ФГБОУВО «Российский
государственный университет
правосудия»
Северо-Кавказский филиал
г. Краснодар, Российская Федерация

Университет «Туран»
Гуманитарно-юридический
факультет
г. Алматы, Республика Казахстан

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОГО И ПРАВОВОГО ПРОСТРАНСТВА В СОВРЕМЕННОМ МИРЕ

Материалы
IV Международной Российско-Казахской
научно-практической конференции
(10 декабря 2020 г.)

Сборник статей

Краснодар
2022

УДК 341:23:005.44
ББК 67.401.114
Т33

Ответственные редакторы:

***Гараева Г.Ф.**, доктор философских наук, профессор,*
заместитель директора по научной работе
СКФ ФГБОУВО «Российский государственный
университет правосудия» (г. Краснодар);
***Бегларян М.Е.**, кандидат физико-математических наук,*
доцент, заведующий кафедрой социально-гуманитарных
и естественнонаучных дисциплин
СКФ ФГБОУВО «Российский государственный
университет правосудия» (г. Краснодар);
***Сарина С.А.**, кандидат юридических наук, доцент кафедры юриспруденции*
и международного права Университета «Туран» (г. Алматы)

Т33 **Теоретические и прикладные аспекты формирования информационного и правового пространства в современном мире** : Материалы IV Международной Российско-Казахской научно-практической конференции (10 декабря 2020 г.). Сборник статей / Отв. ред. Г.Ф. Гараева, М.Е. Бегларян, С.А. Сарина. – Краснодар : Издательский Дом – Юг, 2022. – 174 с.

ISBN 978-5-91718-684-9

В сборнике представлены статьи участников IV Международной Российско-Казахской научно-практической конференции, состоявшейся 10 декабря 2020 года. В сборнике отражен широкий спектр вопросов теоретического и прикладного характера, связанных с проблемами и перспективами формирования информационного, образовательного и правового пространства в цифровом мире. В статьях рассматриваются социально-правовые, экономические, образовательные, воспитательные и иные задачи, характеризующие информационное и правовое пространство России и Казахстана.

Сборник адресован научным и педагогическим работникам, практикующим юристам, аспирантам, студентам и всем тем, кто интересуется проблемами становления информационного общества.

ББК 67.401.114
УДК 341:23:005.44

ISBN 978-5-91718-684-9

СОДЕРЖАНИЕ

Раздел 1

Формирование системы информационного, правового и образовательного пространства: социально-гуманитарные аспекты

Бурняшов Б.А.
Социально-правовые аспекты электронного доступа
к научной информации 7

Гараева Г.Ф.
Цифровизация как фактор развития правопонимания 11

Гарбовская Н.Б., **Землякова Н.В.**
Профессиональная юридическая лексика
в информационном и правовом пространстве 14

Голуб В.В.
Стратегия развития информационного обеспечения как формы
институциональных инноваций профессионального образования 17

Карданова И.В.
Актуальные проблемы формирования государственной
информационной системы в сфере социального обеспечения 19

Красюк Г.В.
Модельные характеристики учебных занятий физической культурой
и спортом в условиях дистанционного обучения 26

Малейченко Е.А., **Доценко Н.А.**
Информация о спорте и современное
информационно-правовое пространство 29

Никифорова Е.А.
Фактор времени в конституционном процессе
информационного общества 31

Рагер Ю.Б.
Цифровая история как часть всеобщей цифровизации:
перспективы развития 38

Стамкулова Г.А.
Некоторые аспекты формирования информационного,
образовательного и правового пространства
в проекте «Концепции развития высшего образования
в Республике Казахстан до 2025 года» 42

Терентьев И.А.
Социально-философский анализ тенденций развития правового пространства в условиях цифровизации современного общества 47

Шевченко А.И.
Философское осмысление процесса информационных коммуникаций 50

Раздел 2
Информационные технологии как инструмент создания информационного, образовательного и правового пространства

Бегларян М.Е., **Добровольская Н.Ю.**
Экстрагирование студенческих сообществ на основе данных социальных сетей 54

Васильева Е.Г.
Единый налоговый платеж в условиях развития российской цифровизации 58

Ващекин А.Н., **Ващекина И.В.**
Об алгоритмизации анализа элементов цифрового пространства 64

Волкова В.В.
Электронный документооборот в деятельности публичных служащих 66

Дудченко Ю.Л., **Ковалева В.В.**
Правовое регулирование цифровых инноваций: проблемы и тенденции 70

Королев М.П.
Информационный технологии как инструмент повышения эффективности механизма принудительного исполнения актов судов и иных юрисдикционных органов 74

Малышева Е.Ю., **Фетисова Т.В.**
К вопросу о целесообразности квалификации новых «технологических» правовых явлений в качестве особых разновидностей правоотношений 77

Мелоян В.Г.
Формирование электронной информационно-образовательной среды вуза: анализ эффективности и результативности функционирования 82

Уварова А.В.
Нейронная сеть для ситуационного моделирования правонарушений 86

Паршинцев А.А.
Роль интеллектуального капитала в системе управления знаниями высокотехнологичных проектно-ориентированных компаний как фактора повышения конкурентоспособности страны в условиях информатизации экономики 89

Петрушкина А.В.
К вопросу реализации права на информацию в сфере трудовых отношений 91

Хуноян А.С.
Правовые аспекты применения средств искусственного интеллекта в банковской сфере 95

Чеботарева И.Ю.
Эффективное законодательство как задача информационной безопасности 98

Черных А.М.
Процессы ситуационного управления в Автоматизированных системах обучения 102

Шиянов Г.П., **Шиянов Б.Г.**
Электронное правосудие для игровых видов спорта в информационном обществе 107

Раздел 3

Обеспечение информационной безопасности в правовом и образовательном пространстве

Аванесова Р.Р., **Слюсаренко Э.Е.**
Актуальные проблемы правового и организационного обеспечения информационной безопасности 111

Акимжанов Т.К.
Информационная безопасность – как вид национальной безопасности Республики Казахстан 117

Бочкарева Е.А., **Кривцов А.С.**
Информационная составляющая финансовой безопасности государства: правовые аспекты 123

Жанузакова Л.Т.
Правовые основы обеспечения безопасности персональных данных 129

Лузин А.И.
Тенденции развития информационной безопасности
в образовательной сфере 135

Петухов А.Ю.
Проблемы оперативно-розыскного противодействия
преступлениям в сфере компьютерной информации 140

Сарина С.А.
Вопросы признания и приведения в исполнение решений
иностранных арбитражных судов в республике Казахстан
с использованием информационных технологий 145

Соловьева С.В.
Ограничение права на доступ к информации – как способ
обеспечения информационной безопасности 154

Цимбал В.Н.
Организация обеспечения международной
информационной безопасности 158

Шаповалова Я.В.
Средства и способы защиты персональной информации
в образовательном пространстве 163

Раздел 4

Актуальные проблемы методики преподавания в условиях информационного общества

Скидан М.Н.
Преподавание физической культуры в вузах
в формате дистанционного обучения 167

Черепова А.О.
К вопросу методики формирования естественнонаучного
мышления студентов юридических специальностей 170

Раздел 1

Формирование системы информационного, правового и образовательного пространства: социально-гуманитарные аспекты

Бурняшов Б.А.,
кандидат педагогических наук, доцент,
доцент кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

СОЦИАЛЬНО-ПРАВОВЫЕ АСПЕКТЫ ЭЛЕКТРОННОГО ДОСТУПА К НАУЧНОЙ ИНФОРМАЦИИ

В настоящее время в странах-членах Евразийского экономического союза (далее – ЕАЭС) действует правовая норма об обязательном электронном экземпляре издаваемых печатных изданий; рукописи всех научных работ – диссертаций, монографий, статей в научных журналах, докладов на конференциях – являются электронными, созданными в текстовых редакторах того или иного пакета офисных программ; все материалы репозиториев, большая часть научных журналов, сборников научных статей по итогам проведения конференций публикуются не в бумажном, а в электронном виде, при этом редакции журналов, публикующихся только в бумажном варианте, имеют электронный архив выпущенных материалов.

Как итог трансформировалась работа исследователя с научной литературой по теме исследования – для проведения значительной части исследований необходимость работы в читальных залах научных библиотек отпала, на повестку дня вышли вопросы получения онлайн-доступа к научным электронным публикациям и онлайн-распространения итогов собственных научных исследований.

Ряд авторов указывают на резкое обострение в начале XXI века противоречия между новыми техническими возможностями и положениями авторского права, а также методами распространения знаний по традиционной модели подписки на научные журналы[1]. При этом обозначилась проблема: для проведения глубокого качественного исследования научных материалов, размещённых в Open Access (OA) – открытом доступе, недостаточно:

[1] Отношение российского научного сообщества к открытому доступу: 2018 г. Анализ результатов опроса / И.К. Разумова [и др.] // Наука и научная информация. – 2018. – № 1(1). – С. 6–21.

по оценкам исследователей в открытом доступе находится 28 % научной литературы[1], в 2019 году 52 % просмотров статей относились к статьям открытого доступа[2], а наиболее массовая категория исследователей – преподаватели вузов – не имеет достаточных средств для оплаты доступа к материалам, за которые издательства и специализированные Интернет-сервисы требуют плату.

Социально-правовые аспекты электронного доступа к научной информации и стало предметом нашего исследования, а целью – предложение вариантов расширения доступа учёных к научным трудам. На сегодняшний день в открытом доступе в Фонде диссертаций Российской государственной библиотеки находятся всего 2926 оцифрованных диссертаций по специальностям ВАК, 74 из которых защищались в 1888 году. Тексты диссертаций из собрания в 440 тысяч наименований на сайте disserCat, позиционирующем себя как научная электронная библиотека, доступны исследователям только за плату.

Несмотря на разделяемое нами мнение ряда учёных о том, что вхождение России в публикационную гонку с выращиванием глобальных университетов обрекает Россию и её ведущие университеты на роль догоняющих, отрезая их от выработки собственной идеологии и собственного пути развития[3], очевидно, что ученые, игнорирующие технологии и инструменты открытого доступа, катастрофически теряют свою конкурентоспособность.

По данным исследования, проведенного издательством Springer Nature и COARD, немедленный открытый доступ к научным книгам, многократно увеличивает аудиторию их читателей: в среднем такие книги скачиваются в 10 раз чаще и цитируются в 2,4 раза больше, чем книги, доступные только платно[4].

Преподаватели вузов в сложившейся ситуации вынуждены искать альтернативные варианты использования платных научных ресурсов: просмотр на платных сервисах превью монографий позволяет использовать цитаты из доступных 5–10 страниц; использование хакерских инструментов и научных материалов, предоставляемых сервисом SciHub, позволяет бесплатно читать платные научные материалы. По данным сервиса ежегодное суммарное количество просмотров его страниц превышает 1 миллиард.

---

1 Открытый доступ сегодня: широкомасштабный анализ распространенности и влияния статей открытого доступа / Х. Пивовар [и др.] // Наука и научная информация. – 2019. – Т. 2. – № 4. – С. 228–247.

2 Piwowar H. The Future of OA: A large-scale analysis projecting Open Access publication and readership / H. Piwowar, J. Priem, R. Orr. bioRxiv795310.

3 Московкин М.В. Движение открытого доступа: вызовы для России / М.В. Московкин // Научное издание международного уровня – 2017: мировая практика подготовки и продвижения публикаций: Материалы 6-й международ. науч.-практ. конф. Москва, 18–21 апреля 2017 г. – М., 2017. – С. 82–89.

4 Springer Nature, Open Access Books; Pyne, Ros; Lucraft, Mithu; Emery, Christina; Neylon, Cameron; Montgomery, Lucy; [et al.]. (2020): Diversifying readership through open access: A usage analysis for OA books. figshare. Journal contribution.

Социальные аспекты сложившейся практики обеспечения доступа к научной информации: снижение качества научных публикаций, снижение уровня требований к публикациям сотрудников со стороны администрации вузов и научного сообщества, терпимость научного сообщества к использованию нелегитимных инструментов доступа к платному научному контенту, неудовлетворённость преподавателей качеством своей работы: авторы научных статей хотели бы иметь неограниченный доступ к результатам труда своих коллег и одновременно иметь максимально широкую читательскую аудиторию своих статей.

Правовые аспекты недоступности научных публикаций: сложившаяся практика обеспечения доступа к научной информации нарушает права учёного, ограничивая его доступ к научной информации, нарушает права автора, ограничивая его стремление предоставить результаты научного исследования как можно более широкому кругу читателей; пиратское использование научных статей нарушает права издателя; возникает вопрос о правомерности торговли текстами диссертационных исследований Интернет-сервисами типа disserCat.

Имело бы смысл, на наш взгляд, в странах-участниках Евразийского экономического союза (Армения, Беларусь, Казахстан, Киргизия, Россия) начать продвижение к закреплению правовой нормой права учёного на свободный доступ к научной информации. Предложение перестаёт выглядеть абсурдным, если обратиться к истории вопроса: Д.А. Медведев в бытность Президентом РФ предложил открыть бесплатный доступ ко всем диссертациям, защищаемым в нашей стране. Предложение до сих пор не реализовано. В благоприятные для российского бюджета годы обсуждался вопрос о приобретении авторских прав на весь мировой массив научной литературы и передаче его в пользование российским учёным.

Движение в направлении предоставления исследователям открытого доступа к научным публикациям уже началось в США и Европе. 17.07.2012 Европейской комиссией для государств-членов Европейского Союза был принят документ «Рекомендация об обеспечении доступа и сохранении научной информации», которым рекомендовано обеспечение открытого доступа к публикациям по результатам научных исследований в максимально возможные короткие сроки, желательно немедленно, но в любом случае не позднее чем через 6 (для социально-гуманитарных наук – 12) месяцев после даты публикации[1]. Поскольку рекомендации не являются обязательным для исполнения документом, страны-члены Европейского Союза имплементируют его требования в национальное законодательство по своему усмотрению. В настоящее время в Австрии, Великобритании, Германии, Дании, Нидерландах, Финляндии, Франции, Швеции уже существуют правовые нормы, в соответствии с которыми соглашения, заключаемые

[1] Commission Recommendation of 17.07.2012 on access to and preservation of scientific information // Official Journal of the European Union. 21.07. – 2012. – L 194. – P. 39–43.

национальными консорциумами с ведущими информационными провайдерами, должны включать положения об открытом доступе, согласно которым все статьи авторов-резидентов должны публиковаться по модели золотого (право читать, скачивать, цитировать) открытого доступа, при этом для авторов эти публикации должны быть бесплатны. Инициативу открытого доступа поддерживают уже сотни журналов США, Европы, России. Из созданных бесплатных репозиториев крупнейший – ArXiv.org, аккумулирующий электронные публикации научных статей и их препринтов по физике, математике, информатике, астрономии, биологии, статистике, финансам. Материал не проходит рецензирование со стороны arXiv, ответственность за отнесение их к категории «актуальные для предметной области и имеющие научную ценность» полностью ложится на автора, который в соответствии с правилами репозитория должен быть «эндорсером» или статья должна быть рекомендована другим «эндорсером»; статус «эндорсера» получают автоматически авторы из признанных академических учреждений.

Международный открытый немодерируемый репозиторий Figshare, стартовавший в 2012 году, предоставляет авторам DOI, гарантируя тем самым подтверждение времени публикации, что важно при установлении вопросов авторского приоритета выдвигаемых научных идей и обеспечивает индексацию статей в Google Scholar, которая учитывается некоторыми вузами стран ЕАЭС при определении эффективности научной работы профессорско-преподавательского состава.

Российский опыт организации открытого доступа к научным публикациям представлен проектами eLibrary.ru, КиберЛенинка, НОРА. Проект российского консорциума НЭИКОН «Национальный агрегатор открытых репозиториев» (НОРА) призван стать единым пространством для сбора информации о результатах исследований российских ученых и предоставления доступа к материалам, опубликованным в открытом доступе, на сегодняшний день он объединяет 25 университетских открытых репозиториев, в т.ч. 5 вузов Беларуси. На начало 2021 года в российской электронной научной библиотеке eLibrary.ru из 35499942 научных публикаций был открыт доступ к 6252817 полным текстам, научная электронная библиотека открытого доступа КиберЛенинка содержала 2370811 научных статей.

Для облегчения доступа исследователей стран ЕАЭС к научной литературе можно предложить следующие меры:

– закрепить в странах ЕАЭС правовой нормой обязанность издателей (в т.ч. вузы), получающих финансовую поддержку от государства, размещать научные материалы в открытом доступе;

– в рамках ЕАЭС на условиях софинансирования:

– на базе уже существующих площадок (например, eLibrary) размещать в открытом доступе тексты всех диссертаций, защищаемых в странах ЕАЭС;

– создать для исследователей ЕАЭС открытый репозиторий с системой предварительного подтверждения (например, на базе NORA);

– создать для исследователей ЕАЭС немодерируемый репозиторий, аналогичный репозиторию FigShare;

– обеспечить учёных стран ЕАЭС бесплатным доступом к электронному реферативному журналу ВИНИТИ.

Гараева Г.Ф.,
доктор философских наук,
профессор, профессор кафедры
общетеоретических правовых дисциплин,
СКФ ФГБОУВО РГУП
г. Краснодар

ЦИФРОВИЗАЦИЯ КАК ФАКТОР РАЗВИТИЯ ПРАВОПОНИМАНИЯ

Правопонимание – важнейшая категория философско-правовой и теоретико-правовой мысли. В ней закрепляется парадигмальный уровень постижения сущности права. Складывается правопонимание под влиянием разнообразных факторов, в числе которых господствующие политические интересы, уровень развития правовой науки, результативность правового регулирования и правоприменительной практики, степень научной коммуникации, уровень научно-технического прогресса и др. В современном мире особое значение для развития правопонимания стал иметь процесс цифровизации, который привёл к новым подходам в отношении субъекта права, фундаментальных основ прав человека, правовых границ в виртуальном пространстве и т.д.

Цифровизация ещё не завершилась, но уже можно говорить о серьезных переменах в социальных отношениях, об их трансформации в социальных сетях, в Интернете. В современном мире активно формируется цифровая экономика, институт цифрового права, новые виды производств на основе цифровых технологий. Новые информационно-коммуникационные технологии оказывают существенное влияние на реализацию фундаментальных прав человека и гражданина, порождают потребность в новых подходах к правопониманию, правовому регулированию, правореализации и защите прав человека. Так, например, практика ЕСПЧ свидетельствует, что в современном мире, в цифровом пространстве, прежде относимое к правам частного характера, право интеллектуальной собственности (право авторства, право на товарный знак, право на патенты), относится теперь к основным правам человека[1].

[1] Laurent Sermet. The European Convention on Human Rights and property rights. Human rights fi les, N 11 rev. Council of Europe Publishing. – URL : http://www.echr.coe.int/ ttp://www.echr.coe.int

Кроме изменения под влиянием процессов цифровизации некоторых устоявшихся положений, например, на правосубъектность, на систему прав человека, в современном цифровом пространстве сформировались правовые проблемы, требующие решения: защита персональных и биометрических данных, обеспечение неприкосновенности частной жизни, защита чести, достоинства и деловой репутации человека и гражданина, обеспечение кибербезопасности и др.

