ФУНКЦИОНАЛЬНЫЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. Е. ЖАТКАНБАЕВА,
заведующая кафедрой таможенного, финансового и экологического права КазНУ им. аль-Фараби, д.ю.н., профессор

В статье рассматриваются наиболее важные составляющие информационной безопасности. В частности раскрыты социальный, правовой, финансовый, экономический, военный, экологический и технический аспекты информационной безопасности как сложного социального явления.

Ключевые слова: безопасность, информационная безопасность, информационная среда, информационный сегмент рынка, информационная составляющая, информационный обмен.

Информационная безопасность является важным институтом личной, общественной и государственной жизни. Ее сущность просматривается посредством анализа различных аспектов информационной безопасности. Их многообразие позволяет понять разносторонность и специфику данного явления, роль и ценность обеспечения защиты информационного оборота в процессе жизнедеятельности человека, а также общественных и государственных образований.

Информационная безопасность имеет различные аспекты своего значения: социальный; нормативно-правовой; экономический; финансовый; военный; экологический; программно-технический.

Социальный аспект информационной безопасности представляет собой сложный сегмент. Неоднократно отмечалось, что информация играет важное значение в жизни социума. Ее значимость является разносторонней, начиная с необходимости наличия информации и заканчивая тем, что в информационном секторе работает достаточно большая часть населения. Так, в экономически развитых обществах примерно 2% населения заняты в сельском хозяйстве, 12% в промышленном секторе (переработка вещества и выпуск продукции), 70% – в информационной сфере. В Казахстане цифра работников информационного сектора гораздо ниже – 25% (сельском хозяйстве – 46%, остальные – в промышленном). И эта цифра является значительной. В связи с этим, развитие информационного сектора, обеспечение его безопасности и стабильности – одна из первоочередных задач, как экономики Казахстана, так и национальной безопасности страны.

Концепция информационной безопасности РК раскрывает отдельные аспекты социального содержания информационной безопасности. В частности, в ней указано, что «анализ современного состояния информационной безопасности в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государства. Сегодняшние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение»[1].

Кроме того, приходится осознавать, что общество в целом не готово к безопасному функционированию в свободной информационной среде. К этому же выводу приходят и социологи: «В целом приходится осознавать, что наше общество не вполне готово существовать и нормально функционировать в условиях возможных негативных и деструктивных информационных воздействий, информационно не защищено.

Достаточно вспомнить, что население восприняло такое явление, как финансовые пирамиды. Люди всех социальных слоев с удовольствием и даже с азартом бросились исполнять предписания недобросовестных информационных (рекламных) воздействий на массовое сознание. Это наводит на грустные мысли о том, какие беды стране может принести применение информационного оружия, если общество не выработает иммунитета к негативным информационным воздействиям, т.е. не научится приемам безопасного обращения с информацией»[2].

То есть, внутренним, социальным сегментом информационной безопасности является отношение общества к необходимости реализации основных принципов информационной безопасности и обеспеченность общества необходимыми информационными ресурсами.

Вторым, не менее важным сегментом информационной безопасности, является *нормативно-правовой аспект*, то есть нормативная обеспеченность и правовое регулирование процесса оборота информации.

Быстрое развитие информационных отношений, появление новых способов и приемов информационного обмена, возрастание роли информации в жизни личности, общества и государства, раз-

[1] Концепция информационной безопасности Республики Казахстан. Одобрена Указом Президента Республики Казахстан от 10 октября 2006 г. № 199 // Информационная система «Параграф».

[2] Куприянов А. И., Сахаров А. В., Шевцов В. А. Основы защиты информации: Учебное пособие. М.: Академия. 2008. С. 9.

витие информационного инструментария государственного управления и регулирования – все это требует создания и постоянного совершенствования нормативно-правовой базы. В настоящее время формируется и систематизируется новейшая комплексная отрасль права – информационное право. К сожалению, в Казахстане данная отрасль права только начала свое развитие, несмотря на существование определенного нормативного сегмента, но еще не получила должного научного обоснования и анализа.

