих личность, способно гарантировать целостность, подлинность, конфиденциальность данных и обеспечивает высокий уровень идентификации и защиты, а также делает невозможным подделку документов.

Список использованной литературы:

1. Резолюция 1373 (2001) Совета Безопасности от 28 сентября 2001 г.: Документ ООН S/RES/1373 (2001), 2 октября 2001. URL: http://zakon2.rada.gov.ua/laws/show/995_854

2. Про запровадження стандартів для елементів захисту та біометричних елементів, включених в паспорти та проїзні документи, видані державами-членами: Регламент Ради (ЄС) № 2252/2004 від 13 грудня 2004 року. URL: https://minjust.gov.ua/m/str_45889

3. Применение средств биометрической идентификации и электронного хранения данных в МСПД. Doc 9303. Машиносчитываемые проездные документы. Издание 7. Часть 9. ИКАО, 2016. URL: http://www.icao.int3

4. Documentele de identitae si noile tehnologii ale elementelor de protective = Идентификационные документы и новые технологии элементов защиты: (îndrumar) / N. D. Gaibu, Gh. C. Cretu, T.V. Grosul,... Ch.: S. n., 2005 (Tipogr. Baçtina-RADOG). 268 p.

5. Передовые биометрические решения. URL: http://www.biolink.ru/technology/biometric.php

ИНФОРМАЦИЯ ОБ АВТОРЕ

Белоус Ирина Владимировна – заведующий отделом Киевского научно-исследовательского института судебных экспертиз Министерства юстиции Украины

INFORMATION ABOUT THE AUTHOR

Belous Irina Vladimirovna – Head of the Kyiv Institute of Forensic Examination Department of the Ministry of Justice of Ukraine

iraeksp@gmail.com

УДК 342.7

ПРАВА И ОБЯЗАННОСТИ ОБЩЕСТВЕННЫХ СОВЕТОВ ПРИ ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Александр ВИННИЦКИЙ,
соискатель
Научно-исследовательского института публичного права

АННОТАЦИЯ

Целью деятельности общественных советов при органах исполнительной власти является общий результат деятельности, нацеленной на содействие участия общественности в формировании и реализации государственной политики во всех сферах. Определено, что задача общественных советов при органах исполнительной власти – детализированные направления деятельности, которые раскрывают её сущностное содержание и приводят к желаемому результату. Права и обязанности общественных советов при органах исполнительной власти как элементы административно-правового статуса – это закреплённые нормативно-правовыми актами возможности и обязательства общественных советов при органах исполнительной власти по реализации поставленных законодателем перед этими органами целей и задач.

Ключевые слова: демократия, советы, государственное управление, публичная администрация, контроль за деятельностью государственных органов.

RIGHTS AND DUTIES OF PUBLIC COUNCILS UNDER EXECUTIVE POWER BODIES

Aleksandr VINNITSKIY,
Applicant of the Research Institute of Public Law

SUMMARY

The purpose of the activity of public councils under the executive authorities is the general result of the activity aimed at promoting the participation of the public in the formation and implementation of state policy in all spheres. It is determined that the task of public councils at the executive authorities is detailed directions of activity, revealing its essential content, and desired result. The rights and obligations of public councils in executive authorities as elements of administrative and legal status are the powers and obligations of public councils under the executive power bodies on the implementation of the goals and tasks set by the legislator before these normative legal acts.

Key words: democracy, councils, state administration, public administration, control over the activities of state bodies.

Постановка проблемы. Правоспособность индивидов возникает с момента рождения и прекращается с наступлением биологической смерти. Никто не может быть ограничен в правоспособности. Правоспособность организаций возникает с момента регистрации устава, положения в органах власти или с момента издания компетентным органом акта об их создании (если таковые действуют на основе общего положения о такого рода организации). Дееспособность – это предусмотренная нормами права способность личными действиями приобретать юридические права и обязанности. Дееспособность вводит в правосубъектность активный элемент, однако, как и правоспособность, является не врождённым свойством человека, а юридической категорией. Существует полная, неполная, частичная и ограниченная дееспособность. Полностью недееспособными по решению суда признаются лица, имеющие тяжёлые психические заболевания.

Актуальность темы исследования продиктована необходимостью усовершенствования системы прав и обязанностей общественных советов при органах исполнительной власти.

Состояние исследования. Отдельные вопросы общественного совета