Динамика современного социального пространства, безусловно, требует философско-правового осмысления. Ведь сложившиеся типы правопонимания соответствовали той реальности, которую они теоретически объясняли и тем целям, которые люди ставили на предыдущих исторических этапах. Происходящий сегодня процесс цифровизации оказывает влияние, прежде всего, на общественные отношения и те фундаментальные права, которые гарантирует Конституция Российской Федерации, в частности, неприкосновенность частной жизни, защиту информации о частной жизни, свободу мысли и слова, достоинство личности и т.д. Однако современные технологии, криминализация интернет-пространства создают как важные предпосылки для прогрессивного общественного развития и правового регулирования, так и серьезные препятствия для конституционной гарантии соблюдения прав человека. На наших глазах, как верно подчеркнул председатель Конституционного суда РФ В.Д. Зорькин, «зарождается новое право – «право второго модерна», регулирующее экономические, политические и социальные отношения в контексте мира цифр, больших данных, роботов, искусственного интеллекта»[1]. Однако неизменными остаются гарантии прав человека, обеспечиваемые международным и внутринациональным правом, Конституцией Российской Федерации. Иными словами, сегодня в условиях вектора цифровизации, изменяющего социальное пространство, место человека в системе социальных отношений, еще важнее становится обеспечение конституционно-правовой гарантии безопасности человека, гражданина, общества и государства. В этой связи, нам представляется важным, сохранить все прогрессивные возможности правового регулирования, которыми обладает Конституция, а современные подходы к развитию правопонимания соотносить с конституционным обеспечением прав человека в условиях цифровизации. Иными словами, цифровизация, порождая новые формы общественных отношений и создавая новую среду для реализации и защиты прав человека и гражданина, не должна подрывать достигнутый уровень конституционных гарантий в обеспечении эффективного действия механизма реализации и защиты прав человека. Это станет возможно в том случае, когда развитие правопонимания, отражающее происходящие

[1] Зорькин В.Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума / В.Д. Зорькин // Российская газета. 2018. Столичный выпуск № 7578 (115). – URL : https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-izashchishchat-cifrovye-prava-grazhdan.html

процессы цифровизации, будет основываться на общечеловеческих ценностях, положенных в основу современной цивилизации.

Цифровизация не отменяет сложившиеся типы правопонимания, даже, напротив, все они обретают большую актуальность. Так, например, естественные права человека требуют формирования механизма защиты на просторах виртуальной реальности, а анонимность поведения сетевого общения заставляет обратиться к вопросу адресата правовой нормы, рассматриваемой в позитивистском типе правопонимания. В этой связи развитие правопонимания в современных условиях активного процесса цифровизации общественной жизни имеет не революционный, т.е. прерывающий связь с предшествовавшей парадигмой, а эволюционный характер, т.е. поступательного углубления наших знаний о сущности права, правах человека, субъектах и объектах правового регулирования и т.д.

Также следует обратить внимание на то, что наряду с развитием правопонимания в условиях цифровизации права и общественных отношений в целом, возникает потребность формирования и изучения адекватного происходящим процессам правосознания.

Вообще правосознание и правопонимание – однопорядковые явления, но каждое из них отражает только ему свойственный набор существенных признаков обозначаемого явления. Так, правосознание выступает как одна из форм общественного и индивидуального сознания, заключающая в себе совокупность идей, правовых взглядов, оценок, настроений по отношению к существующему и желаемому праву, правовым явлениям во всем их многообразии, обеспечивая правовое поведение людей в обществе.

Сегодня, в условиях цифровизации права правосознание человека также претерпевает перемены и очень важно, чтобы их направленность оставалась в рамках правового поля. В тех случаях, когда в виртуальном пространстве существуют пробелы в праве, большую роль сегодня играют правосознание, правопонимание, нравственные и религиозные нормы. Однако они не могут заменить механизм эффективного правового регулирования, оставаясь регуляторами только для определенного круга людей.

Таким образом, цифровизация права сегодня вызвала потребность целостного развития на уровне всех сопряжённых элементов – правопонимания, правосознания, правового регулирования, отраслевого законодательства и т.д.

Системный характер взаимосвязи названных элементов обусловливает их взаимодействие и взаимовлияние, а также однонаправленный вектор трансформации, направленный на то, чтобы право адаптировалось в условиях цифровизации, порождённой научно-техническим прогрессом.

Гарбовская Н.Б.,
кандидат филологических наук,
доцент кафедры языкознания
и иностранных языков,
СКФ ФГБОУВО «РГУП»
г. Краснодар

Землякова Н.В.,
кандидат филологических наук, доцент,
заведующий кафедрой языкознания
и иностранных языков,
СКФ ФГБОУВО «РГУП»
г. Краснодар

ПРОФЕССИОНАЛЬНАЯ ЮРИДИЧЕСКАЯ ЛЕКСИКА В ИНФОРМАЦИОННОМ И ПРАВОВОМ ПРОСТРАНСТВЕ

Средства коммуникации и массовой информации в настоящее время являются важнейшими элементами для хранения и передачи информации. В нашей работе мы обратимся к специфике профессиональной юридической лексики, функционирующей в текстах, содержащих факты и события правовой сферы жизни общества. Тексты юридического дискурса не только представляют информацию правового характера, но и воздействуют на массы с целью побуждения их к анализу происходящих событий, а также к активным сознательным действиям.

Профессиональная юридическая лексика не является общеупотребительной, поэтому использование её в речи требует особого внимания. Напомним, что профессионализмы – слова и выражения, используемые людьми одной профессии. Эти слова в большинстве случаев не относятся к официальным, узаконенным наименованиям. Для профессионализмов характерна большая детализация в обозначении специальных понятий, производственных процессов, орудий труда и т.д. Основу их составляет группа слов ограниченной сферы употребления – терминологическая лексика. По определению В.М. Савицкого, «термин выражает качественную или количественную характеристику стоящего за ним юридического понятия»[1]. Он (термин) понимается как слово или словосочетание, имеющее юридическое значение и является точным обозначением определённого правового понятия. Для законодательного языка точность и ясность являются основными коммуникативными качествами, как указывал Л.В. Щерба: «…язык законов не допускает каких-либо кривотолков»[2].

---

[1] Савицкий В.М. Язык процессуального закона: Вопросы терминологии. – М., 1987. – С. 24.

[2] Щерба Л.В. Избранные работы по русскому языку. – М., 1957. – С 188.

Лексика юридического подстиля обслуживает сферу письменных официально-деловых отношений и имеет следующие стилеразличительные признаки:

– чётко выраженную социально-функциональную направленность;
– относительную стилевую закрытость;
– стандартизацию и унификацию имён;
– наличие функциональных коннотаций;
– распространённость языковых штампов.

В её составе выделяется большое количество тематических парадигм, называющих различные отрасли права: уголовное, административное, семейное, гражданское и др. Функциональные коннотации этого пласта лексики – «специализированное», «унифицированное», «служебное»[1].

Состав терминов какой-либо отрасли знаний называется терминологией, которая отражает исторический процесс накопления и осмысления знаний в определённой области деятельности человека.

Термины права можно разделить на общеправовые и специальные. Термины юридического характера, используемые во многих других отраслях права и имеющие одно и то же значение, являются общеправовыми. К ним можно отнести такие, как: гарантии, исполнитель, право, законность, гражданин и другие.

Одной из характеристик юридического термина считается его однозначность. Поэтому требованием точности обусловлен выбор понятийных и стилистических синонимов термина, когда из всех выделенных лексических вариантов выбирается один и становится постоянным средством выражения какого-либо правового понятия.

В информационном и правовом пространстве термины, обозначающие виды преступлений и наказаний выражены чаще всего отглагольными существительными: грабёж, вымогательство, сговор, истязание, просрочка.

Значительная часть терминов закона сформирована на базе общелитературного языка. Однако нередко функцию терминов выполняют такие отглагольные существительные, которые не характерны для общего употребления, например: дознание, недонесение, отобрание.

Обратим внимание на то, что профессиональная юридическая лексика обладает теми признаками, которые присущи любой лексико-семантической группе. Для неё характерна: синонимия (имущество должника – конкурсная масса, обыск – досмотр, закон – кодекс), антонимия (купля – продажа, кредитор – должник, фиктивное банкротство – объективное банкротство, цессионарий – цедент), паронимия (подсудность – судимость, преступность – преступление, индоссант – индоссат), градация (лёгкие телесные повреждения – повреждения средней тяжести – тяжкие телесные повреждения).

---

[1] См., подробнее: Диброва Е.И. Современный русский язык: Теория. Анализ языковых единиц : учеб. для студ. высш. учеб. заведений : в 2 ч. – М. : Издательский центр «Академия», 2002. – Ч. 1.

Особенности терминов отдельной отрасли права обусловлены назначением кодекса и определяются спецификой обозначаемых понятий, такие термины можно назвать специальными. В информационном пространстве они отражают содержание правовых отношений, которые зафиксированы в различных кодексах.

Например, термины:

– налог, налогоплательщик, акциз из Налогового кодекса;
– дети, семья, родители, опекуны, брак из Семейного кодекса;
– преступление, умысел, помилование из Уголовного кодекса;
– стаж, прогул, зарплата, оклад из Трудового кодекса;
– иск в арбитражном процессе, постановление арбитражного суда из Арбитражного кодекса.

Разновидностью специальных терминов являются термины, которые отражают специфику судопроизводства и характерны для процессуальных кодексов: истец, ответчик, стороны, протест, прения, свидетель, банкротство юридических и физических лиц, арбитражный управляющий и другие.

Юридические термины, функционирующие в информационном и правовом пространстве, по составу могут быть простыми, состоящими из одного слова, (кража, контрабанда, мошенничество, оскорбление, самоуправство), и составными, выраженными словосочетаниями, (захват заложника, банковская гарантия, оставление в опасности, неосновательное обогащение, возмещение убытков, воинские преступления, террористический акт, смягчение наказания).

Предельная точность и однозначность являются предпосылкой использования многословных составных терминов. Достаточно много в юридическом языке терминов, которые состоят из трёх и более знаменательных частей речи: неправомерные действия при банкротстве, оглашение информации с ограниченным доступом, воспрепятствование осуществлению права на свободу совести и вероисповедания.

В зависимости от соотнесённости и связанности выражаемых терминами понятий условно их можно разделить на несколько рядов (семантических групп).

Самые многочисленные из них называют:

– виды правоотношений;
– юридические факты (действия, события, состояния), с которыми закон связывает возникновение, изменение, или прекращение правоотношений;
– объекты прав и преступлений;
– субъектов права и преступлений.

Главной особенностью термина является его определённость, а это значит, что значение термина должно быть равным его понятийному содержанию, прямому и однозначному соотношению с обозначаемым понятием, действием или предметом. Выше названные особенности терминов юридической отрасли позволяют закону успешно регулировать права и обязанности граждан и охранять их.

Заметим, что каждая отрасль права использует большое количество терминов неюридического характера из различных областей жизни и деятельности, правоотношения в которых она регулирует. В связи с этим наблюдается процесс терминологизации, при котором общеупотребительные слова, функционирующие в языке права, начинают обозначать юридические понятия и становятся терминами. Например: находка, материнство, неосторожность, хранение и др. Как правило, в качестве терминов используется книжная лексика, но так как для наименования юридических понятий необходима предельная точность, в качестве терминов могут использоваться слова различных стилей. Бродяжничество, попрошайничество – слова разговорного стиля – ст. 151 УК РФ, отмывание – из жаргона – ст. 174 УК РФ.

Таким образом, профессиональная юридическая лексика в информационном и правовом пространстве, представляет собой явление, обусловленное требованием предельной точности.

Голуб В.В.,
кандидат педагогических наук, доцент,
доцент кафедры гуманитарных
и социально-экономических наук,
РФ ФГБОУВО «РГУП»
г. Ростов-на-Дону

СТРАТЕГИЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ КАК ФОРМЫ ИНСТИТУЦИОНАЛЬНЫХ ИННОВАЦИЙ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

Объем знаний в мире почти удваивается, а темпы технологического и научно-технического прогресса устаревают в течение 3–5 лет. Опережающее образование требует, чтобы новые знания поступали в систему образования непосредственно в процессе обучения. Поэтому возникло новое условие выживания цивилизованного общества – непрерывное образование, которое можно получать, в том числе – путем дистанционного обучения. Работа над созданием электронных курсов и учебников повышает уровень профессиональной квалификации их создателей. Информационное обеспечение, по нашему мнению, следует рассматривать как активный элемент образовательной деятельности и подготовки специалистов. Необходимо обеспечить развитие способности студента к генерации новой информации и постоянной креативности в будущей профессиональной деятельности, чтобы поднять качество подготовки специалистов на принципиально иной уровень.

В связи с этим актуализируется необходимость дополнительных специальных знаний юридического и психолого-педагогического характера о возможностях и средствах информационного обеспечения. На первый план выходят ряд принципов, обеспечивающих эффективность информационного учебно-методического обеспечения, а именно:

– активное вовлечение курсантов в процесс получения знаний, где центром внимания является обучаемый, а не преподаватель;

– гибкость совершенствующегося методического и информационного обеспечения позволяет преподавателям адаптировать и разрабатывать задания, соответствующие индивидуальным возможностям курсантов, благодаря чему преподаватель имеет возможность поощрять как индивидуальную, так и групповую работу;

– совместная (командная) работа студентов в процессе практических работ и семинарских занятий повышает роль вклада каждого в достижение общей цели.

При работе в оболочке электронного учебника возможно расширение информации, доступной конкретной группе благодаря ознакомлению с точками зрения других групп. При совместной работе качество дискуссий растет, а студенты осуществляют более глубокий и широкий анализ.

Совершенствование информационного обеспечения позволяет разнообразить формы проведения семинарских занятий, поскольку электронная оболочка включает сам текст, тесты и задачи, самотестирование, библиотеку, электронную конференцию, обмен файлами, обеспечивающими проведение разнообразных мероприятий, как в режиме реального времени, так и в ходе самостоятельной работы студентов во вне учебное время. Новые информационные технологии активно используются в управленческой, образовательной, воспитательной деятельности профессиональных учебных заведений. Создается учебно-программное обеспечение, которое позволяет совершенствовать образовательный процесс и создать методическое обеспечение педагогических инноваций.

При этом учитывается технологическая, социально-гуманитарная, научно-педагогическая, экономическая грани образовательного процесса. Преодоление стереотипов, тормозящих реализацию информационного потенциала образования, позволяет расширить исследовательский инструментарий специалистов и повысить конкурентоспособность выпускников на рынке интеллектуального труда. Позитивным следствием интенсивного информационного обеспечения образования выступает повышение его наукоемкости, интеллектуализации, экономия материальных, энергетических и трудовых ресурсов за счет эксплуатации информационных ресурсов.

Внедрение сетевых коммуникаций в образовательный процесс открывает новые организационно-педагогические и методические возможности, новые перспективы персональной подготовки кадров, в том числе гибкость структуры учебного процесса, максимальный учет индивидуально-типологических особенностей, индивидуализацию режима работы, а также повышение эффективности подготовки специалистов.

Карданова И.В.,
старший преподаватель кафедры
государственно-правовых дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ФОРМИРОВАНИЯ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В СФЕРЕ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ

Невозможно переоценить важность владения информацией о предоставлении гражданам различных видов социального обеспечения. В период пандемии[1] COVID-19, стало особенно актуальным не только информирование, но и возможность фактического получения различных мер государственной поддержки гражданам, попавшим в трудную жизненную ситуацию.

В Указе Президента РФ от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию» определено: «… право на информацию является одним из фундаментальных прав человека»[2].

В федеральном законе от 27.07.2006 № 149-ФЗ закреплено понятие «информация», согласно которому это сведения (сообщения, данные) независимо от формы их представления[3].

Следует отметить, что в национальном законодательстве вопросу регулирования информации отведено значительное место. Так, ст. 24, 29, 42 Конституции РФ регулируют право на информацию[4], четвертая часть ГК РФ посвящена правовому регулированию информации[5], а УК РФ содержит составы преступления, в основе которых лежит нарушение правил

---

1 Пандемия (от греч. *pandemia* – весь народ) – эпидемия, охватывающая значительную часть населения страны, группы стран, континента (См.: БЭС.). – URL : https://gufo.me/dict/bes/ПАНДЕМИЯ (дата обращения 15.01.2021).

2 Указ Президента РФ от 31 декабря 1993 г. № 2334 «О дополнительных гарантиях прав граждан на информацию». – URL : http://base.garant.ru/102839/ (дата обращения 17.01.2021).

3 Федеральный закон от 27.07. 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция). – URL : http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 15.01.2021).

4 Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – URL : http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения 15.01.2021).

5 Гражданский кодекс Российской Федерации (ГК РФ) Часть четвертая. Федеральный закон от 18 декабря 2006 № 230-ФЗ. – URL : http://www.consultant.ru/document/consdocLAW64629/ (дата обращения 15.01.2021).

получения, использования или распространения информации (ст. 128.1, 137, 138.1, 183 УК РФ)[1].

Кроме уже названных нормативных документов, в России действуют Федеральные законы: № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»[2], № 8-ФЗ от 09.02.2009 «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[3] и № 210-ФЗ от 27.07.2010 «Об организации предоставления государственных и муниципальных услуг»[4], которые регулирует отношения по обеспечению доступа к информации о деятельности государственных органов и органов местного самоуправления, а также по обмену информацией в форме электронных документов при осуществлении деятельности публичной власти.

Внедрение такого способа взаимодействия граждан и организаций, а также направленность на повышение качества предоставляемых услуг государственными и муниципальными органами можно считать одной из передовых идей, которые, по мнению законодателя, должны облегчить указанные процедуры и стереть административные барьеры.

Но так ли это на современном этапе? Информационные и телекоммуникационные технологии широко используются органами государственной власти, министерствами и ведомствами, Пенсионным фондом Российской Федерации (ПФР), Фондом социального страхования Российской Федерации (ФСС), Федеральной налоговой службой (ФНС) и другими учреждениями, предоставляющими государственные услуги населению.

С целью доступности информации для граждан и органов государственной власти ПФР реализуются масштабные федеральные проекты: Федеральный реестр инвалидов (ФРИ) и Единая государственная информационная система социального обеспечения (ЕГИССО).

В рамках нашего исследования мы остановимся на ЕГИССО, поскольку ограничены рамками данной статьи, а ФРИ хоть и важная, но всё же одна из витрин данных единой государственной информационной системы (рис. 1).

---

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ (ред. от 30.12.2020). – URL : http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 15.01.2021).

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция). – URL : http://www.consultant.ru/document/consdocLAW61798/ (дата обращения 15.01.2021).

[3] Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления». – URL : http://www.consultant.ru/document/cons_doc_LAW_84602/ (дата обращения 17.01.2021).

[4] Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ. – URL : http://www.consultant.ru/document/consdocLAW103023/ (дата обращения 17.01.2021).