Анализ действующего законодательства в области информационного оборота и информационной безопасности позволяет выстроить их единую систему, которая и является нормативно-правовой системой Информационного Права Республики. А именно:

1) информационно-правовые нормы, закрепленные международно-правовыми актами;
2) информационно-правовые нормы Конституции Республики Казахстан;
3) информационно-правовые нормы, оформленные в форме законов;
4) информационно-правовые нормы, закрепленные подзаконными нормативными правовыми актами:
   а) Указы Президента РК
   б) Постановления Правительства РК;
   в) акты центральных исполнительных органов власти, в системе которых особую роль занимают акты Агентства информатизации и связи РК и Комитета национальной безопасности РК.

Отдельно следует отметить специальные акты предприятий, корпораций, банковских, финансовых и иных структур. Они носят внутренний, локальный характер и направлены на регулирование конкретных вопросов, связанных с обеспечением вопросов информационной безопасности этих организаций.

Эта иерархия обусловлена тем, что зачастую в такой новой сфере законодательства, как информационная, требуется принятие большого числа подзаконных нормативных правовых актов, в том числе и локального характера. Кроме того, она позволяет соблюдать принцип верховенства закона, что является особо важным сейчас, когда государство усиленно взялось за разработку данной сферы и, соответственно, совершенствует и расширяет данное законодательство. Иерархия актов также определена кругом полномочий государственных органов, их компетенцией и сферой регулирования (управления).

Конституция РК от 30 августа 1995 г. закрепила ключевые принципы информационного оборота и защиты информации в Республике, круг основополагающих прав и обязанностей основных участников информационного оборота и их ответственность. Конституционные нормы находят свою дальнейшую регламентацию, уточнение в нормах законодательных и подзаконных актов.

В республике принят ряд нормативных актов в области информационного обмена и информационной безопасности. К наиболее значимым следует отнести: Закон РК «Об информатизации» от 11 января 2007 г., Закон РК «О связи» от 5 июля 2004 г., Закон РК «О средствах массовой информации» от 23 июня 1997 г., Закон РК «Об электронном документообороте» от 7 января 2003 г., Закон РК «О государственных секретах» от 15 марта 1999 г., Закон «Об электронном документе и электронной цифровой подписи» от 7 января 2003 г. и другие. Данные законодательные акты регулируют специфические общественные отношения.

Нормативные правовые акты, регулирующие основания привлечения к юридической ответственности, содержат в себе нормы, статьи, предусматривающие применение мер уголовной, административной и гражданской ответственности за нарушение в области информационной безопасности и свободы информации.

Но существующая нормативно-правовая база не является достаточной для регламентирования существующих и ожидаемых разновидностей общественных отношений в области информатизации, информационного оборота и защиты информации. Действующие нормы не охватили должного объема такого рода отношений. В качестве основы для анализа можно привести такой, на наш взгляд, достаточно яркий пример – Концепция информационной безопасности не предусматривает в качестве объекта информационной безопасности и, соответственно, он не подпадает под объект регулирования – коллективные субъекты, а именно юридические лица. Обеспечение ими собственной безопасности, в том числе и в информационной сфере – есть их собственная проблема, собственное нормотворчество, о чем уже указывалось ранее. Однако нельзя забывать, что именно эти юридические лица являются основой экономики страны, местом работы и материальной основой для жизни достаточно большого процента населения. Государство должно установить основные параметры, в том числе и технического характера, обязав их соблюдать (как это сделано в Соединенных Штатах Америки).

Так, в США был принят целый ряд специальных нормативных правовых актов, устанавливающих определенные критерии информационного обмена, с целью защиты интересов собственных компаний, банков и прочих юридических лиц. Так, например, Закон, называемый Актом Сарбейнса-Оксли (Sarbanes-Oxley Act of 2002, SOX), другое название – Закон о реформировании отчетности компаний и защите инвесторов (Public Company Accounting Reform and Investor Protection Act of 2002), предусматривает жесткие меры, направленные на усиление контроля за сохранностью финансовой информации. Закон SOX явился следствием нескольких крупных скандалов, разразившихся в США на рубеже XX-XXI вв., причиной которых были нарушения рядом корпораций деловой этики (сокрытие истинного состояния финансов, неадекватные данные аудиторских проверок, факты проявления коррупции и др.), в результате чего оказалось подорванным доверие инвесторов. Поэтому цель закона состояла в переходе к более строгой отчетности, укреплении корпоративного менеджмента и увеличении прозрачности финансового состояния корпораций. Закон создает обязательную для использования всесторонне обоснованную форму отчетности для всех компаний, занимающихся бизнесом в Соединенных Штатах. Согласно его положениям аудиторские компании должны быть полностью независимы, они могут по своему усмотрению нанимать и увольнять сотрудников и консультантов. Считается, что положения Закона SOX существенно затрудняют попытки отмывания денег[3]. И это далеко не первый и не единственный акт такого рода.