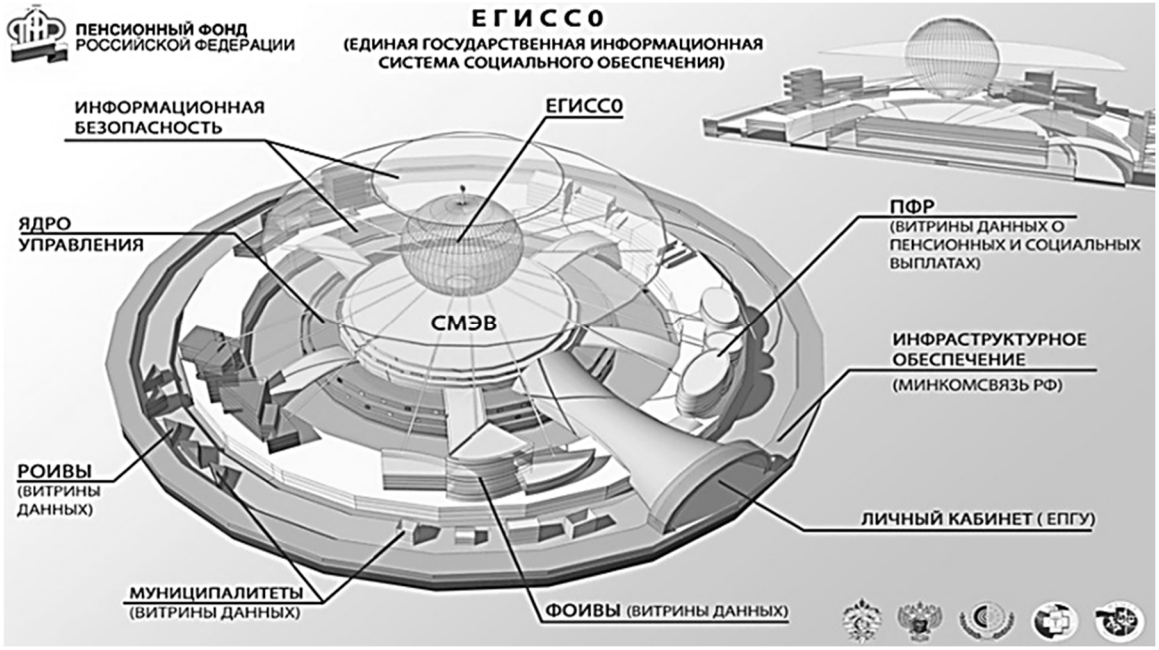

Рисунок 1 – Единая государственная информационная система социального обеспечения (ИТ в Пенсионном фонде РФ)

Целью создания указанной системы является совершенствование учета прав граждан на различные виды социального обеспечения в соответствии с действующим законодательством, а также обеспечение доступа к информации как самих граждан, так и различных органов государственной власти.

С 01 января 2018 года вступила в силу глава 2.1. в законе о государственной социальной помощи[1], которая полностью посвящена информационной системе социального обеспечения. Не вдаваясь в подробности, следует отметить, что в информационную систему включены:

1. Сведения о получателях социальной поддержки (паспортные данные, СНИЛС, адрес проживания, сведения о периодах трудовой деятельности, сведения о законных представителях, о лишении и восстановлении в родительских правах, и др.).

2. Персонифицированные сведения о мерах социальной защиты сведения о мерах социальной защиты, социальных услугах, иных социальных гарантиях и выплатах, предоставляемых за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов.

3. И другие сведения (всего 12 пунктов), которые предусмотрены Постановлением Правительства РФ № 181 от 14.02.2017 г.[2].

---

[1] Федеральный закон «О государственной социальной помощи» от 17.07.1999 № 178-ФЗ. – URL : http://www.consultant.ru/document/cons_doc_LAW_23735/ (дата обращения 17.04.2021).

[2] Постановление Правительства РФ от 14.02.2017 № 181 (ред. от 03.12.2020) «О Единой государственной информационной системе социального обеспечения» (вместе с «Положением о Единой государственной информационной системе социального обеспечения», «Порядком предоставления информации в Единую государственную информационную систему социального обеспечения»). – URL : http://www.consultant.ru/document/consdocLAW212876/ (дата обращения 17.04.2021).

Взаимодействие ЕГИССО с порталом государственных услуг позволяет оперативному отражению в личном кабинете гражданина информации о предоставляемых мерах социальной поддержки. Для государственных органов, предоставлена возможность получения необходимой информации обо всех видах предоставляемого социального обеспечения отдельно взятому гражданину, что позволяет принять обоснованное решение о его нуждаемости в той или иной мере поддержки. Соответствующие запросы направляются через электронную форму в ЕГИССО или через систему межведомственного взаимодействия, при этом важно отметить, что формирование запросов для деятельности, не связанной с предоставлением мер господдержки, не допускается! (рис. 2).

Рисунок 2 – Схема информационного взаимодействия (ИТ в Пенсионном фонде РФ)

Как видно из рисунка 2, социальное обеспечение, имеет несколько уровней (федеральный, региональный и муниципальный). Учитывая конституционное закрепление в ст. 72: «социальная защита, включая социальное обеспечение» находится в совместном ведении Российской Федерации и её субъектов, на каждом из этих уровней установлены и предоставляются свои меры поддержки.

При детальном изучении проблемы, было установлено, что таких мер насчитывается более 100 видов по десяткам и сотням категорий граждан,

имеющих на них право и предоставляемых за счет бюджетов различных уровней. Это притом, что под разным названием, по сути, устанавливаются одни и те же виды социальной поддержки по одинаковым основаниям, а каждый уровень и каждое ведомство ведет свой учет по получателям и объемам, но целостной картины по расходам на конкретного гражданина нет ни у кого. Это первая проблема, которую в ближайшей перспективе позволит решить информационная система. При наличии полной базы данных и взаимодействии заинтересованных структур станет возможным перейти к адресной поддержке по фактической нуждаемости и провести аналитику по количеству предоставленных услуг конкретной семье или отдельно взятому человеку.

Ещё очень важной составляющей является классификатор мер социальной поддержки (далее – Классификатор), который является базовым государственным информационным ресурсом и формируется в составе ЕГИССО[1]. По мнению специалистов, ощутимым эффектом создания единого классификатора видов социальной поддержки и категорий лиц, которым они предоставляются, станет стандартизация и унификация указанных мер. О проблемах с понятийным аппаратом в праве социального обеспечения говорится много, но законодатель продолжает один и тот же вид социального обеспечения называть по-разному. К давно установленным понятиям «пенсия», «пособие», «компенсация», добавляются новые «ежемесячные денежные выплаты», «меры государственной поддержки», «социальные выплаты», «социальная поддержка» и т.п. Более того, внутри каждого понятия идут разновидности, напр. пенсия по старости, пенсия по инвалидности, пенсия за выслугу лет, пособие на ребенка, пособие по временной нетрудоспособности, пособия в связи с материнством и т.п. Упорядочить понятийный аппарат, как в федеральном, так и в региональном законодательстве, а так же в целях единообразного понимания мер государственной защиты и призван Классификатор. Для примера приведем структуру по обязательному социальному страхованию, которое относится к федеральному уровню ответственности.

Таким образом, информационная система станет базой данных включающая в себя все виды государственной поддержки всего населения РФ. Такой подход напоминает 2005 год, когда была реализована «монетизация» льгот и созданы федеральный и региональный регистр отдельных категорий граждан (льготников). Создание этих регистров, помогло разобраться, кто и

---

[1] Приказ Минтруда России от 30.06.2017 № 542н «Об утверждении Порядка формирования классификатора мер социальной защиты (поддержки), его актуализации и использования участниками информационного взаимодействия при размещении информации в Единой государственной информационной системе социального обеспечения» (Зарегистрировано в Минюсте России 14.08.2017 № 47766). – URL : http://www.consultant.ru/document/consdocLAW222702/ (дата обращения 17.03.2021).

на какие ежемесячные выплаты имеет право, поскольку один и тот же гражданин мог одновременно обладать несколькими льготными статусами.

Это непростая задача и большой труд сотрудников всех структур. От качества выполненной работы будет зависеть успех реализации ЕГИССО и качество предоставляемых мер социальной поддержки. Это позволит исключить дублирующие меры увеличить помощь, предоставляемую адресно. В конечном итоге, переход на межведомственное взаимодействие позволит снизить затраты на содержание государственных структур исключив избыточные функции служащих, а информационная система станет прозрачной и более доступной для её участников.

Новый алгоритм предполагает, что весь процесс от приема заявления гражданина через Единый портал государственных и муниципальных услуг (ЕПГУ) до фактического предоставления меры социальной защиты будет осуществляться непосредственно в ЕГИССО, либо через информационные системы региона, но по единым стандартам (рис. 3).

Рисунок 3 – Присвоение кода категории получателей МСЗ локального уровня в соответствии с Классификатором

Следует отметить, что Пенсионный фонд постоянно работает над совершенствованием предоставляемых информационных услуг. Развивая информационную систему, он выводит качество услуг на новый уровень и уже почти 80 % обращений поступает в электронной форме. Система предоставления Госуслуг Пенсионным фондом постоянно пополняется (рис. 4).

Рисунок 4 – Новые сервисы портала ПФР (ИТ в Пенсионном фонде РФ)

Пенсионный фонд всё больше внедряет проактивное оформление документов и уведомлений граждан. Так, например, с 15.04.2020 г. сертификат на материнский семейный капитал (МСК) уже оформляется автоматически. И теперь семья может распоряжаться МСК, получив сертификат в электронной форме в беззаявительном порядке.

С декабря 2020 года с использованием ЕПГУ будет осуществляться информирование граждан о правах на МСЗ по трем жизненным ситуациям: рождение ребенка; установление инвалидности; наступление пенсионного возраста. Этот перечень планируется расширять.

С 2021 года ПФР начнет информировать граждан о размере будущей пенсии, сформированной на дату уведомления. Такие сведения станут доступны достигшим 45 лет и старше, что позволит оценить перспективы по достижении установленного возраста[1]. И это важно! Современная пенсионная система сложна для понимания, а просчитать свои шансы заработать страховую пенсию невелики. К указанному возрасту у большинства граждан уже сформированы определенные пенсионные права, который позволит спрогнозировать уровень пенсионного обеспечения и за оставшееся время исправит ситуацию в свою пользу.

Таким образом, совершенствование электронного документооборота и внедрение проактивного информирования граждан позволила платформа ЕГИССО. Субъекты РФ и муниципальные образования активно наполняют

[1] Российская Газета. RG.RU. Официальный сайт. Россияне старше 45 лет будут получать уведомления о будущих пенсиях. – URL : https://rg.ru/2021/01/02/rossiiane-starshe-45-let-budut-poluchat-uvedomleniia-o-budushchih-pensiiah.html?utm_source=yxnews&utmmedium=desktop (дата обращения 18.03.2021).

информационную систему необходимыми данными, что позволит достичь поставленных целей. Пока нет точных сведений, какие конкретно и в каком количестве услуги были предоставлены в 2020 году через электронные сервисы ПФР, динамику проследим по имеющимся доступным данным (рис. 5).

Сегодня работают 35 электронных услуг ПФР. Доступ посредством ЕСИА.
В 2016 г. электронными сервисами ПФР воспользовались более 6 млн человек.

Наиболее востребованные сервисы по итогам 2016 г.:

№	Электронный сервис	Число запросов
1	Справка о состоянии ИЛС	2 млн.
2	Заявление о назначении и доставке пенсии	1,9 млн.
3	Информирование о пенсионном обеспечении и установленных социальных выплатах	525 тыс.
4	Информирование о размере (остатке) материнского капитала	320 тыс.
5	Заявление о единовременной выплате за счет средств МСК	255 тыс.
6	Справка о размере пенсии и иных социальных выплатах	190 тыс.
7	Заявление о единовременной выплате средств пенсионных накоплений	125 тыс.

Рисунок 5 – Электронные сервисы ПФР (ИТ в Пенсионном фонде РФ)

Красюк Г.В.,
старший преподаватель
кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

МОДЕЛЬНЫЕ ХАРАКТЕРИСТИКИ УЧЕБНЫХ ЗАНЯТИЙ ФИЗИЧЕСКОЙ КУЛЬТУРОЙ И СПОРТОМ В УСЛОВИЯХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

В процессе спортивной подготовки студентов на академических занятиях в условиях дистанционного обучения преподаватель решает задачи образовательного стандарта.

Модельные характеристики учебно-тренировочного процесса по дисциплине физическая культура и спорт, в условиях дистанционного выполнения программы обучения студентами высших и средне-специальных учебных заведений многообразны и имеют важное значение для воспитания всех видов физических качеств, овладения двигательными навыками и их совершенствования, воспитание морально-волевых и нравственных качеств.

В процессе спортивной подготовки у студентов воспитываются умения и навыки. Это достигается многократным повторением упражнений, которые, в свою очередь, оказывают положительное воздействие на работу всех систем и органов человека. Таким образом, под спортивной подготовкой следует понимать направленное использование всей совокупности факторов, обеспечивающих готовность занимающихся к спортивным результатам.

В этом плане наглядно просматривается единство обучения и тренировки.

Под обучением в спортивных научных кругах принято понимать начальную фазу овладения занимающимися базовой системой знаний, умений и навыков. Главным пунктом содержания обучения следует отнести освоение техники выполнения элементов упражнений, простейших тактических действий, выполняемых индивидуально или в группе, формирование умений и навыков.

Дальнейший этап подготовки, выполняющий функцию по закреплению и совершенствованию имеющихся знаний, навыков и умений, следует называть тренировкой. Тренировка решает задачи совершенствования техники выполнения упражнений, совершенствования тактических действий в команде, группе, или индивидуально, развитие волевых, моральных и физических качеств. Таким образом, учебно-тренировочное занятие – это модель системы, построенной на основе методов управления.

Тренировку и обучение следует рассматривать как многолетний, единый, организованный педагогический процесс. Они дополняют друг друга, между ними нет резких разграничений, так как обучая, преподаватель одновременно тренирует, а тренируя, он обучает.

Разграничение терминов обучения и тренировки как понятий, дает возможность четче сформулировать своеобразие целей и задач учебно-тренировочного процесса. Анализируя разные этапы подготовки студентов, следует сказать, что удельный вес самой тренировки и самого обучения, существенно варьируется, так как контингент занимающихся неоднороден, и имеет различную степень уже имеющейся подготовленности.

Процесс обучения и тренировки относится к педагогическим процессам, и поэтому должен иметь свои направленность и воспитывающий характер. Ввиду этого, к учебно-тренировочным занятиям предъявляются большие требования. Построение занятий должно способствовать развитию гармоничной личности студентов.

Успешное решение задач обучения и тренировки, в условиях дистанционного обучения, не смотря на огромную зависимость от современного мультимедийного комплекса, который в значительной степени влияет на эффективность и качество обучения, прежде всего определяется личностью преподавателя-тренера, который является центральной фигурой в

структурной модели дистанционного образования. Таким образом, структура вышесказанной модели включает в себя преподавателя-тренера, контингент занимающихся, рабочие программы, мультимедийный комплекс, дополнительные средства обучения. Учитывая первостепенность своего значения, преподаватель должен непрерывно совершенствовать специальные знания, изучать и применять новейшие достижения науки и практики, эффективно внедрять их в проводимый им учебно-тренировочный процесс.

Организованные учебные занятия по физической культуре и спорту призваны решать задачи, стоящие перед государственной системой физического воспитания. Основным содержанием занятий является гармоничное совершенствование учащейся молодежи, всестороннее развитие физических и духовных способностей, необходимых для творческого труда.

Несмотря на необходимость достижения высоких спортивных результатов, преподаватель не должен не учитывать оздоровительную направленность тренировки и обучения, их воспитательный характер. Осуществление многостороннего подхода является хорошим показателем эффективности работы тренера.

Модельная база для владения студентами учебно-методических знаний складывается из решения таких образовательных задач, как совершенствование двигательных навыков и волевых качеств, расширение функциональных возможностей организма занимающихся, сохранения и повышения физической работоспособности, расширение научных знаний по теме физической культуры и спорта, а также воспитания навыков самоконтроля, и привитие гигиены, воспитание дисциплинированности, трудолюбия, активности, сознательности.

Последовательное решение вышеперечисленных задач в условиях моделирования дистанционного обучения, позволяет более полно использовать колоссальные ресурсы человеческого организма для достижения успехов в физической культуре и спорте.

Положительное влияние повышенных требований к учебно-тренировочной подготовке в условиях дистанционного обучения обеспечивается путем последовательной реализации педагогических принципов учебно-тренировочных занятий, и в первую очередь, неукоснительных соблюдений законов научного управления процессом.

Малейченко Е.А.,
кандидат социологических наук,
доцент кафедры
социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

Доценко Н.А.,
старший преподаватель
кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

ИНФОРМАЦИЯ О СПОРТЕ И СОВРЕМЕННОЕ ИНФОРМАЦИОННО-ПРАВОВОЕ ПРОСТРАНСТВО

Медицинские и технологические компании, а также учёные во всем мире разрабатывают новые решения, которые помогают справиться с пандемией и поддержать здоровье в этот непростой период.

В современном обществе технологии используются почти во всех видах деятельности, но в данном случае информационные технологии очень нужны и полезны для здоровья человека.

Существует множество приложений для телефона, различных технологий и советов по профилактике здоровья, также появляются технологии по предотвращению заражения новыми инфекционными заболеваниями.

Если говорить именно об информационных технологиях для здоровья человека в условиях изоляции или локдауна, то существуют такие новые как:

– интерактивные карты продвижения пандемии (с их помощью на картах отмечаются точки, районы в которых больше всего заболевших, а также с помощью этих карт можно узнать данные о смертности, выздоровлениях и распространении пандемии).

– смарт-часы (по сердечному ритму смарт-часы при наличии соответствующего функционала могут контролировать уровень стресса, измерять сатурацию крови и даже снимать кардиограмму, но эта функция пока доступна далеко не во всех смарт-часах. Например, в Apple Watch она пока заблокирована везде кроме США из-за необходимости получить соответствующие разрешения в государственных надзорных органах. Росздравнадзор недавно сертифицировал функцию измерения ЭКГ в Apple Watch в России).

Во время пандемии очень важным остается спорт и спортивное движение. Регулярные тренировки – это прекрасный способ поддержать как

психологическое, так и физическое состояние. упражнения помогают улучшить и укрепить иммунную систему (иммунитет).

Большое количество людей в современном мире ведут малоподвижный образ жизни. Это объясняется сидячей работой, длительным и активным использованием современных гаджетов, которые часто заменяют людям живое общение с окружающим миром. Это всё не оказывает положительного влияния на здоровье, потому что в последствии люди много едят и впадают в депрессивное состояние.

В данное время COVID-19 радикально изменил жизнь людей всего мира. Они были вынуждены долгое время оставаться дома. В условиях самоизоляции у многих был вынужденный малоподвижный образ жизни, который может ослабить иммунитет человека, тем самым привлечь к себе многие инфекции и заболевания.

Если человек до пандемии вёл активный образ жизни, занимаясь каким-либо видом спорта и посещая тренировки, то в карантинных условиях очень трудно сохранять прежний метаболизм, выносливость и физическую форму. В отсутствии физических нагрузок можно с легкостью потерять форму и подвергнуть опасности сердечно-сосудистую систему.

Огромным плюсом в данной ситуации является то, что при достаточном количестве физических нагрузок можно укрепить свой иммунитет. Вследствие чего обеспечить себе дополнительную безопасность от различных инфекций (если даже заболеть при хорошей, укреплённой иммунной системе, то легче и быстрее организм может справиться с недугом).

В тот момент, когда у людей проходит период самоизоляции, в интернете появляется большое количество онлайн тренировок, курсов, при помощи которых можно выполнять физические нагрузки (тренировки) с тренерами находясь дома, огражденными от инфекции. Существуют как платные, так и бесплатные (пробные) тренировки. В интернете есть множество видео, в которых показываются упражнения и их правильное выполнение (что не менее важно).

Так же в этой ситуации необходимо понимать и рассчитывать нагрузку, не переусердствовать с тренировками, для этого стоит соблюдать некоторые правила:

– не тренироваться, если обнаружены симптомы болезни.

– нельзя тренироваться до сильной усталости и изнеможения (это так же увеличивает риск инфицирования).

– не рекомендуется проводить тренировки больше 5 раз в неделю.

– не стоит злоупотреблять употреблением воды, потому что это может привести к состоянию общей гипергидратации организма.

Никифорова Е.А.,
кандидат юридических наук, доцент,
доцент кафедры
государственно-правовых дисциплин,
ПФ ФГБОУВО «РГУП»
г. Нижний Новгород

ФАКТОР ВРЕМЕНИ В КОНСТИТУЦИОННОМ ПРОЦЕССЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Конституционный (конституционно-правовой) процесс, означающий трансформацию конституционно-правовых норм, всегда предопределен временными факторами, предполагающими более или менее длительное время подготовки нормативных изменений. В первом приближении можно предположить, что хронологические характеристики такого процесса коррелируют с формой преобразований, взаимосвязанной с видом систематизации норм (так как в большинстве случаев речь идет о систематизации правового регулирования). Так, консолидация и кодификация – намного более длительные во времени процедуры, чем скажем, внесение отдельных точечных изменений в конституционные тексты. Необходимо отметить, что, говоря о конституционном процессе, мы имеем в виду как способы внесения изменений в основной закон, так и в иные акты конституционного законодательства, а в некоторых случаях – одновременное взаимосвязанное изменение смысла конституционного текста в связи с актами толкования. В данном аспекте можно говорить о:

1) временных (темпоральных) нормах конституционного права и временном конституционном регулировании,

2) времени (сроках) подготовки и проведения конституционных изменений.

Нормы, рассчитанные на временное (однократное или непродолжительное по времени) применение, довольно часто встречаются в конституционном праве, несмотря на его фундаментальный, системообразующий характер правового регулирования. К временным относят нормы, которые имеют указание в диспозиции нормы на сроки ее действия – такие конструкции широко распространены в конституционном праве и других отраслях[1]. Отмечается, что временными являются такие нормы, которые обычно отражаются в переходных положениях конституций либо содержатся в иных

[1] Демичев Д.М. Классификация конституционно-правовых норм: теория и практика / Д.М. Демичев // Материалы международной научно-практической интернет-конференции «Новые векторы развития демократии». Вестник Института комплексных исследований аридных территорий. – 2013. – № 2(27).

нормативных актах временного действия[1]. В российском конституционном праве в качестве примеров таких норм можно приводить большинство положений раздела второго Конституции РФ, а после внесения поправок в марте 2020 года – в том числе и положения раздела первого, в частности, часть 3.1 статьи 81. При этом, на наш взгляд, следует различать временные нормы и нормы, указывающие в диспозиции срок, на который устанавливается регулирование правоотношения. Так, к примеру, нормы Федерального конституционного закона «О чрезвычайном положении», имеющие в своей диспозиции какие-либо сроки, являются постоянными – до тех пор, пока данные законодательные позиции не будут изменены в законотворческом порядке, – то есть сам срок, на который вводится режим чрезвычайного положения, не превращает норму во временную. Таких норм достаточно и в тексте самой Конституции РФ, – это, например, положения, регламентирующие этапы законодательного процесса.

Очевидно, что такие нормы отличаются от норм, содержащихся в разделе втором «Заключительные и переходные положения» Конституции РФ, действие которых исчерпывается либо реализацией правоотношения, которое они регулируют, либо принятием предусмотренного нормативного правового акта, либо определенно установленным сроком и т.п. Это истинно временные нормы, в отличие от постоянных норм, в содержание диспозиции которых в качестве элемента включен срок действия установленного нормой правового отношения, режима и т.п., то есть срок (время) выступает содержанием действия нормы.

Истинно временными могут являться не только отдельные нормы (как приведенные выше примеры заключительных и переходных положений Конституции РФ), но также и целые нормативные правовые акты, в том числе и в форме федеральных законов (например, ряд таких законов был принят в связи с проведением Олимпиады в Сочи[2]). Поэтому, как нам представляется, целесообразнее применять определение не «временные», а «темпоральные» нормы конституционного права – такое наименование норм отражает ту существенную разницу, которая отмечена выше. В современных исследованиях сущности, видов и действия конституционных норм, например, в комплексной работе Н.Е. Таевой, предложена классификация темпоральных норм, отражающая особенности действия данных норм в системе правового регулирования Российской Федерации, придания ей свойства

---

[1] Демичев Д.М. Классификация конституционно-правовых норм: теория и практика / Д.М. Демичев // Материалы международной научно-практической интернет-конференции «Новые векторы развития демократии». Вестник Института комплексных исследований аридных территорий. – 2013. – № 2(27).

[2] Федеральный закон от 01.12.2007 № 310-ФЗ (ред. от 28.06.2014) «Об организации и о проведении XXII Олимпийских зимних игр и XI Паралимпийских зимних игр 2014 года в городе Сочи, развитии города Сочи как горноклиматического курорта и внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 01.01.2017) // Российская газета, № 272, 05.12.2007 [и др.].

динамичности. В зависимости от устанавливаемых временных параметров предлагается выделять:

1) конституционно-правовые нормы, устанавливающие конкретные даты конституционно-правовых явлений, действий;

2) конституционно-правовые нормы, устанавливающие длительность конституционно-правовых явлений, действий (неопределенная длительность, относительно определенная длительность, абсолютно определенная длительность);

3) конституционно-правовые нормы, устанавливающие повторяемость конституционно-правовых явлений, действий (через конкретные сроки, без использования конкретных сроков – систематичность);

4) конституционно-правовые нормы, устанавливающие одновременность конституционно-правовых явлений, действий;

5) конституционно-правовые нормы, устанавливающие последовательность конституционно-правовых явлений, действий. В зависимости от способа установления временного параметра темпоральные конституционно-правовые нормы могут:

1) устанавливать конкретный срок;

2) устанавливать временные параметры через оценочные категории («своевременно», «непрерывно», «в разумный срок» и т.п.)[1].

Представляется возможным, на наш взгляд, вести речь о временном конституционном регулировании, которое представляет собой установление правовых норм для определенного индивидуализированного случая либо на определенное время. Так, Постановлением Конституционного Суда РФ от 01.07.2015 № 18-П по делу о толковании статей 96 (часть 1) и 99 (части 1, 2 и 40 Конституции Российской Федерации[2] принято решение индивидуализированного характера – разрешающего однократный перенос даты выборов депутатов Государственной Думы и сокращение конституционного срока полномочий нижней палаты шестого созыва.

Иной хронологический аспект конституционно-правовых процессов может быть рассмотрен применительно к вопросу длительности периода разработки и принятия новых конституционных норм, включая в первую очередь нормы Основного закона. Этот вопрос связан с качеством легитимности регулятивных обновлений, их целесообразности и обоснованности. Интересно, что, в сравнении с другими важными конституционными процедурами, например, процедурой отрешения Президента РФ от должности, Конституция РФ не задает временных параметров своих изменений. Речь, конечно, идет не об устанавливаемом на будущее сроке действия положений Конституции, а о хронологической регламентации самого процесса внесения изменений. Косвенно он урегулирован нормами законодательной

---

[1] Таева Н.Е. Нормы конституционного права в системе правового регулирования Российской Федерации : автореф. … д-ра юрид. наук. – М., 2018. – С. 22–23.

[2] Постановление Конституционного Суда РФ от 01.07.2015 № 18-П по делу о толковании статей 96 (ч. 1) и 99 (ч. 1, 2 и 4) Конституции Российской Федерации // Российская газета, № 147, 08.07.2015.

процедуры в парламенте, если речь идет об изменениях в форме поправок к главам 3–8, указанием в статье 136 на порядок принятия федерального конституционного закона. Для пересмотра Конституции таких сроков не установлено.

В науке отмечается, что при разработке и принятии новых конституций предпочтителен долгий период подготовки, так как это влияет на качество текста[1]. При этом, отметим, в этот период стоит включать не только саму непосредственную формально-юридическую процедуру изменений, но также и возможности предварительного обсуждения необходимости таких изменений в демократическом обществе, общественную дискуссию, целесообразность которой проистекает из сущности современной конституции как результата компромисса различных социальных сил, групп, интересов, потребностей, которая вот уже более тридцати лет, с начала конституционных изменений в конце 80-х годов прошлого века, преобладает в конституционно-правовой мысли. Не будучи формализованным вообще, процесс общественной (в том числе и научной) дискуссии по изменению конституции и его временные рамки не являются обязательным элементом конституционного процесса современности. История (в том числе и новейшая) развития российского конституционализма показывает нам различные примеры.

Так, научная дискуссия последних лет, предшествующих конституционным изменениям 2020 года, являла собой достаточно большое разнообразие взглядов на проблему. Например, о неизменности текста действующей Конституции, нежелательности «ревизии» основного закона и использовании креативных возможностей действующей Конституции РФ писал С.М. Шахрай: так, если идея правительства парламентского большинства окажется политически востребованной, то, по его мнению, с правовой точки зрения достаточно внести необходимые изменения в регламенты обеих палат и Федеральный конституционный закон «О Правительстве РФ»[2]. Профессор Н.А. Умнова-Конюхова предложила считать проблему легитимности Конституции РФ 1993 года исчерпанной и нецелесообразной для дальнейшего обсуждения по причине связанности с вопросом легитимности всего законодательства, принятого на ее основе[3], и предполагать дальнейшее конституционное развитие («конституционный дизайн») в плане развития проблематики конституционной нравственности, глобализации и универсализации конституционных ценностей, выработки универсальных конституционных стандартов.

Между тем, А.И. Ковлер, обращаясь к истории принятия Конституции РФ, отмечает оригинальность российского конституционного идеала по

---

[1] Масловская Т.С. Новые направления конституционных реформ в зарубежных странах (динамика последних пяти лет) / Т.С. Масловская // Журнал зарубежного законодательства и сравнительного правоведения. – 2016. – № 4. – С. 83.

[2] Шахрай С.М. Конституция России: стабильность и развитие / С.М. Шахрай // Актуальные проблемы российского права. – 2018. – № 10(95). – С. 51.

[3] Умнова-Конюхова И.А. Конституция Российской Федерации 1993 года: оценка конституционного идеала и его реализация сквозь призму мирового опыта / И.А. Умнова-Конюхова // Lex Russia. – 2018. – № 11(144). – С. 23.

сравнению с конституциями других стран[1]. Предшествовавшая изменениям Конституции в марте 2020 года научная дискуссия, не будучи продолжительной, была достаточно интенсивной и предлагала к обсуждению вопрос о преобразованиях Основного закона, чего не скажешь об общественно-политической дискуссии, которая началась только после декларирования Президентом РФ в Послании Федеральному Собранию необходимости изменять Конституцию. Профессор Н.А. Власенко в статье «Модернизация Конституции России (к итогам обсуждения в связи с 25-летием)»[2], обобщая ее итоги, указал на предлагаемые варианты модернизации: неизменность, реформа, точечные изменения, отдавая предпочтение последнему варианту, для чего предлагал начать с проведения круглых столов по некоторым вопросам, а также устранить из Конституции идеологически и фактически себя не подтвердивших положений, в частности, о правовом государстве и социальном государстве. Интересно, что он отмечает тот факт, «что точку зрения о стабильности Конституции РФ, ее неисчерпаемом потенциале в период празднования 25-летия активно излагали профессиональные юристы-политики, прежде всего, работающие в системе представительной власти»[3], которые впоследствии приняли активное участие в разработке поправок и руководили рабочей группой, созданной в этих целях.

Если воспользоваться историко-сравнительным методом, то следует отметить, что процесс общественного обсуждения конституционных изменений в разные периоды отечественного развития выглядел по-разному. Обратить внимание на этот этап конституционных преобразований кажется нам важным, в связи с тем, что он, наряду с такими формами, как референдум (всенародное голосование) или общероссийское голосование, легитимизирует новые конституционные нормы. Так, впервые общественное

---

1 Ковлер А.И. Конституция России как сравнительный проект (к истории создания Конституции Российской Федерации) / А.И. Ковлер // Журнал зарубежного законодательства и сравнительного правоведения. – 2019. – № 1. – С. 8.

2 Вестник РУДН. Серия Юридические науки. – 2019. – Т. 23. – № 2.

3 Так, П. Крашенинников заявил следующее: «Дискуссии особенно жарко разгораются в период важных политических решений. Однако, возвращаясь к политической и правовой истории, стоит отметить, что первая советская Конституция действовала 12 лет. «Сталинская» – 41 год. «Брежневская» – 14 лет. «Ельцинская» работает уже 24 года. Есть надежда, что на этом чехарда с основными законами страны закончится, по крайней мере – на ближайшие сто лет». В достаточно большом материале автор не предложил ни одной позиции по совершенствованию Основного Закона. Другой профессионал-юрист и политик А.А. Клишас заявил следующее: «Конституция еще не исчерпала своих возможностей и справляется с основной функцией: быть механизмом разрешения противоречий между обществом и властью». В. Матвиенко накануне празднования 25-летия Конституции РФ дала большое интервью, помещенное в «Российской газете» Из него, можно заключить следующее: ничего менять в действующей Конституции не следует. По крайней мере, ни одной идеи, ни одной позиции предложено не было // Там же. См. также: Крашенинников П. Как рождалась наша Конституция / П. Крашенинников // Российская газета. 2017. 12 декабря; Клишас А.А. Путь к успеху – любовь к своему делу / А.А. Клишас // Дружба. 2018. 26 ноября; Матвиенко В. Закон прямого действия / В. Матвиенко // Российская газета. – 2018. – 12 декабря.

обсуждение изменяющейся Конституции было проведено в 1936 году. Оно продолжалось несколько месяцев, целями обсуждения стали: опора на широкие народные массы и преодоление пассивного сопротивления партии, первый шаг к идеологической консолидации общества. Данные по количеству участников и предложений при этом существенно разнятся[1]. Обсуждение народом проекта Конституции СССР 1977 длилось с мая по октябрь 1977 (май 1977 – решение о всенародном обсуждении, 04 июня – опубликована во всех газетах)[2].

Если подвергать анализу сроки конституционных процессов в России в целом (а не только этап предшествующего общественного или научного обсуждения), то по сути получается, что Конституция 1918 готовилась 6 месяцев (январь – июль 1918), начавшись с обобщения и сбора материалов сразу после III Всероссийского съезда Советов (10–18 января 1918)[3].

Конституция СССР 1936 года, принятая 5 декабря 1936 года, разрабатывалась около 2 лет[4]. Конституция РСФСР 1937 года – с 5–23 января 1935 по 15–21 января 1937 года, то есть тоже 2 года[5]. Конституция СССР 1977 года готовилась 15 лет (январь 1926 – рабочая группа подготовила предложения о разработке новой Конституции; 07 октября 1977 – принятие). Действующая Конституция России 1993 года – более 3 лет (42 месяца – с 12 июня 1990 по 12 декабря 1993 года), при этом одновременно в действующий текст Конституции РСФСР 1978 года в период с ноября 1991 года по декабрь 1992 года было внесено более 400 поправок. Широкого общественного обсуждения проектов Конституции за этот период не было.

Реформа российской Конституции 2020 года как официальная повестка со стороны публичной власти была заявлена Президентом РФ в ежегодной пресс-конференции 19 декабря 2019 г., когда глава государства отметил, что Конституция – «это живой инструмент, он должен соответствовать уровню развития общества». Президент, оценив возможности конституционных изменений, отметил, что «требуется хорошая подготовка и глубокая дискуссия в обществе»[6]. Такая дискуссия имела место на различных

---

1 Шершнева Е.А. Создание Конституции 1936 года : дис. … канд. юрид. наук. – М., 2011.

2 Лукьянов А.И. Разработка и принятие Конституции 1977 г. (1962–1977). – URL : https://constitution.garant.ru/history/ussr-rsfsr/1977/3001/ (дата обращения 10.01.2021).

3 Чистяков О.И. Конституция РСФСР 1918 года. – 2-е, изд. перераб). – «Зерцало-М», 2003.

4 Летом 1934 Сталин приступил к работе над подготовкой проекта; формально отсчет ведут от письма Сталина 25 января 1935 года (по другим данным – 06 февраля 1935 года, Постановление Съезда Советов СССР «О внесении некоторых изменений в Конституцию Союза ССР»).

5 Решение о составлении новой конституции было принято XVI Всероссийским Съездом Советов рабочих и крестьянских депутатов и она была принята Постановлением XVII чрезвычайного Всероссийского Съезда Советов рабочих и крестьянских депутатов от 21 января 1937 года «Об Утверждении Конституции (Основного Закона) РСФСР».

6 Стенограмма большой пресс-конференции В.В. Путина. – URL : http://prezident.org/tekst/stenogramma-bolshoi-press-konferencii-putina-19-12-2019.html (дата обращения 10.01.2021).

общественных площадках, включая Общественную палату Российской Федерации, а также публичные обсуждения с участием широкого круга представителей гражданского общества[1]. В составе рабочей группы по подготовке предложений о внесении поправок в Конституцию представителей общественности было преобладающее большинство, а предложения о поправках вносились непосредственно членам рабочей группы, а также в приемную Президента, при этом при общем количестве более девятисот, шестьсот поправок поступило именно от общественных объединений и граждан, и более трехсот учтены в тексте проекта[2]. 23 января 2020 года законопроект был принят в первом чтении, 10 марта – во втором, таким образом, возможный срок внесения предложений о поправках составил чуть больше месяца, при этом срок продлевался дважды. Профессор Т.Я. Хабриева, сопредседатель рабочей группы, комментируя сроки, отметила, что «например, статус конституционного совета Франции был изменен ровно за 30 дней с момента внесения до вступления в силу. В Бельгии в 2012 году внесение изменений в Конституцию заняло ровно 36 дней. Принятие Конституции Венгрии тоже заняло 36 дней»[3].