Таких аспектов достаточно много. Нормативная база Казахстана не является достаточной для обеспечения должного уровня информационной безопасности. Необходимость полноправного членства в информационном обществе, помимо свободного доступа и обмена информацией, соответствующей технической и образовательной базы, требует высоко развитой и гибкой правовой базы. В связи с этим, на наш взгляд, первоочередными задачами Казахстана в области информационной безопасности являются:

1) разработать национальное законодательство по вопросам правовой регламентации обращения с информационными ресурсами, установления правового статуса пользователей открытых мировых систем, в частности Интернета;
2) продолжать активную работу по разработке и принятию специальных законодательных и подзаконных актов по вопросам информационного обмена и защиты информации, направленную на исполнение не только государственными органами и организациями, но и иными юридическими лицами (не являющимися государственными). В том числе определить перечень информации, не подлежащей передаче по открытым сетям;
3) активно участвовать в разработке и заключении международных договоров и соглашений, а также нормативов обеспечения функционирования мировых открытых сетей.

Экономический аспект информационной безопасности подразделяется на два критерия: 1) информационные аспекты экономики и 2) экономика информационной безопасности.

Первый аспект, а именно информационные аспекты экономики, обозначен как ценность полной, достоверной и свежей информации в принятии решений, в том числе и в области экономики. От этого во многом зависит конкурентоспособность национальной экономики, социальная и политическая стабильность республики.

«Сегодня многие предприятия не имеют возможности получать достоверную информацию о той среде, в которой они работают, о тех возможностях, которыми они располагают, о конкурентах и своих конкурентных преимуществах. Во многом, поэтому они не в состоянии выдерживать конкуренцию и вынуждены сдавать свои позиции»[4]. Тому можно привести множество примеров. Так, незнание информации о состоянии и реальном положении дел в БТА банке могло привести к кризисному состоянию экономики страны, банкротству фирм и предприятий, утрате накопленных финансовых средств населением – вкладчиками банка.

К одной из серьезных проблем в данной сфере нужно отнести и то, что в республике не обеспечена достаточная прозрачность финансовых потоков, операций. Важным является и то, что зачастую достаточно сложно узнать, кто стоит за теми или иными финансовыми программами, корпорациями и пр. Так, многие дольщики, принимавшие участие в строительстве жилых домов и коттеджей (Ак Ауыл, Елисейские поля и др.), отмечают, что они не имели бы дел с теми лицами, чьи имена стали известны только после вмешательства органов прокуратуры, зная об их финансовом прошлом. Многие экономисты отмечают, что некоторые информационные потоки искусственно закрываются и используются в частных интересах, большой процент такой информации касается тендеров, конкурсов и пр.

Не менее важным является экономика информационной безопасности. Как уже отмечалось ранее, затраты на информационную безопасность должны быть адекватны важности, значимости и цене на охраняемую информацию. Расходы на современную технику, ее содержание, обновление, программное обеспечение занимают существенное место в расходах не только фирм, корпораций, но и государственных органов. Сказывается необходимость постоянного поддержания уровня безопасности, в том числе и в совершенной технике и лицензированных программах, которые стоят немалых денег. Однако отказываться от этого нереально, если есть, что охранять и оно того стоит. Некоторые предприятия запретили использовать на своей территории Internet, с целью избежать информационных атак, утечки информации и пр. Но и это не является решением проблемы.