При принятии закона в первом чтении депутат О.Е. Смолин указал, что рабочая группа по доработке проекта «активно обсуждала вопрос о скорости прохождения законопроекта», а также о нецелесообразности сократить обычный срок – 30 дней – на 15-дневный, предложенный Комитетом по конституционному законодательству (который и был принят, но впоследствии продлялся)[4].

---

[1] Например, в феврале 2020 года слушания с участием руководителей и представителей более шестидесяти политических партий, общественных организаций, экспертно-аналитических сообществ, религиозных организаций подготовили обращение с предложениями поправок. – URL : https://ruskline.ru/news_rl/2020/02/07/poiniciativenarodnogo_sobora_sostoyalos_obwestvennoe_obsuzhdenie_popravok_v_konstituciyu (дата обращения 10.01.2021).

[2] Встреча с рабочей группой по подготовке предложений о внесении поправок в Конституцию. – URL : http://www.kremlin.ru/events/president/news/62862 (дата обращения 10.01.2021).

[3] Поправка в календарь. Срок подачи предложений по изменению Конституции продлили до 14 февраля. – URL : https://rg.ru/2020/02/04/srok-podachi-predlozhenij-poizmeneniiu-konstituciiu-prodlili-do-14-fevralia.html (дата обращения 10.01.2021).

[4] Текст стенограммы заседания 272(1820) от 23.01.2020 // Бюлл. № 272 (1820). – Ч. 1. – С. 11–74. Председатель Думы В.В. Володин отметил: «Эти поправки выстраданы, причём начиная ещё со времён императорской России, потому что не было у нас тогда парламентаризма, только парламент был образован – его распустили, затем была революция, потом у нас была Страна Советов, при этом органы советской власти полномочий тоже не имели, потом мы знаем, какие в новой России были полномочия, этот вопрос мы не раз обсуждали. Те же стандарты: правильно сказал Геннадий Андреевич о самой лучшей Конституции, но эта Конституция была в советское время во многом декларацией, ведь расслоение общества тоже было - на партноменклатуру и на тех, кто работал». – URL : //http://cir.duma.gov.ru/duma/document/text/?doc_id=373900&QueryID=5025&HighlightQuery=5025&query_target=news

Определяя сроки современны конституционных преобразований, важно учитывать, что с принятием поправок в марте 2020 года реформа только началась – изменение основного текста Конституции потребует принятия или изменения большого количества актов конституционного законодательства, а это предполагает длительную работу законодателя.

Рагер Ю.Б.,
кандидат исторических наук, доцент,
доцент кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУ ВО «РГУП»
г. Краснодар

ЦИФРОВАЯ ИСТОРИЯ КАК ЧАСТЬ ВСЕОБЩЕЙ ЦИФРОВИЗАЦИИ: ПЕРСПЕКТИВЫ РАЗВИТИЯ

Технический и вслед за ним социальный прогресс современной информационной эпохи двояко воздействует на общество, создавая более эффективные и облегчающие жизнь условия существования человечества, но при этом, формируя крайне опасные условия для манипуляции общественным сознанием и формирования общественным мнением, о которых нельзя было подумать еще в 1990-х годах 20 века.

Цифровизация оказалась разносторонней и многообразной. Она охватывает и серьёзные области науки и развлечения, «рискуя» стать всеобъемлющей и буквально поглотить мир. Думаем, что многое в её несомненных подвигах и открытиях на благо человечества ещё впереди.

«Цифровизация» затронула процессы бурного развития цифровой инфраструктуры и вносит сегодня большой вклад в более эффективное, чем раньше сохранение всего наследия человечества. Идет процесс «оцифровывания», а значит и сохранения в перспективе до бесконечности всех достижений человеческой мысли, культурных ценностей, исторических объектов и источников[1]. История и культура становиться более доступной и открытой. Но при этом находит своё место и ложная информация, различные фейки и замена фактов нарративами, позволяющих в перспективе управлять представлениями о прошлом, навязывать ложные точки зрения.

За последние десятилетия сложилось важное направление получившее название Digital Humanities – цифровые гуманитарные науки. В его

[1] Шпырня О.В. Использование информационных технологий в подготовке кадров для индустрии туризма / О.В. Шпырня, А.А. Юрченко // Теоретические и прикладные аспекты формирования информационного и правового пространства в современном мире : Материалы Междун. Рос.-казах. науч.-практ. конф. – Краснодар : Издательский Дом – Юг. – С. 124–126.

рамках существует Digital History – цифровая история. Это симбиоз, результат межпредметного взаимодействия академических гуманитарных наук и мощи современных цифровых технологий[1]. Правда историки в большинстве своём рассматривают этот союз как прикладной призванный справиться с систематизацией и анализом резко возросших информационных потоков, с которыми традиционная инфраструктура уже давно не справляется. Причина вполне очевидна – глобальный взрывной рост цифровой информации. Современную информацию сложно длительно хранить, что порой приводит серьезным курьёзам. Поэтому, не смотря на прикладной характер, цифровая история уверенно развивается, в том числе и в получившем массовый характер в последние годы вовлечении в процесс исторических исследований массы людей, которые хотят узнать и сохранить в информационной памяти потомков свои родословные, жизнь отдельных людей, истории отдельных местностей, городов регионов и пр. Цифровая история обеспечивает технологические возможности реконструкции событий. Она активно представлена сегодня в блогосфере. Можно со всей определенностью сказать, что её развитие важный этап развития исторической науки.

Обращение к истории в информационном обществе полно негативных явлений. Это широкое использование различных нарративов (выдуманных опирающихся только на мнение автора псевдоисторических произведений), фейковых новостей (откровенно ложных, извращающих истину утверждений) и явно необъективной и совершенно ненаучной информации, но в большинстве своем процесс «демократизации истории», её «народности» вызывает интерес и может быть рассмотрен позитивно. Даже поверхностный анализ интернета показывает глобальную вовлеченность общества в проблемы истории.

Digital Humanities или цифровой гуманизм меняет представление о формах и методах гуманитарных и исторических исследованиях в цифровую эпоху. Например, оцифровывание архивных источников и книг, каталогизация, развитие межличностных коммуникаций посредством создания благоприятной исследовательской «экосистемы», а процесс «демократизации истории» через значительное расширение исторических источников об отдельных регионах, социальных группах, семьях, жизни конкретных людей, размещаемых в информационной среде. Необходимо отметить, кардинальные сдвиги произошли в отношении источниковой базы, особенно той, которая формируется именно сейчас. Её запечатливание или картирование позволяет создать такие массивы информации о современной эпохе, как по объему, так и по разнообразию, которые до начала 21 века были технически невозможны. В этой связи возникает важный технический вопрос, как эту информацию можно будет долговременно, а лучше бессрочно сохранять?

---

[1] Поддубная Т.Н. Контрольно-измерительная процедура оценки сформированности компетенций обучающихся (на примере подготовки кадров высшей квалификации) / Т.Н. Поддубная, А.А. Юрченко // Вестник Майкопского государственного технологического университета. – 2020. – № 1(44). – С. 86–94.

Цифровизация пока окончательно не ответила на вопрос о сохранении всех цифровых источников при общей тенденции исчезновения материальных основ носителей информации.

Однако, начиная с 2000 года процесс информатизации (цифровизации) получает динамизм и широкую государственную поддержку в виде общефедерального нормативного документа «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[1]. Следовательно, 2020 год является начальным этапом его исполнения. Это означает, что страна реализовывает его положения и запланированные действия.

Документ характеризует общие тенденции и проблемы развития цифровой среды. Негативное её влияние определяется как «смещение акцентов в восприятии окружающего мира, особенно в сети «Интернет», с научного, образовательного и культурного на развлекательно-справочный сформировало новую модель восприятия – так называемое клиповое мышление, характерной особенностью которого является массовое поверхностное восприятие информации…».

Целью «Стратегии…» в рамках глобального процесса цифровизации с его не только плюсами, но и минусами является формирование в нашей стране общества знаний. Данная цель предполагает решение простых и сложных задач, охватывающих процесс формирования «информационного пространства знаний»[2].

Цифровизация позволяет сохранить и донести до массового потребителя громадное количество информации, имевшей до этого только бумажные носители и поэтому очень ограниченные возможности для сохранения и распространения. Оцифрованные документы целенаправленно заменяют архивные дела. Тоже касается редких изданий книг, особенно находящихся на хранении в зарубежных хранилищах. Оцифрованные или размещенные в виде фотографий бесценные материалы, безусловно, расширили и обогатили возможности для изучения. Приходится признать, что цифровизация не превратилась в нечто самодостаточное и самостоятельно развивающееся явление. Архивы и библиотеки оказались не в полной мере готовы к полноценной работе по удалённой схеме.

Сложно рассуждать о современности с позиции историка. Являясь современником событий, можно легко ошибиться в оценке происходящего или совершить, по крайней мере, две большие ошибки. Первая – это переоценка «судьбоносности» того, что происходит. Другой, явной ошибкой, является недооценка событий и явлений. Пожалуй, это меньшая ошибка, но «не увидеть», а значит и неправильно сделать выводы, оценить можно

---

[1] О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы. – URL : http://www.consultant.ru / (дата обращения 01.10.2020).

[2] О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы. – URL : http://www.consultant.ru / (дата обращения 01.10.2020).

многое. Поэтому следует, воздержимся от окончательных выводов и оценочных заключений при рассмотрении современной эпохи – эпохи информационных или цифровых технологий. Хотя бы потому, что выводы и заключения, сделанные 10–15 лет назад, в оценке этой эпохи, сегодня выглядят довольно поверхностными и неоднозначными. Да и более современные утверждения 8-ми и даже 5-летней давности показывают нам, как быстро развивается мир и в какие исторические условия человечество сегодня попадает.

Тем не менее, процесс освоения новых цифровых технологий ускорился в последние годы по объективным причинам. Исторической науки это коснулось, прежде всего, в усилении дигиталицации или перевода в цифру письменных носителей информации и развитие тех направлений, о которых было сказано выше. Но только сейчас в последнее десятилетие начинает постепенно обретать единство и системность.

Хотелось подчеркнуть, нам современникам очень сложно оценивать это явление и определить, на сколько оно влияет на общественное сознание. Данное влияние имеет как позитивную, так и негативную стороны. Мы можем бесконечно говорить о многочисленных искажениях истории, об извращении истины, большого количества лжи и политической ангажированности тех, кто это делает. Но далеко не только они «делают погоду» на исторических форумах и в YouTube каналах. Много информации даётся объективно и искренне. Это заставляет активно участвовать в информационном процессе большую плеяду профессиональных историков, готовить адаптированные для неискушённой аудитории исторические повествования.

Один вывод мы можем сделать уже сегодня. О монополии профессиональных ученых историков на изложение и интерпретацию исторических фактов и событий можно забыть навсегда. «Цифровая история», опирающаяся на постоянно возрастающее могущество интернета, разрушила окончательно эту монополию, предоставив право конкурировать с учёными любому желающему, где главным критерием успеха являются не статьи в научных журналах и индексы цитирования, а количество посещений канала, голосование лайками, количество подписчиков и объемы перечисленных спонсорских и благотворительных средств.

Современный цивилизационный вызов, требует от нас напряжения сил и неординарных смелых решений. От правильного выбора будет зависеть перспективы развития всего общества и современной исторической науки в том числе. Все усилия, направленные на развитие цифровизации должны привести к качественному росту и её развитию.

Стамкулова Г.А.,
кандидат юридических наук,
доцент кафедры юриспруденции
и международного права,
Университет «Туран»
г. Алматы

НЕКОТОРЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОГО, ОБРАЗОВАТЕЛЬНОГО И ПРАВОВОГО ПРОСТРАНСТВА В ПРОЕКТЕ «КОНЦЕПЦИИ РАЗВИТИЯ ВЫСШЕГО ОБРАЗОВАНИЯ В РЕСПУБЛИКЕ КАЗАХСТАН ДО 2025 ГОДА»

Система высшего образования направлена на воспроизводство кадров высшей квалификации и должна гибко и адекватно реагировать на перспективные и текущие задачи общественного развития

В современный период для системы высшего образования в Казахстане существуют следующие вызовы: пандемия COVID-19; цифровое неравенство; замедление экономического роста; расширение автономии вузов; востребованность в softs kills: лидерство, предприимчивость, навыки коммуникации; низкая приоритетность научной деятельности; слабое взаимодействие вузов и производства; слабый управленческий потенциал вузов; недостаточно развитая инфраструктура и лабораторная база вузов; недостаточная прозрачность принимаемых решений в вузах. Эти вызовы учтены при разработке «Концепции развития высшего образования» (далее- Концепция) до 2025 года, которую представили для обсуждения общественности, определив, что необходимо выработать меры по повышению конкурентоспособности системы высшего образования в условиях глобальных вызовов и требований рынка труда, формированию исследовательской и цифровой экосистемы вузов с учетом новых технологий, что обеспечит вклад в социально-экономическое и научно-техническое развитие Казахстана.

В Концепции поставлено 10 основных задач:

1. Создание условий для равного доступа молодежи к высшему образованию и реализации их личностного и профессионального потенциала на основах справедливости
2. Подготовка педагогов, способных формировать в своих учениках метакомпетенции для их личного благополучия и процветания страны
3. Повышение конкурентоспособности высших учебных заведений
4. Формирование современной академической, исследовательской, управленческой и инфраструктурной экосистемы вузов, интегрированной в национальный и региональный контекст
5. Формирование однородной институциональной системы вузов, развитие менеджмента вузов, формирование пула прогрессивных лидеров высшего образования

6. Повышение конкуренции среди вузов путем открытия кампусов зарубежных университетов.

7. Гармонизация Национальной системы обеспечения качества, основанной на принципах институциональной инклюзии и академической честности.

8. Формирование адаптивности системы оценивания результатов обучения и достижений обучающихся с учетом форм обучения в течение всей жизни.

9. Формирование ценностно-патриотического мировоззрения обучающихся

10. Развитие вузовской науки для увеличения интеллектуального вклада в науку, экономику страны[1].

В законе Республики Казахстан «Об образовании» закреплена следующая структура высшего профессионального образования:

Высшее базовое образование – программа бакалавриата – с продолжительностью обучения 4 года.

Обучающемуся, прошедшему итоговую аттестацию по освоению образовательной программы высшего образования, присуждается степень «бакалавр» или присваивается квалификация «специалист».

Послевузовское образование осуществляется в магистратуре, резидентуре и докторантуре организаций высшего и (или) послевузовского образования, научных организаций по основному профилю деятельности и направлениям подготовки кадров. Подготовка кадров в магистратуре осуществляется на базе образовательных программ высшего образования по двум направлениям:

1) научно-педагогическому со сроком обучения не менее двух лет;
2) профильному со сроком обучения не менее одного года.

Подготовка кадров в докторантуре осуществляется на базе образовательных программ магистратуры по двум направлениям:

1) научно-педагогическому со сроком обучения не менее трех лет;
2) профильному со сроком обучения не менее трех лет.

Основными видами организаций высшего и (или) послевузовского образования являются национальный исследовательский университет, национальная организация высшего и (или) послевузовского образования, исследовательский университет, университет, академия, институт и приравненные к ним (консерватория, высшая школа, высшее училище). Формирование многоуровневой структуры высшего образования направлено на обеспечение многоступенчатости по вертикали и альтернативности по горизонтали, динамичности, гибкости подготовки специалистов, ее фундаментальности и универсальности одновременно.

---

[1] Концепции развития высшего образования до 2025 года. – URL : https://enic-kazakhstan.kz/files/1605782374/koncepciya-razvitiya-vysshego-obrazovaniya-do-2025-goda.pdf

Тенденцией развития высшего образования является повышение качества подготовки специалистов, обеспечение новых направлений подготовки, инновационного развития, интеграция с интенсивной научно-исследовательской деятельностью, тесная связь вузовских исследований с потребностями общества на основе совершенствования образовательных и информационных технологий.

Для реализации основных целей Концепции есть некоторые достижения и проблемный вопросы.

Для повышения конкурентоспособности высшего образования развитые страны инвестируют в научно-исследовательский потенциал университетов. По версии рейтинга мировой конкурентоспособности IMD-2018, США, Гонконг, Сингапур, Нидерланды, Швейцария входят в пятерку стран, где высшее образование отвечает потребностям экономики. Казахстан занимает 38-е место среди 63 стран мира[1].

Для повышения доступа к высшему образованию число государственных грантов на подготовку кадров в 2020–2021 году достигло рекордной цифры (на бакалавриат 53864 гранта (в прошлом году 53785). на магистратуру – 13300 (в прошлом году 13179); на докторантуру – 2355 (в прошлом году 2315).

Для совершенствования образования и науки утверждена Постановлением Правительства Республики Казахстан от 27 декабря 2019 года № 988 «Государственная программа развития образования и науки Республики Казахстан на 2020–2025 годы».

За последние 3 года проведена большая работа по правовому регулирования высшего образования. Результатом активной нормотворческой работы стало принятие в июле 2018 г. Закона о внесении дополнений в закон «Об образовании». В нем предусмотрено внесение изменений в 4 кодекса и 15 законов. Всего было внесено 200 поправок, из них 125 являются новыми, то есть не были предусмотрены законопроектом, и 75 предусматривают корректировки норм, предложенных ранее законопроектом, расширяющего полномочия вузов. Закон предусматривает расширение полномочий вузов в академических, управленческих и финансовых вопросах. Министерством в ведение вузов переданы 24 компетенции. Теперь вузы могут самостоятельно разрабатывать и утверждать правила приема в вуз, образовательные программы, присуждать студентам степени «бакалавр» и «магистр», создавать эндаумент-фонд, юридические лица по научно-образовательной деятельности, стартап-компании, филиалы в иностранных государствах, привлекать дополнительные источники финансирования и др.

Дальнейшим шагом развития самостоятельности должна стать проработка механизмов внедрения автономии вузами и оказание научной и методической поддержки вузам в ее реализации. Для эффективного внедрения

[1] IMD (2018), IMD World Competitiveness Rankings 2018 Results. – URL : https://www.imd.org/wcc/worldcompetitiveness-center-rankings/world-competitiveness-ranking-2018

автономии необходимо проводить постоянный мониторинг эффективности реализации автономии вузами и обучающие тренинги для АУП и ППС в вопросах академической, управленческой, финансовой и кадровой самостоятельности.

Отсутствие у студентов навыков предприимчивости и понимания механизмов коммерциализации является основным вызовом на пути к внедрению студенческих стартапов. Задача вузов заключается в создании условий для стартаперов, обучении их навыкам предпринимательской деятельности, поиске инвесторов для реализации бизнес-идей. Профессиональные пробелы можно восполнить участием вузов в акселерационных программах. На данных программах стартаперы получают навыки ведения бизнеса, в частности, выстраивания операционных процессов и работы с финансовой отчетностью.

Другой проблемой является копирование казахстанскими вузами зарубежных идей, бизнес-моделей и концепций. Необходимо продвижение собственных идей с учетом экономических, региональных, экологических, географических и климатических условий Казахстана.

Обеспечение качественного высшего образования – вопрос высокой важности как для студентов, ППС и вузов, так и для всего общества. Казахстан входит в число стран –не членов ЕС, где национальная система обеспечения качества строится на основе европейских стандартов. В системе высшего образования республики внедряются Европейские стандарты и принципы обеспечения качества (The Standards and Guidelines for Quality Assurance in the European Higher Education Area, ESG). С января 2017 года государственную аттестацию вузов заменила международная аккредитация. Проводится процедура независимой аккредитации вузов (институциональная аккредитация) и образовательных программ (специализированная аккредитация). В Национальном реестре аккредитационных органов 10 агентств. По итогам 2018 г. институциональную аккредитацию прошли 110 вузов. Рассматривая специализированную аккредитацию, на уровне бакалавриата аккредитовано 2111 образовательных программ, магистратуры – 1214, докторантуры – 316.

С началом пандемии была необходима полная определенность с дистанционным обучением, поскольку это влияет на практику и правоприменение в сфере образования. В закон «Об образовании» внесена отдельная норма, что в случаях введения чрезвычайного положения, ограничительных мероприятий, в том числе карантина, на соответствующих административно-территориальных единицах (на отдельных объектах), объявления чрезвычайных ситуаций местные исполнительные органы и организации образования вводят дистанционное обучение для всех обучающихся в порядке, определяемом уполномоченным органом в области образования. Дистанционное обучение осуществляется в организациях среднего, дополнительного, технического и профессионального, после среднего, высшего и (или) послевузовского образования в порядке, определяемом уполномоченным органом в области образования.

Казахстан, наряду с 48 странами, принял на себя обязательства по исполнению параметров Болонского процесса, в том числе по обеспечению качества высшего образования. Качественное высшее образование подразумевает приверженность ценностям и принципам, развивающим личную честность в обучении и оценивании, другими словами, соблюдение академической честности.

Для улучшения качества системы оценки знаний студентов была создана Лига академической честности стало ответом на назревшую необходимость объединения ведущих вузов в борьбе за обеспечение качества высшего образования. Кроме того, она соответствует рекомендации ОЭСР (Организация экономического сотрудничества и развития) по совершенствованию прозрачности управления государственными и частными вузами. Цель Лиги академической честности лежит в повышении качества высшего образования, противодействии плагиату, неприятии коррупции в обществе. С учетом расширения самостоятельности вузов необходимость в продвижении принципов академической честности в вузах будет только расти.

Видение Лиги академической честности – довести до рынка труда только самых лучших и конкурентоспособных выпускников. Университеты в составе Лиги возьмут обязательства выпустить не более 60 % выпускников от общего числа поступивших студентов. Так, Лигой была утверждена медиана оценок, т.е. принцип ранжирования оценок. Согласно данному новшеству, оценки «отлично» (A, A–) и «хорошо» (B, B–) могут получить не более 35 % от всех студентов группы, а оценку «неудовлетворительно» (F, FX) – не менее 10 %. При этом не менее 55 % от всех студентов должны получить оценку «удовлетворительно» (C, C–, D+, D).

Большое значение отведено подготовке педагогов, способных формировать в своих учениках метакомпетенции для их личного благополучия и процветания страны. Достижения студентов в значительной степени зависят от мотивирующей академической среды, создаваемой опытным и увлеченным ППС. Успехи студентов зачастую зависят от способности преподавателя эффективно организовывать занятия и проявлять экспрессию. Экспрессия, т.е. сила выражения преподавателем своих чувств, оказывает огромный эффект на посещаемость лекций и объем домашней работы, выполняемой студентами Данные качества выражаются в умелом планировании силлабуса своей дисциплины, структурировании предметного материала, выборе увлекательных тем и заголовков, подготовке эксклюзивных презентаций и кейсов, поддержании атмосферы соучастия в обучении. Очень важно, чтобы академическая среда, в которой пребывает преподаватель, способствовала именно такому пониманию «качественного преподавания». В этом случае продолжительность опыта ППС будет влиять на усваиваемость материала студентами. Соответственно, чем дольше преподаватель работает в такой среде, тем лучше развиваются навыки преподавания, что, в свою очередь, повышает уровень знаний студентов.

Впервые число казахстанских вузов, отмеченных в рейтинге QS WUR, увеличилось до десяти. В 2018 г. казахстанские вузы дебютировали в

рейтинговом издании Times Higher Education. Данные достижения свидетельствуют о международном признании казахстанского высшего образования. Вузам необходимо постоянно реагировать на вызовы рынка труда и конкурировать за преподавателей, студентов, научные гранты и другие ресурсы.

Для решения поставленных в Концепции задач, разделе «Структура концепции» определены основные мероприятия.

Для реализации управленческой самостоятельности – внедрение стратегического корпоративного менеджмента, формирование новых лидеров высшего образования, развитие кадрового потенциала и новая архитектура организационной структуры вузов.

Казахстан участвует в Европейском пространстве высшего образования, нужна реализация глобальных образовательных программ, создание Центрально-азиатского хаба высшего образования.

Один из разделов Концепции посвящен цифровой трансформации вузов. Определена следующая модель. Для подготовки кадров в сфере здравоохранения, хореографии, авиационной техники – не более 30 кредитов будет в формате ДОТ, для подготовки кадров, связанных с безопасностью людей – не более 20 % дисциплин.

Планируется открытие цифровых университетов с отдельными требованиями к ним. Будут применяться отдельные цифровые инструменты как дополнение традиционных решений онлайн и смешанное обучение - «Интеллектуальное» обучение на основе интегрированных цифровых систем.

Концепция содержит ожидаемые результаты, определены качественные и количественные показатели.

Терентьев И.А.,
кандидат философских наук, доцент
кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

СОЦИАЛЬНО-ФИЛОСОФСКИЙ АНАЛИЗ ТЕНДЕНЦИЙ РАЗВИТИЯ ПРАВОВОГО ПРОСТРАНСТВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА

Правовое пространство, также как и все иные элементы правовой системы испытывает трансформирующее воздействие процессов цифровизации. Безусловно, существенные признаки правового пространства не теряют своих качеств, никуда не уходит понятие правовой границы, правовых явлений, в совокупности определяющих правовую природу этого вида

пространства. Однако происходит расширение наших представлений о возможностях формы, а в некоторых случаях и содержания правового пространства.

Вообще, термин «правовое пространство» играет важную роль в современной социально-философской и теоретико-правовой науке, так как позволяет отделить этот вид пространства от других, например, экономического, культурного, политического и т.д. Правовое пространство неразрывно связано и определяется совокупностью действующих нормативно-правовых актов, механизмом правового регулирования, пределами и объемами прав и обязанностей человека и гражданина, обеспечиваемых и защищаемых государством и т.д. Являясь социальным феноменом, правовое пространство испытывает влияние всех факторов, которые определяют развитие социальных процессов.

В настоящее время одним из важнейших факторов, оказывающих большое влияние на общество в целом и на правовое пространство в частности, является цифровизация. Она привела к тому, что многие виды социальных отношений получили возможность реализовываться в виртуальном пространстве. Это породило проблему отсутствия правового регулирования социальных отношений в условиях интернет-пространства. Учитывая, что субъектами социальных отношений в виртуальном пространстве остаются все те же граждане, права которых обеспечивает и защищает государство, и которые остаются незащищенным в интернет-пространстве, например, от нарушения их права на неприкосновенность частной жизни, на защиту чести, достоинства и деловой репутации, соблюдение авторского права на произведение и т.д., становится очевидным, что требуется внесение существенных изменений в механизм правового регулирования, который должен действовать и в виртуальном пространстве.

Таким образом, сегодня можно говорить о задаче синхронизации правовых гарантий гражданам как в реальной действительности, так и в виртуальной. Связующим звеном этих уровней социальных отношений выступает гражданин и человек, права которого гарантируются международными правовыми нормами и внутринациональным правом.

С точки зрения социальной философии перед исследователями стоят задачи постижения общего и особенного в аспекте цифрового правового пространства, выявления его противоречий, тенденций и перспектив развития. При этом надо понимать, что цифровое правовое пространство имеет свою специфику, особенности, характеризуется отсутствием физического контакта участников диалога или беседы, отсутствием контроля, ролевым общением, возможностью коммуникации с людьми разных стран, правовых систем.

Возможности интернета заключают как большие позитивные возможности для развития человека, получения нового знания, быстрого обмена информацией и т.п., так и негативные, асоциальные последствия. Ведь определенная анонимность поведения в интернет-пространстве и возможность

уйти от ответственности порождает кражи персональных данных, распространение ложной информации, создание фейковых аккаунтов, заказную дискредитацию деловой репутации человека или фирмы и т.д. Кроме того, необходимость формирования цифрового правового пространства порождается острой необходимостью защиты несовершеннолетних граждан от противоправной информации и преступлений.

Сегодня а интернете создаются скрытые сети, позволяющие вести незаконную деятельность: торговать наркотиками, органами, нелегальным оружием и т.д. Все это говорит о том, что цифровое правовое пространство имеет менее выраженные границы и подвержено нарушениям в силу активного использования технических средств. Это в определенной степени отличает его от нецифрового правового пространства. При этом следует подчеркнуть, что цифровое правовое пространство нельзя рассматривать как нечто самостоятельное, так как оно выступает лишь как вид правового пространства.

Как верно заметили И.В. Понкин и А.И. Редькина, цифровое правовое пространство отличается неоднородностью, что выражается в существовании двух его форм: пассивное цифровое (виртуальное) пространство, где программно-компьютерными средствами воссоздано правовое пространство и активное цифровое (виртуальное) пространство, в котором вся нормативно-правовая масса принудительно релевантно упорядочивается (иерархизируется), автоматизируется и администрируется[1]. Такая неоднородность порождается техническим основанием цифрового правового пространства.

Завершая рассуждения об особенностях правового пространства в условиях цифровизации следует подчеркнуть, что несмотря на то, что право – это универсальный регулятор, однако и в интернет-пространстве не все может подлежать правовому регулированию. Всегда остаются такие грани отношений между людьми, которые регулируются иными регуляторами, например, религией, моралью, саморегулированием[2]. Иными словами, сегодня происходит активное формирование цифрового правового пространства, ставящее перед законодателем и учеными такие задачи, решение которых раскрывает новые грани возможностей и пределов правового регулирования.

---

[1] Понкин И.В. Цифровые онтологии права и цифровое правовое пространство / И.В. Понкин, А.И. Редькина // Пермский юридический альманах. – 2019. – № 2. – С. 31.

[2] Залоило М.В. Фрагментация как современная тенденция развития правового пространства / М.В. Залоило // Право. Журнал Высшей школы экономики. – 2020. – № 4. – С. 31.

Шевченко А.И.,
доктор философский наук, доцент,
профессор кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

ФИЛОСОФСКОЕ ОСМЫСЛЕНИЕ ПРОЦЕССА ИНФОРМАЦИОННЫХ КОММУНИКАЦИЙ

Информационное взаимодействие – это один из базовых аспектов существования общества. И хотя термин «информация» используется, преимущественно, применительно к вычислительным процессам и механизмам опосредованной техническими средствами коммуникации, данное понятие существенно шире и включает в себя многообразные результаты познавательной и творческой деятельности. Еще до возникновения таких средств запечатления информации, как фотография и аудиозапись, и даже до возникновения письменности существовали механизмы передачи знания, реализованные в языковой форме. Именно способность к передаче знания от одного человека к другому определили развитие общества и его постепенный переход к тому состоянию, которое мы наблюдаем в настоящее время. И, безусловно, изменения в условиях осуществления информационного обмена являются в данном случае событиями, определяющими развитие цивилизации[1].

В этом контексте представляет интерес то, что процессы информационного взаимодействия не статичны – они подлежат изменению как в содержательном плане, так и в плане совокупности существующих форм информационного взаимодействия. Немаловажно и то, что со временем возникают новые механизмы запечатления и передачи информации и трансформируются существовавшие ранее. Все это заставляет взглянуть на область информационного взаимодействия с точки зрения ее процессуальности и, соответственно – изменчивости. А с учетом того, насколько большое значение имеет информационная коммуникация для общества, речь идет о том, что непрерывному развитию подлежит один из базовых аспектов его существования. Все это заставляет обратиться к изучению информационного аспекта общественной жизни и, в частности, поставить вопрос о том, какое конкретно влияние оказывает на общество развитие (и изменение) области информационного взаимодействия.

Существует два основных подхода к аналитике информационного взаимодействия и его влияния на общество – рассмотрение общих принципов

[1] Маклюэн М. Понимание медиа: внешние расширения человека. – М. : Кучково поле, 2007.

и взаимосвязей между состоянием информационно-коммуникационной среды и системой общественных отношений и конкретно-исторический анализ, ухватывающий актуальные для определенного исторического промежутка тенденции. В настоящей работе целесообразно совместить указанные подходы, поскольку тематика исследования предполагает освещение проблемы информационной коммуникации на общем уровне, однако отдельные уникальные (в особенности это применимо к современности) тенденции требуют рассмотрения, актуально развертывающихся в информационной среде процессов.

Начнем с базового для теории коммуникации понятия канала коммуникации. Данное понятие отображает способ запечатления, передачи и воспроизведения информации. Понятие канала коммуникации включает в себя не только указание на форму, которую принимает информация, но также и отражение средств, при помощи которых эта информация запечатлевается, хранится и передается. Исторически первым каналом коммуникации являлась устная речь, относящаяся к аудиальной форме информации; вместе с тем, аудиозапись и дальнейшая трансляция человеческой речи по радио представляют собой уже принципиально иной канал коммуникации, поскольку здесь идет речь о принципиально иных механизмах донесения информационного сообщения до адресата, опосредованных технической аппаратурой, а также об иных характеристиках аудитории информационного сообщения, масштабе информационного взаимодействия, его скорости и т. д.. Точно так же, например, письменность представляет собой иной по отношению к печатному слову канал коммуникации, в силу различий по представленным выше критериям.

События в информационно-коммуникационной сфере, так или иначе, тесно связаны с проблематикой каналов коммуникации. Здесь можно выделить следующие возможные варианты:

– возникновение нового канала коммуникации;
– изменение востребованности определенного канала коммуникации;
– деактуализация определенного канала коммуникации.

Каждый канал коммуникации обладает определенными возможностями и, одновременно с этим – определенными ограничениями, которые задают конечное влияние данного способа информационного взаимодействия на общество и культуру в целом. При этом, говоря об определенном канале коммуникации, мы, чаще всего, говорим о комплексном средстве информационного взаимодействия, включающем в себя не только средства передачи информации, но и средства ее накопления (и сохранения). Насколько это является важным можно легко проиллюстрировать на примере классических литературных произведений, которые дошли до нашего времени только благодаря тому, что были когда-то записаны.

Возможность запечатления информации является одним из ключевых факторов ее накопления, при этом, возникновение определенного способа запечатления информации на материальном носителе становится одним из

факторов, стимулирующих процессы производства подобного рода информации и, в целом, ее приумножения в культурной среде. С возникновением письменности возникла литература, способность запечатлевать звук стала основанием для развития музыки, возможность видеосъемки породила огромный пласт культуры, связанный с кинематографом, мультипликацией, игровыми телепрограммами и т.д. И здесь мы рассматриваем два аспекта понятия «возможность» применительно к сфере информационной коммуникации: с одной стороны, речь идет о технической возможности определенного способа оперирования информацией, с другой – подразумевается возможность, которая возникает у человечества (или, как минимум, отдельных его представителей) благодаря возникновению определенной технологии. В качестве примера можно привести письменность, которая породила возможность накопления знаний людьми. Благодаря возникновению письменности стал возможным первый серьезный цивилизационный скачок, связанный с накоплением такого количества знаний, которое дало основу для формирования философии и науки. Следующим значимым событием для общества и культуры стало возникновение печатного станка, который, фактически, сделал возможным массовое изготовление печатной (в плане применяемой символической системы – той же письменной) продукции, что впервые сделало возможным массовое тиражирование информации1.

Рассматривая в данном ключе процесс развития системы информационных коммуникаций, мы можем выделить следующие его стороны:

– техническая (изобретение средств запечатления, хранения, передачи и воспроизведения информации);

– культурная (возникновение и обширное развитие пластов культуры, относящихся к конкретному каналу коммуникации, взаимодействие носителей различных культур посредством средств коммуникации, приобщение к культурным продуктам, относящимся к другой культуре и доступным благодаря информационно-коммуникационному процессу);

– социально-обусловленная (влияние социальных факторов на информационные отношения, например, доступ к определенным каналам коммуникации, связанный с социальным статусом, уровнем образования, материальными возможностями по использованию определенных технических средств коммуникации);

– социально-детерминирующая (влияние информационно-коммуникативных процессов на общество, например – воздействие определенных разновидностей масс-медиа на общественное сознание, реализация социализационной, политической, образовательной функций посредством существующих каналов коммуникации и т.д.).

По мере развития системы информационных отношений, наблюдается последовательный и неуклонный рост уровня приобщения членов

---

[1] Маклюэн М. Галактика Гутенберга. Становление человека, печатающего / М. Маклюэн; Пер. с англ. И.О. Тюриной. – М. : Академический Проект, 2020.

общества к новым каналам коммуникации (что происходит, впрочем, за счет частичного оттока внимания массовой аудитории от ранее существовавших медиа). Речь идет как о росте доступности новых средств коммуникации (в немалой степени за счет научно-технического прогресса и конкуренции между компаниями, обеспечивающими информационные услуги), так и о росте их востребованности, связанном с возникновением нового, соответствующего возникшему каналу коммуникации, формата культурной продукции.

На протяжении всего XX века и в течение первых двух десятилетий XXI века наблюдается тенденция неуклонного роста уровня информационного взаимодействия, связанного с развитием технического обеспечения информационных отношений, и одновременно с этим можно констатировать колоссальное увеличение влияния информационных процессов на состояние общества. Информационные процессы в настоящее время составляют существенную долю экономических, политических, образовательных отношений, они влияют на состояние института семьи (в частности, в настоящее время уже существует прецедент формирования семей между людьми, познакомившимися в Интернете). Все это позволяет судить о том, что информационные процессы оказывают глубочайшее влияние на современное общество, и многие из аспектов этого влияния нам еще лишь предстоит осознать. Вместе с тем, с учетом того, что всякий канал коммуникации имеет свои возможности и свои ограничения, хотелось бы отметить важность научно-философского анализа, с одной стороны, возможностей современных технологий информационной коммуникации, с другой – рисков, связанных с современным развитием информационных технологий (на основании понимания которых их возможно определенным образом ограничивать или, как минимум, регулировать отдельные аспекты их направленности).