Финансовый аспект информационной безопасности представляет собой защиту финансовой информации. Особую роль этот аспект играет не только для финансовых корпораций, инвестиционных и иных фондов, банков, но и для обычных граждан, которые также имеют определенную конфиденциальную информацию и также подвержены финансовым рискам во стороны мошенников. Например, заключение кредитных договоров на граждан, которые даже об этом не подозревают, посредством использования их конфиденциальной информации (удостоверения личности, ИИНа). В данном случае виной является то, что эти документы не сохраняют своего статуса, хотя в принципе являются конфиденциальными. Граждан зачастую заставляют оставлять копии любых документов во всех как финансовых, так и нефинансовых структурах, обоснованно и необоснованно. Это свидетельствует о неразработанности правового регулирования данного вопроса – обеспечение конфиденциальности личной информации, запрета требовать копии основных документов, что приводит к незащищенности граждан и потери денег банками. Не разработанным в данном случае остается вопрос ответственности самих банков перед потерпевшими гражданами, в случае злоупотребления должностными полномочиями сотрудниками банка, мошенничества с их стороны. Интересным было бы вспомнить опыт США, принявших Закон Грэмма-Лича-Блили (Gramm-Leach-Bliley Act of 1999, GLBA), или Акт о модернизации финансовых услуг (Financial Services Modernization), подписанный президентом Клинтоном в ноябре 1999 г. Его разработка и принятие были вызваны участившимися случаями крупного мошенничества, совершенного в результате получения от банков сведений об их вкладчиках. В США информация, которую считают конфиденциальной (например, номера банковских счетов вкладчиков), на самом деле может продаваться и покупаться. В этом процессе, происходящем в киберпростанстве, участвуют банки, компании по продаже кредитных карт и другие организации (например, рекламные агентства). В ноябре 1997 г. калифорнийский Чартер Пасифик Банк (Charter Pacific Bank) продал несколько миллионов номеров кредитных карточек фирме, занимавшейся бизнесом в сети Интернет. Эта фирма разослала на номера кредитных карточек требования об оплате фиктивных услуг, включая просмотр порносайтов. Такие требования получили даже те обладатели кредитных карточек, у которых вообще не было компьютеров. При этом фирма использовала несколько названий и номеров своих банковских счетов. Несмотря на это, мошенничество удалось разоблачить, и в сентябре 2000 г. в результате судебного разбирательства фирме пришлось выплатить 37,5 млн долл[5].

Обеспечение конфиденциальности банками возложено на сами банки, и осуществляется ими же. При этом Национальный Банк РК осуществляет общую координацию этого процесса. Так, Постановлением Правления Национального Банка РК от 31 марта 2001 г. № 80 были приняты «Правила по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные банковские операции», реализация которых отслеживается банками.

[3]Ваганов П. А. Правовая защита киберпространства в США // Правоведение. 2006. № 4. С. 73-88.

[4]Правовое обеспечение информационной безопасности: Учебник / Под общ. научной ред. Минаева В. А., Фисуна А. П., Крыля С. В., Дворянина С. В., Никитина М. М., Хохлова Н. С. М.: Маросейка. 2008. С. 368.

[5]Шиверский А. А. Защита информации: проблемы теории и практики. М.: Юристъ. 1996. С. 73-88.

Банки и иные финансовые корпорации стремятся не разглашать информацию о своих финансовых упущениях, потерях, вызванных незащищенностью своих информационных потоков, что, конечно, негативно скажется на их коммерческом имидже.

Военный аспект информационной безопасности является довольно традиционным. Именно данный аспект получил наибольшее изучение, как с технической, так и с практической точек зрения. Но с развитием информационного общества, его способностью к практически мгновенной передаче информации и безграничной аудитории восприятия кардинально поменялись инструменты войны. Появилось новое доселе понятие – информационная война, где основным видом оружия является информационное воздействие на сознание масс, на сознание каждого отдельно взятого человека. В своей работе «Информационные войны» Г. Г. Почепцов отметил: «Информационным оружием являются любые средства, сознательно используемые для воздействия на разум противника с минимальной физической силой и таким образом, чтобы иметь высокую вероятность заставить противника выполнить наше желание»[6].

Информационное воздействие может применяться как в позитивных, так и в негативных целях. В качестве ярких примеров информационного воздействия за последние десятилетия можно привести информационное противостояние СССР и США, а также применение информационной «утки» о наличии оружия массового поражения в Ираке, что позволило США с молчаливого согласия всего мира оккупировать территорию данной страны. Кроме того, достаточно показательными являются информационные противоборства США и Китая, приведшие к победе последнего и резкому скачку доллара, соответственно, к снижению экспорта продукции Соединенных Штатов Америки.