Раздел 2

Информационные технологии как инструмент создания информационного, образовательного и правового пространства

Бегларян М.Е.,
кандидат физико-математических наук,
доцент, заведующий кафедрой
социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

Добровольская Н.Ю.,
кандидат педагогических наук, доцент,
доцент кафедры информационных технологий,
ФГБОУ ВО «КубГУ»
г. Краснодар

ЭКСТРАГИРОВАНИЕ СТУДЕНЧЕСКИХ СООБЩЕСТВ НА ОСНОВЕ ДАННЫХ СОЦИАЛЬНЫХ СЕТЕЙ

В настоящий момент социальные сети являются не только основной площадкой для общения, но и источником различной количественной и качественной информации о пользователях. Мониторинг данных, которые предоставляют пользователи сети самостоятельно (пол, возраст, интересы, место жительства), наборы подписок пользователей, анализ реакции пользователя на то или иное сообщение, позволяет многим коммерческим компаниям выполнять анализ популярности или востребованности того или иного тренда или продукта. Подобные технологии можно применять не только при продвижении некоторого бренда, но и при организации информационного пространства вуза.

В рамках одного образовательного учреждения задача выделения отдельных сообществ обучаемых, определение тематики их интересов, выделение лидеров различных течений студенческой жизни, является достаточно востребованной. С одной стороны, подобный мониторинг позволит скорректировать управленческие воздействия внутри студенческой учебной и внеучебной деятельности, с другой стороны, предупредит нежелательные движения агрессивной направленности.

Простейшие алгоритмы выделения групп пользователей, связанных одной целью основаны на анализе количественных характеристиках, таких как количество сообщений по некоторой теме, число лайков, активность и частота участия. На основе данных, извлекаемых из соцсетей, строится граф

пользователей сети[1]. Далее в этом графе следует выделить более общие группы – сообщества. Под студенческим сетевым сообществом будем понимать добровольные объединения учащихся в поле социальной сети, основанные на общих интересах и направленные на некоторую социокультурную деятельность.

Выделим типы студенческих сообществ, получаемые на основе данных из соцсетей.

1. Научно-профессиональные. Такие сообщества являются узкопрофессиональными, объединены общими научными и учебными интересами. Тематика таких сообществ, их численность поможет сориентироваться педагогическому составу в определении направлений научной деятельности студентов, их мотивации к будущей специальности. Такие сообщества будут достаточно многочисленными и разнообразными на факультетах и скорее всего, будут объединять учащихся одной или близких специальностей.
2. Творческие. Подобные сообщества помогают развить творческую составляющую личности. Участие в таких сообществах раскрывает творческий потенциал учащихся. Подобные сообщества обычно являются межфакультетными.
3. Развлекательные. Определяют различные хобби учащихся, их интересы, расположенные за рамками процесса обучения.
4. Гражданско-политические. Эти сообщества объединяют учащихся общих политических взглядов, придерживающихся одной гражданской позиции.

Для построения графа пользователей соцсети необходимо классифицировать информацию, извлекаемую из сети. Будем выделять общесетевые и личностные данные. К общесетевым данным отнесем информацию, определяющую социальную связь между пользователями, например, пол, возраст, количество лайков, наличие подписок, количество друзей и т.д. Личностные данные определяют эмоциональную окраску сообщений, объемы постов, поиск различных событий в сети. Общесетевые данные в большинстве являются числовыми характеристиками, для выявления личностных данных необходимо применять дополнительные методы, например, классификацию текстовых сообщений.

Для выделения сообществ на графе на первом этапе необходимо выполнить анализ количественных (общесетевых) характеристик с помощью нейронной сети. Нейронная сеть позволит решить задачу классификации данных, отнести набор характеристик конкретного пользователя к тому или иному классу.

Процедура анализа при решении задачи экстрагирования студенческих сообществ предполагает два этапа: мелкособытийный и крупнособытийный анализ (рис. 1).

---

[1] А.В. Омельченко. Теория графов. – М., 2018.

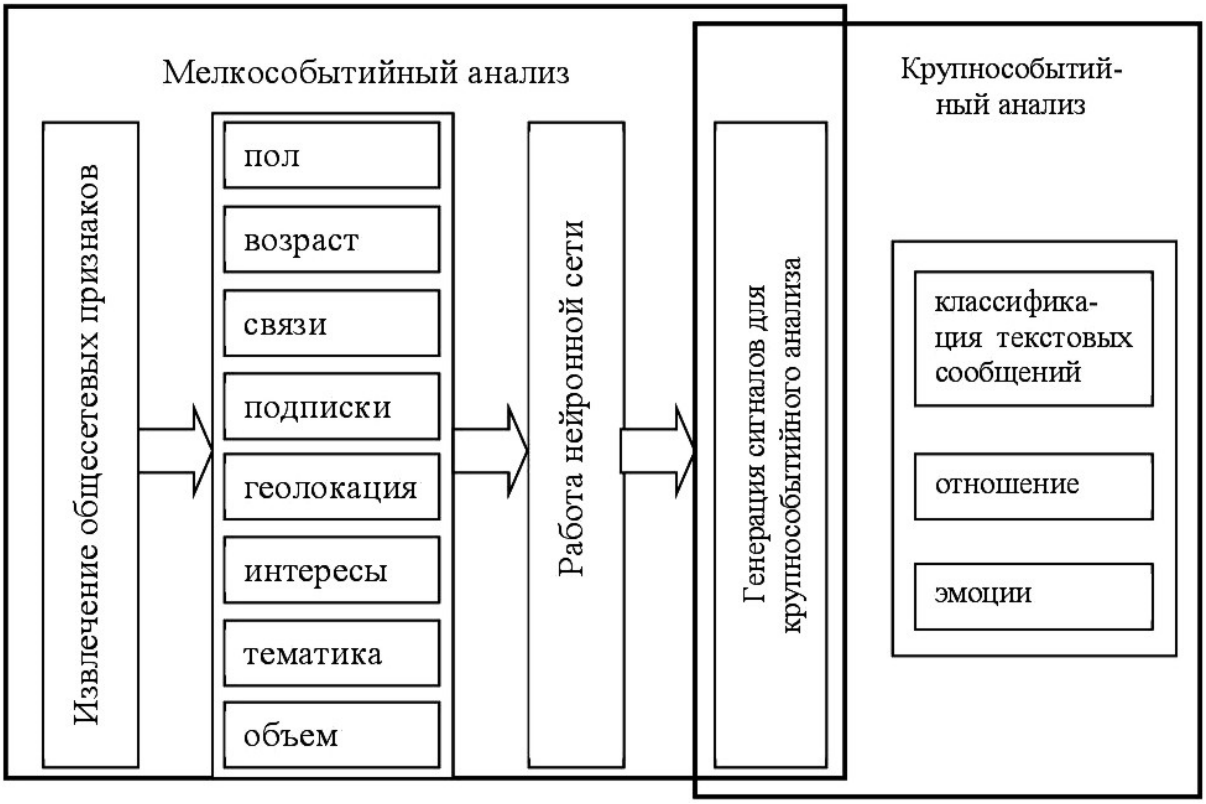

Рисунок 1 – Работа мелкособытийного и крупнособытийного анализа

На первом этапе осуществляется извлечение сетевых данных и признаков, которые помещаются в базу данных. Хранение наборов данных осуществляется с помощью СУБД MongoDB, которая располагает данные в облачном хранилище. Нейронная сеть на этом этапе выполняет классификацию характеристик текущего пользователя, отнеся его к тому или иному классу.

На втором этапе учитывается эмоциональная окраска текстовых сообщений пользователей, их реакция на внешние события.

Вообще социальную сеть можно рассматривать граф G (N, E), в котором N = {1, 2, ..., n} – конечное множество вершин (пользователей) и E – множество ребер, представляющий взаимосвязи между пользователями. На основе этого, можно вычислить основные метрии графовой структуры и наглядно представить связь между вершинами графа.

Обработка графа выполняется стандартными методами, например, для построения списка друзей некоторого пользователя заданной глубины используется метод рекурсивного обхода графа в глубину. Построение и визуализация графовых структур осуществляется с помощью соответствующих модулей.

После классификации и извлечения признаков пользователей, вычисляются статистические характеристики пользователей в твитах и постах, такие как среднее количество сообщений в день, среднее количество хэштегов и URL-адресов на сообщение, среднее количество постов в день и некоторые другие статистические характеристики.

Уровень взаимосвязей пользователей удобнее воспринимать визуально. Для этого используется среда Gephi, позволяющая загрузить данные для работы с графами. Это продукт обладает мощным инструментарием и богатыми возможностями кастомизации. Связь с приложением Gephi устанавливается с помощью запуска сессии стриминга, с помощью которой передаются данные, определяющие граф: узлы, ребра, метки узлов и ребер, вес узлов, направление ребер и проч.

На рисунке 2 можно видеть граф, построенный с помощью среды Gephi, который отображает взаимосвязи подписчиков некоторого контента социальной сети ВКонтакте. Данный граф отражает экстрагированное сообщество на основе подписки. Затемненный фрагмент показывает лидера группы.

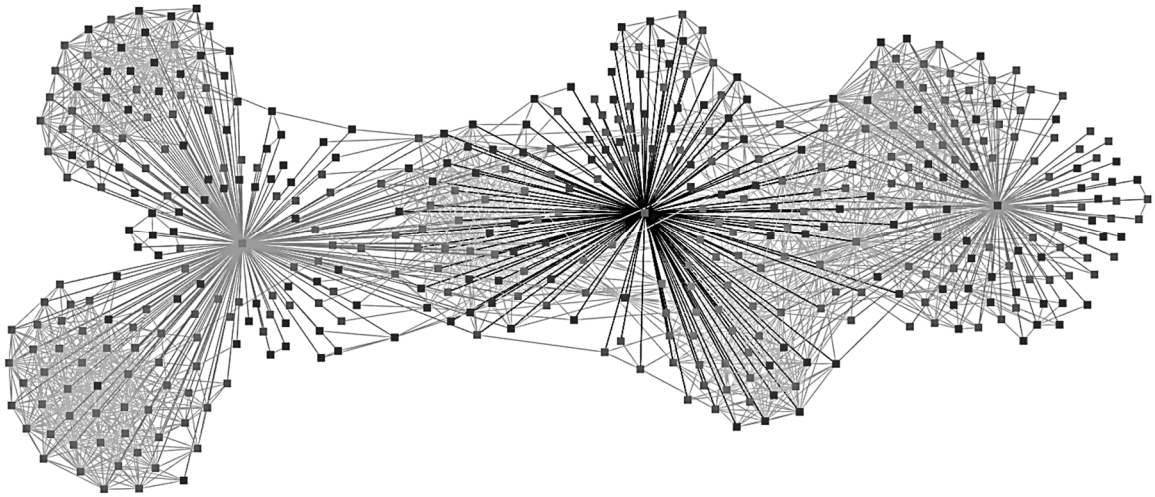

Рисунок 2 – Граф друзей ВКонтакте

Таким образом анализ данных, извлекаемых из социальных сетей, позволяет не только классифицировать интересы пользователей, но и экстрагировать отдельные сообщества узкой направленности, определить лидеров этих групп, наиболее активных участников. Полученная информация может быть использована при организации досугового пространства студентов, а также развития их научных интересов.

Васильева Е.Г.,
кандидат юридических наук, доцент,
доцент кафедры административного
и финансового права
СКФ ФГБОУВО «РГУП»
г. Краснодар

ЕДИНЫЙ НАЛОГОВЫЙ ПЛАТЕЖ В УСЛОВИЯХ РАЗВИТИЯ РОССИЙСКОЙ ЦИФРОВИЗАЦИИ

Стремительное развитие цифровых технологий (цифровизация) затронуло сферу налогового законодательства, оказало существенное влияние на трансформацию порядка исполнения налоговой обязанности.

С учетом изложенного, в 2019 году в РФ появился новый, альтернативный традиционному способ оплаты имущественных налогов физических лиц за 2018 год – единый налоговый платеж (транспортного налога, налога на имущество физических лиц, земельного налога). Так произошли существенные изменения в действующем законодательстве в части появления новых способов исполнения налоговой обязанности физическими лицами[1]. Возник новый КБК для единого налогового платежа физического лица – 18210607000011000110. В результате с 2018 года в НК РФ появился новый термин – единый налоговый платеж (статья 45.1 НК РФ, введена Федеральным законом от 29.07.2018 № 232-ФЗ)[2]. С 01 января 2019 года начал свое непосредственное действие, а с 01 января 2020 года вступили новые изменения в отношении НДФЛ (в ред. Федерального закона от 29.09.2019 № 325-ФЗ[3]).

Теперь же законодатель решил применять единый налоговый платеж не только для физических лиц, но и в отношении организаций и индивидуальных предпринимателей. По данному вопросу подготовлен Проект федерального закона «О внесении изменений в статьи 45 и 45.1 части первой Налогового кодекса Российской Федерации»[4]. Изучив данный законопроект, можно выделить следующие аспекты. Цели изменения

---

1 Налоговый кодекс Российской Федерации (часть первая) от 31 июля 1998 г. № 146-ФЗ (ред. от 17.02.2021) // Собрание законодательства РФ. 1998. № 31. Ст. 3824.

2 Федеральный закон от 29.07.2018 № 232-ФЗ «О внесении изменений в часть первую Налогового кодекса Российской Федерации в связи с совершенствованием налогового администрирования» // Собрание законодательства РФ. 2018. № 31. Ст. 4821.

3 Федеральный закон от 29.09.2019 № 325-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации» // Собрание законодательства РФ. 2019. № 39. Ст. 5375.

4 Проект федерального закона «О внесении изменений в статьи 45 и 45.1 части первой Налогового кодекса Российской Федерации». – URL : https://minfin.gov.ru/ru/document/npa_projects/?id_4=6702 (дата обращения 13.02.2021).

законодательства по данному вопросу: совершенствование порядка исполнения обязанности по уплате налогов, сборов и страховых взносов, с помощью данных изменений появится возможность улучшения налогового администрирования организаций и индивидуальных предпринимателей. Необходимо отметить, что предпосылки на изменение положений статьи 45.1 НК РФ прежде всего возникли из-за того, что налогоплательщики при оплате налогов по существующей системе допускают ошибки при заполнении платежных документов. Некоторые плательщики несвоевременно уплачивают налоги в бюджеты. Все эти явления приводят к негативным последствиям и к начислению пеней[1]. Плательщик сможет заплатить налоги, торговые сборы и страховые платежи одним платежом, мы считаем, что это положительный момент изменений. Не нужно будет уточнять вид платежа, а также его срок уплаты и принадлежности к бюджету бюджетной системы Российской Федерации, что также является плюсом данных изменений. Налоговый орган при этом, самостоятельно будет делать зачет полученных средств, в счет обязательств налогоплательщика[2]. ЕНП будет считаться правом организации и ИП. У них останется возможность уплачивать налоги по налоговым обязательствам по существующему порядку. При оплате налогов по существующей системе будет предусмотрено, что если вдруг у компании образуется переплата, то можно будет перевести эти средства на счет единого налогового платежа и эти деньги будут списаны на погашение налогов. Порядок зачисления суммы ЕНП будет таков: налоговый орган будет засчитывать деньги начиная с того налога или сбора, по которому сумма меньше, такой же порядок будет и в отношении недоимок. У компаний будет возможность запросить возврат излишка, но в том случае, если у них не будет задолженности. Рассмотрев плюсы и минусы планируемых изменений ЕНП, хотелось бы остановиться на следующем.

Единый налоговый платеж – это относительно новый способ взимания денежных средств с физических лиц на добровольной основе. Попробуем охарактеризовать новый вид российского налогового платежа.

Итак, единый налоговый платеж физического лица – это определенная сумма денежных средств, перечисляемых налогоплательщиком добровольно в бюджет на соответствующий счет Федерального казначейства в счет уплаты НДФЛ и имущественных налогов: транспортного, земельного и налога на имущество физлиц (анализ положений ст. 45.1 НК РФ). Периодичность внесения средств и конкретные суммы налогоплательщик определяет самостоятельно. Поэтому зная свои налоги, налогоплательщик может

---

[1] Сводный отчет о проведении оценки регулирующего воздействия к проекту федерального закона «О внесении изменений в статьи 45 и 45.1 части первой Налогового кодекса Российской Федерации». – ULR : https://minfin.gov.ru/ru/document/npa_projects/?id_4=6702 (дата обращения 13.02.2021).

[2] Пояснительная записка к проекту федерального закона «О внесении изменений в статьи 45 и 45.1 части первой Налогового кодекса Российской Федерации». – ULR : https://minfin.gov.ru/ru/document/npa_projects/?id_4=6702 (дата обращения 13.02.2021).

распределить их во времени и выбрать наиболее комфортную для себя схему оплаты. Оплата возможна любым удобным для налогоплательщика способом: через банк; почту России; МФЦ; кассу местной администрации; сервис оплаты налогов на сайте ФНС России[1]; а также через личный кабинет налогоплательщика, закладка «Мои налоги» / «Единый налоговый платеж». Отметим, что произвести оплату возможно лично, либо данную обязанность может исполнить любое иное лицо.

Думается, что единый налоговый платеж условно можно назвать «копилкой» для хранения, необходимых средств для оплаты налогов до наступления срока платежа. Как мы видим ЕНП это добровольный платеж для физических лиц. Его ввели для уплаты имущественных налогов авансом – то есть до момента выставления налоговым органом уведомления. Особенно это наглядно проявляется при сроках его оплаты. Обращаю внимание, что вносить единый платеж можно через личный кабинет налогоплательщика. При этом следует понимать, что в течение года он будет отражаться как аванс, а 01 декабря текущего года зачтется в счет налогов, но никак не раньше, что не совсем удобно в части досрочного исполнения налоговой обязанности. Кроме того, зачет проведет сама налоговая инспекция по такому принципу: сначала погашаются долги, затем – начисленные налоги, начиная с меньших сумм.

В рамках данных нововведений еще раз отметим, что единый платеж в РФ можно вносить за любое лицо (также, как и за налоги). Последний не вправе будет требовать возврата денежных средств, на это имеет право только сам налогоплательщик. Чтобы заплатить за иное лицо, проще всего сформировать квитанцию в личном кабинете на сайте nalog.ru[2] и в последующем оплатить ее по индексу документа – например, на портале Госуслуг[3] по своей учетной записи. Тогда денежные средства точно дойдут до адресата и зачислятся не на лицевой счет лица, производившего оплату, а на счет налогоплательщика. С процедурной точки зрения представляется вполне удобный способ исполнения налоговой обязанности. Важно, что, если после зачета что-то останется, остаток платежа можно будет вернуть по заявлению. К несомненным достоинствам, следует отнести то, что ЕНП можно вносить без заполнения реквизитов каждого налога - одной суммой в любом размере. Платить можно в течение года, какими угодно частями. То есть налогоплательщик платит заранее – еще до того, как налоговый орган исчислит налоги.

Следует оговориться, чем же тогда отличается ЕНП от уплаты налогов обычным способом. Единый налоговый платёж вносится единожды, т.е.

---

[1] Официальный сайт ФНС России. – URL : https://service.nalog.ru/payment/payment-search.html?svc=tax-fl#fl (дата обращения 20.02.2021).

[2] Официальный сайт ФНС России. – URL : https://www.nalog.ru/rn23/ (дата обращения 20.02.2021).