Компьютеризация военной техники также является одной из форм информационной войны, которая позволяет с использованием новейших информационных технологий «сканировать» военные объекты противника и наносить точечные удары, о чем свидетельствуют военные действия на Ближнем Востоке.

Экологический аспект информационной безопасности заключается в необходимости наличия информации о состоянии экологии, о реальных и потенциальных угрозах для экологии, создаваемых вследствие антропогенных воздействий на окружающую среду, а также об объективных факторах – стихийных бедствиях и катаклизмах и их последствиях.

Важность такого рода информации подчеркивается законодательным закреплением понятия «Экологическая информация» и четким определением перечня таких данных[7].

Осознавая важность и значимость таких сведений, Закон РК «О государственных секретах» относит ее к кругу информации, не подлежащей засекречиванию. Ст.17 Закона относит к ней информацию:

1) о чрезвычайных ситуациях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
2) о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности[8].

[6]Почепцов Г. Г. Информационные войны. М.: «Рефл-бук» и «Ваклер». 2000. С. 383.
[7]Экологический кодекс РК от 9 января 2007 г. № 212-III.
[8]Закон Республики Казахстан «О государственных секретах» от 15 марта 1999 г. № 349-I // Информационная система «Параграф».

Программно-технический аспект информационной безопасности является наиболее продвинутым, в отличие от всех выше рассмотренных. Программно-технические средства защиты информации представляют собой отдельные блоки информационного программирования (криптографию) и электронной механики.

Программно-техническое обеспечение информационной безопасности носит важный прикладной характер, не позволяя хакерам и иным недобросовестным пользователям осуществлять несанкционированный доступ к охраняемой информации. Именно этот аспект является наиболее сложным, дорогим и специфичным, так как основан на применении специальных программных и технических средств.

Использование программных и технических средств направлено на обеспечение безопасности в виртуальной среде. Виртуальное пространство определяется как «информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического либо виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи»[9].

Использование противником программных и технических средств поможет ему совершить следующие действия:

1) несанкционированное нарушение границ в киберпространстве, сопровождающееся проникновением во внутренние информационные системы или базы данных;
2) блокировка доступа к информационной системе, приводящая к так называемому «отказу в обслуживании» (denial of service, DoS); при этом система намеренно переполняется большим объемом посылаемых данных;
3) проникновение в электронную базу данных информационной системы с целью хищения содержимого этой базы или внесения в него каких-либо изменений;
4) внедрение в информационную систему программы, генерирующей заведомо неверные результаты;
5) установка «вынюхивающих» программ (packet sniffer), которые выслеживают, например, распространяемые по информационной сети пароли или электронные адреса и собирают их;
6) «заражение» информационной системы компьютерным вирусом, нарушающим функции этой системы и распространяющимся на другие системы с полным или частичным выходом их из строя;
7) распространение спамов (spamming) — рассылка по электронной почте незапрашиваемых посланий с запрограммированными командами по лавинообразному распространению каждого из них путем «пристегивания» собранных электронных адресов;
8) электронное разрушение информационной системы в целом или ее отдельных блоков.

Средой всякого рода кибератак является Интернет. Именно благодаря ему в США за первую половину 2012 г. количество взломов киберпространства сферы экономики, осуществленных через Интернет, превысило 180 тыс. Ежегодно число атак на Интернет увеличивается на 60%, а количество инцидентов, связанных с недостаточной кибербезопасностью, каждый год удваивается.

[9]Тропина Т. Киберпреступность и кибертерроризм // Компьютерная преступность и кибертерроризм: Сб. науч. статей / Под ред. В. А. Голубева, Н. Н. Ахтырской. Запорожье. 2004. Вып. I. С. 209-215.

Компания Symantec ежегодно проводит исследования киберпреступлений. Результаты ежегодного исследования были опубликованы в Norton Cybercrime Report 2012. Исследователям удалось установить, что каждую секунду киберпреступники причиняют ущерб 18 пользователям по всему миру[10].

Экономический ущерб от кибератак исчисляется многими миллиардами долларов. Для каждого пользователя средний ущерб от кибератак составляет 197 долларов. Также в результате исследований было установлено, что в мире потери от киберпреступности за прошлый год составили 110 млрд. долларов. При этом, в России – примерно 2 млрд. долларов, в Индии и Бразилии – по 8 млрд. долларов, и в Китае – 46 млрд. долларов. Суммарные убытки от распространения по информационным сетям в мае 2000 г. вируса «Love Bug» составили 15 млрд. долл. В начале 2012 г. киберпространство США было почти одновременно «заражено» четырьмя вирусами, убытки от которых превысили 12 млрд. долл. Параллельно росту числа кибератак увеличиваются расходы на безопасность киберпространства. Федеральное правительство США ассигновало на эти цели в 2010 г. 1,01 млрд. долл., а в 2012 г. – уже 2,71 млрд. долл.[11]

Все вышеприведенные данные, сведения и факты свидетельствуют о важности и разносторонности информационной безопасности как социального явления, приобретающего острую социальную значимость. Все рассмотренные аспекты социального бытия относят информационную безопасность как важный компонент своего развития. Информация является важным компонентом жизнедеятельности общества и государства, и ее защита, вне зависимости от вида и способов ее охраны, есть важный компонент безопасности и нормального функционирования.

[10]http://www.cibercriminals.ru/money/kakovyi-poteri-rossiyan-ot-deyatelnosti-hakerov.html.
[11]Там же.

А. Е. Жатқанбаева: Ақпараттық қауіпсіздіктің функционалдық компоненттері.

Мақалада ақпараттық қауіпсіздіктің барынша маңызды құраушылары қарастырылады. Атап айтқанда, күрделі әлеуметтік құбылыс ретінде ақпараттық қауіпсіздіктің әлеуметтік, құқықтық, қаржылық, экономикалық, әскери, экологиялық және техникалық аспектілері ашылады.

Түйінді сөздер: қауіпсіздік, ақпараттық қауіпсіздік, ақпараттық орта, нарықтың ақпараттық сегменті, ақпараттық құраушылар, ақпараттық алмасу, ақпараттық қару, нормативті-құқықтық база, ақпараттық ресурс, кибершабуыл.

A. Zhatkanbayeva. Functional components of the information security.

In this article the most important components of information security are considered. Particular social, legal, financial, economic, military, ecological and technical aspects of information security as difficult social phenomenon are opened.

Keywords: security, information security, information environment, information segment of market, the information component, the exchange of information, information weapons, legal framework, information resource, a cyberattack.

НОВЫЕ КНИГИ

Сборник материалов международной научно-практической конференции «Конституция – основа стратегии развития общества и государства» (29-30 августа 2013 г.) / Под общ. ред. И. И. Рогова, А. О. Шакирова. Ред. колл.: Малиновский В. А., Темербеков А. А., Калюжный В. А. Астана: Издательство: «Идеал – ИС 2009». 2013. – 432 с.

В числе авторов: Абдрасулов Е. Б., Ахпанов А. Н., Бекназаров Б. А., Бусурманов Ж. Д., Дауленов М. М., Когамов М. Ч., Мауленов К. С., Нарикбаев М. С., Наурызбай А. Ж., Нуртаев Р. Т., Рогов И. И., Сарсембаев М. А., Тугжанов Е. Л., Турецкий Н. Н., Ударцев С. Ф., Шакенов М. А., Шакиров А. О., Шахманова М. С. и др.

В сборник материалов международной научно-практической конференции «Конституция – основа стратегии развития общества и государства» включены Обращение Президента Республики Казахстан Н. А. Назарбаева к участникам конференции, приветствия и доклады руководителей государственных органов Казахстана, органов конституционного контроля, омбудсменов, судей конституционных судов и иных аналогичных органов ряда зарубежных стран, представителей авторитетных международных организаций, видных отечественных и зарубежных ученых-правоведов.

В материалах сборника освещены вопросы казахстанского опыта конституционного строительства в свете основных задач, поставленных в Стратегии «Казахстан-2050», а также зарубежной практики конституционного контроля и защиты прав человека.

Сборник рассчитан на широкий круг юридической общественности.