[3] Портал государственных услуг Российской Федерации. – URL : https://www.gosuslugi.ru/new (дата обращения 20.02.2021).

денежные средства идут на уплату сразу всех имущественных налогов: транспортного, земельного, налога на имущество физлиц. Так вместо того, чтобы платить трижды, за каждый налог отдельно, в том числе отдельно еще за НДФЛ налогоплательщик оплачивает всего один раз несколько налогов. Единый налоговый платёж можно внести и за другое лицо. Как уже отмечалось, ранее является добровольным.

С учетом изложенного, подведём предварительные итоги.

С налоговыми уведомлениями не присылают квитанции. Раньше вместе с налоговыми уведомлениями по почте приходили квитанции для уплаты – отдельные для каждого имущественного налога и НДФЛ. Это были заполненные документы с реквизитами и суммами. С 2019 года квитанции не присылают: их нет ни в почтовых конвертах, ни в личном кабинете. Налогоплательщик только получает налоговое уведомление. В налоговом уведомление указаны реквизиты для уплаты каждого налога.

Отметим, что после введения в 2019 году в РФ нового способа оплаты имущественных налогов – с помощью единого налогового платежа (статья 45.1 НК РФ), стало возможным в течение года еще до срока уплаты и даже до рассылки налоговых уведомлений зачислять деньги на авансовый кошелек. Когда подойдет срок уплаты налогов, нужная сумма спишется с баланса – лицевого счета налогоплательщика, до этого момента платеж будет считаться как аванс. Оплатить можно как за себя, так и за иное лицо. Этот вариант удобен тем, что не нужно перечислять деньги разными платежами и искать реквизиты. Единый налоговый платеж – это добровольный способ уплаты. Им можно воспользоваться на свое усмотрение: например, ежемесячно перечислять небольшие суммы, чтобы к нужному сроку накопить средства для погашения начислений. На сайте Госуслуг также возможно оплачивать начисления одним платежом. Но только те, которые отражены на портале: например, автоштрафы, налоговую и судебную задолженность. Обращаю Ваше внимание, что до 01 декабря текущего года – 2021 начисленные имущественные налоги – это еще не задолженность, поэтому на Госуслугах она не будет видна.

Попробуем разобраться для чего это сделали. Задумка как представляется была в следующем. Налогоплательщик укладывает деньги на баланс и не думаете, что с оплатой налогов. Не надо ждать квитанции, платить по разным КБК. Ему необходимо просто внесите платеж, и все зачтут. Необходимо отметить, положительные моменты, состоящие в том, что не надо каждый год оплачивать сразу все имущественные налоги. Получается, что до 01 декабря текущего года нужно сразу внести всю сумму. А чтобы заплатить в течение года небольшими частями, нужно было заполнять квитанции по каждому налогу отдельно. Теперь в течение года можно вносить авансовый платеж. Платить можно как угодно: требований к периодичности внесения сумм авансовых платежей нет. Можно вносить каждый месяц, два раза в год или не вносить вообще и ждать уведомления. Аванс можно внести через личный кабинет на сайте Федеральной налоговой службы (ФНС России).

Специально для этого сервис дополнили разделом «Единый налоговый платеж». Оплата производится с помощью банковской карты или на сайте одного из банков, заключивших соглашение с налоговой инспекцией. В личном кабинете будет отображаться не только сумма платежа, но и распределение средств в счет уплаты имущественных налогов.

Также для авансового платежа можно использовать электронные сервисы «Уплата налогов, страховых взносов физических лиц», «Заполнить платежное поручение» и «Уплата налогов за третьих лиц» на сайте ФНС России. При оплате они предусматривают только возможность перехода на сайт банка, заключившего соглашение с ФНС России. Еще один вариант внесения авансового платежа – визит в отделение банка. Для этого надо предварительно сформировать и распечатать расчетный документ на сайте налоговой службы. Проще всего заплатить в личном кабинете на сайте nalog.ru: там есть ссылка и можно указать любую сумму. Платить можно картой, через банк, портал Госуслуг или по квитанции – она сформируется автоматически. Заметим, что авансом можно оплачивать имущественные налоги и с 01 января 2020 года НДФЛ, с учетом положений ст. 228 НК РФ. Технически процедура проста: деньги налогоплательщика зачисляются на специальный счет Федерального казначейства, откуда потом списываются для погашения задолженности, если она имеется, либо, когда подходит срок, в уплату налогов.

Таким образом, единый налоговый платеж физического лица – это денежные средства, которые гражданин добровольно перечисляет в бюджетную систему Российской Федерации с помощью единого платежного поручения. Эта сумма зачисляется на соответствующий счет Федерального казначейства для уплаты налога на имущество физических лиц, а также транспортного и земельного налогов, а с 01 января 2020 – в отношении НДФЛ. Платежи будут поступать в бюджеты по месту нахождения соответствующих объектов налогообложения. Зачет платежа налоговые органы будут проводить самостоятельно при наступлении срока уплаты имущественных налогов. О принятом решении о зачете налогоплательщик будет проинформирован. Также все данные будут отражаться в «Личном кабинете налогоплательщика для физических лиц». Представляется, что использование единого налогового платежа значительно сократит время, затрачиваемое на оформление платёжных документов, а также минимизирует ошибки граждан при заполнении нескольких платежек.

Как поясняет ФНС России, внесение средств через механизм единого налогового платежа исключает ошибки, которые часто возникают при заполнении нескольких платежных поручений с указанием различных реквизитов. Это уменьшает объем так называемых невыясненных поступлений и позволяет государству вовремя получать платежи. Самому же гражданину, если он заплатил налоги авансом, не приходится больше следить за сроками наступления платежей. При этом он может быть уверенным, что полностью выполнил свои обязательства и никакие пени или налоговые санкции ему не грозят.

Общеизвестно, что по действующему в РФ порядку физическим лицам дается не менее месяца на оплату налогов, уплата производится до 01 декабря очередного текущего года. Многие люди в силу разных факторов и обстоятельств заплатить забывают или не успевают. Новая возможность платить налоги авансом позволит гражданам производить предварительную оплату, не беспокоясь за соблюдение сроков и распределение суммы платежа, подчеркивают в ФНС России. Авансовый механизм будет особенно удобен тем, кто владеет собственностью в разных регионах страны или, к примеру, живет за границей. Налогоплательщику будет достаточно внести некоторую сумму на счет Федерального казначейства, а налоговый орган уже сам распределит оплату по объектам налогообложения. Важно помнить, что единый налоговый платеж принимается только в рублях. Если суммы будет достаточно для уплаты всех налогов, недоимка просто не возникнет. Если средств не хватает, сначала будут зачтены меньшие суммы, причем, это касается не только недоимок по налогам, но и пеней – действует общее правило: сначала списываются меньшие суммы, а затем те, что больше. В этой ситуации гражданам, которые захотят платить налоги авансом, стоит позаботиться о том, чтобы средств, зачисленных на счет Федерального казначейства, хватало для уплаты всех налогов, что немаловажно.

Обращаю внимание, что механизм уплаты налогов авансом - дополнительный сервис для налогоплательщиков. У них остается право оплачивать налоги и привычным способом, после получения налоговых уведомлений. Это очевидное преимущество проектируемого механизма для налогоплательщиков. Убеждены, что ЕНП – это фактически беспроцентный кредит государству. Так называемая, дополнительная возможность заплатить налоги, иным новым способом, отличным от традиционного с периодичностью удобной для налогоплательщика. Для государства – это получение денежных средств авансом, что существенно может улучшить финансовую составляющую государственной политики в области налогообложения. Ранее у налогоплательщиков отсутствовала возможность оплаты сразу трех имущественных налога авансом, теперь благодаря изменениям в НК РФ появилась. Стоит еще раз подчеркнуть, что новый способ не исключает прежнего порядка исполнения налоговых обязательств, налогоплательщик вправе не использовать данный способ оплаты, оставить все по-прежнему.

Ващекин А.Н.,
кандидат экономических наук, доцент,
профессор кафедры информационного права,
информатики и математики,
ФГБОУВО «РГУП»
г. Москва

Ващекина И.В.,
кандидат экономических наук, доцент,
доцент кафедры информационного права,
информатики и математики,
ФГБОУВО «РГУП»
г. Москва

ОБ АЛГОРИТМИЗАЦИИ АНАЛИЗА ЭЛЕМЕНТОВ ЦИФРОВОГО ПРОСТРАНСТВА

Цифровое пространство на современном технологическом этапе образует наиболее весомую часть пространства информационного. Оно порождается цифровой компонентой информационной среды, в некоторой степени совпадающей с территориальными границами определенного государства или союза государств. Оно включает в себя такие образования нового, до сих пор малоизученного типа – цифровые поля (англ. *digital fields*) цифровые площадки (англ. *digital grounds*).

Цифровое пространство базируется на соответствующей инфраструктуре и характеризуется набором своеобразных отличительных свойств. Изучение этой совокупности цифровых норм и социальных практик, отношений между деятелями различных цифровых полей, просьюмерами (англ. *prosumers*), владельцами интернет-сайтов, государством, представляет собой не до конца разрешённую методологическую проблему[1].

Современное информационное пространство базируется на новых элементах цифровой среды – цифровых площадках, включающих в себя различные социальные группы, нередко формирующихся на основе одного сайта, способного обеспечить информационное взаимодействие в рамках конкретного форума, файлообменника, онлайн-магазина по продаже товаров определенного типа, оказания услуг определённой направленности, новостного ресурса, справочной системы.

Цифровые площадки порождают более крупные структурные элементы цифрового пространства – цифровые поля, соответствующие

[1] Иохин В.Я. Влияние цифровизации на экономику, общество и государство / В.Я. Иохин // Научно-аналитический вестник Института Европы РАН. – 2020. – № 3. – С. 62–67.

совокупности деятелей с одинаковыми цифровыми интересами. Комплекс информационных взаимодействий между ними подчиняется общим законам развития и координации элементов сложных самоорганизующихся систем – логистических, финансовых, правовых. Поэтому исследование информационного взаимодействия в цифровом поле следует производить на основе воспроизведения структуры порождающей его цифровой площадки (или нескольких, если поле генерируется их совокупностью). Для формального анализа функционирования цифровой площадки наилучшим образом подходит представление ее структуры в виде графа. В этом случае смысловые разделы площадки (СРП) будут представлены вершинами графа, а цифровые потоки – рёбрами. Весовые характеристики логично задавать как результат нечёткой оценки, проводимой экспертно.

Воспроизведение структуры цифровых полей с помощью графов позволяет производить взаимное сравнение организации информационных потоков внутри каждого из них. В частности, возникает понятие их функциональной идентичности, выявление которой может способствовать решению множества прикладных задач.

Функциональная идентичность устанавливается при выявлении изоморфности структуры. Изоморфизм разнообразных алгебраических структур хорошо исследован в современной математике[1]. В отношении графов он выражается в наличии взаимно однозначного соответствия между множествами их вершин, такого, что любая пара вершин в одном графе соединена тогда и только тогда, когда соответствующая им пара вершин в другом графе тоже соединена.

Простейшим способом проверки графов на изоморфизм является сравнение их матриц смежности. Если при рассмотрении всех возможных перестановок строк и столбцов хотя бы одна приведет из матрицы смежности одного к матрице другого, изоморфизм будет установлен, а задача функциональной идентичности решена. Для определения изоморфизма более сложных структур также разработаны надежные алгоритмы[2].

В дальнейшем предполагается рассмотреть применение изложенного подхода для исследования цифровых полей, генерируемых справочными правовыми системами, средствами массовой информации, социальными сетями и пр.

---

[1] Актарская А.С. Изоморфизмы общих линейных групп над ассоциативными кольцами, градуированными абелевой группой / А.С. Актарская, Е.И. Бунина, А.В. Михалев // Доклады Академии наук. – 2011. – Т. 437. – № 3. – С. 295–296.

[2] Берштейн Л.С. Определение нечетких внутренне устойчивых, внешне устойчивых множеств и ядер нечетких ориентированных графов / Л.С. Берштейн, А.В. Боженюк // ТиСУ. – 1999. – № 1. – С. 161–165.

Волкова В.В.,
кандидат юридических наук, доцент,
доцент кафедры
административного и финансового права,
СКФ ФГБОУВО «РГУП»
г. Краснодар

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ В ДЕЯТЕЛЬНОСТИ ПУБЛИЧНЫХ СЛУЖАЩИХ

Формирование глобальных электронных баз данных является ключевым элементом стратегии создания и развития информационного общества, формирования электронного государства. Многие результаты уже сейчас получили применение в более общем контексте электронного государства и продолжают свое наращивание.

По этой причине проектирование таких решений в рамках реализации системного проекта электронного правительства велось с самого начала с учетом возможности такого расширения использования в будущем.

Следует отметить, что развитие цифровых технологий в сфере государственного управления в целом и контроля в частности зависит от трех основных факторов: уровня технического обеспечения, в том числе проникновения Интернета, уровня образованности населения, структурной и содержательной частей государственных порталов в сети Интернет. Все это формирует возможность позитивного использования возможностей электронного документооборота в деятельности публичных служащих.

В частности, одним из направлений применения электронного документооборота можно считать современные информационно - коммуникационные технологии при осуществлении всех форм правосудия. Данные технологии («электронное правосудие») призваны обеспечить решение нескольких взаимосвязанных задач[1]:

– во-первых, облегчить доступ граждан и организаций к правосудию, сделать обращение в суд более удобным, требующим от заинтересованного лица меньше организационных и физических усилий;

– во-вторых, снизить коррупционные риски, что обусловлено использованием обезличенной формы взаимодействия судебных органов власти и заявителей;

– в-третьих, гарантировать соблюдение процессуальных сроков, комфортность в ознакомлении с материалами судебного дела, быстроту их «движения» при реализации судебных процедур, без чего невозможна эффективная защита конституционных прав и свобод граждан;

---

[1] Колобова С.В. Некоторые вопросы перевода кадровой документации в электронный вид / С.В. Колобова // Современное право. – 2020. – № 2. – С. 41–49.

– в-четвертых, обеспечить информационную открытость (транспарентность) судебных органов власти для общества.

Так, в настоящее время федеральным законодательством допускается обращение в Конституционный Суд РФ (далее – КС РФ) в электронном виде в форме электронного документа, подписанного усиленной квалифицированной электронной подписью (ч. 1 ст. 37 ФКЗ от 21.07.1994 № 1-ФКЗ «О Конституционном Суде Российской Федерации»[1]). В случае направления обращения в виде электронного документа, прилагаемые к нему дополнительны материалы также представляются в электронном виде, при этом приложения копий обращения, документов и иных материалов от заявителя не требуется. Кроме того, вся переписка с КС РФ в этом случае также осуществляется в электронном виде, а в тексте писем указывается предмет обращения, а также перечень приложенных документов.

Регламентом КС РФ предусматривается ведение электронного документооборота в данном органе: он устанавливает необходимость создания, пополнения и хранения судебных дел не только в бумажном, но и в электронном виде. Для обеспечения оперативного документооборота, соблюдения процессуальных сроков, облегчения доступа к различным процессуальным документам используется автоматизированная информационная система «Судоделопроизводство».

Инструкция по делопроизводству в КС РФ предусматривает использование данной системы как при рассмотрении обращений в Секретариате КС РФ (п. 4.1), при подготовке и проведении заседаний КС РФ, на которых решается вопрос о принятии или отказе в принятии обращения к рассмотрению (п. 4.2), подготовке дела к рассмотрению (п. 4.3), при проведении заседания КС РФ по рассмотрению дела (п. 4.4), так и в целом для осуществления делопроизводства, а также обеспечения интеграции системы документооборота КС РФ в общегосударственную систему межведомственного электронного документооборота[2].

Кроме того, достаточно интересным примером электронного документооборота является деятельность органов исполнительной власти, например, Федеральной таможенной службы РФ (далее – ФТС). В частности, на сегодняшний день для выпуска и регистрации электронной декларации органы таможенного регулирования должны соблюдать ряд требований, среди которых:

– наличие необходимых документов в электронном реестре органом таможенного регулирования;
– факт уплаты таможенных платежей;
– действительность электронной подписи.

---

[1] Федеральный конституционный закон от 21.07.1994 № 1-ФКЗ (ред. от 09.11.2020) «О Конституционном Суде Российской Федерации» // СЗ РФ. 1994. № 13. Ст. 1447.

[2] Шелепина Е.А. Применение электронных документов в гражданских правоотношениях: условия и возможности / Е.А. Шелепина // Законы России: опыт, анализ, практика. – 2017. – № 10. – С. 31–39.

Общеизвестным является тот факт, что учет таможенных сделок в настоящее время основывается на подписях, печатях документов, удостоверении личности или личных документов. Однако, как свидетельствует опыт и практика эффективность бумажного документооборота приближается к нулю в современных условиях, также повышается затратность хранения данных, повышаются временные затраты на осуществление аудита таких документов.

В связи с чем ожидаемому упрощению большинства операций способствовало внедрение электронной подписи, но, вместе с тем, такой механизм имеет слишком высокий риск кражи ключа с подписью, а также является достаточно дорогостоящим. Деятельность по обработке информационных сведений о расчетах сделок в крупных таможенных системах централизована, что формируют проблемы сложной системы безопасности, проблемы администрирования и трудности в виде высокой нагрузки[1].

На уровне Правительства Российской Федерации перспективы использования таких технологий в таможенном деле неоднократно обсуждались.

По нашему мнению, положительным направлением будет являться внедрение в органы таможенного регулирования блокчейн-технологий. Конечно, это повлечет определенные изменения. Выделим их:

1. Электронное декларирование. В результате внедрения блокчейн-технологий участник ВЭД сможет регистрировать и заполнять любой вид документации: коммерческие документы, транспортные документы, таможенные документы.

2. Автоматизация системы управления рисками, которая считается одним из перспективных направлений в сфере совершенствования органов таможенного регулирования. В результате того, что информационные данные хранятся в личном кабинете на платформе блокчейн, то можно будет определять уровень риска для каждого отдельного участника внешнеэкономической деятельности. Категорирование основных участников внешнеэкономической деятельности будет осуществляться программой автоматически. Именно поэтому это приведет к снижению участия человеческого фактора при таможенном контроле товаров.

3. С помощью использования технологий блокчейн в таможенной сфере возможен учет таможенных пошлин, которые были уплачены фактически. Так, в личном профиле участника внешнеэкономической деятельности будет отражаться соответствующая информация о направлениях перемещения товара, сумме таможенных пошлин, таможенной стоимости товара и о самом товаре.

---

[1] Карлаш Д.С. Электронный документооборот: вопросы правового регулирования / Д.С. Карлаш // Право и экономика. – 2019. – № 8. – С. 22–28.

В завершение сделаем следующие выводы.

1. Вектор развития российской и мировой системы публичного управления в настоящее время направлен, прежде всего, на модернизацию телекоммуникационных и информационных ресурсов, среди которых можно выделить: развитие информационных систем органов таможенного регулирования и создание электронных таможен.

2. Выделим основные факторы, которые обеспечивают эффективность таможенного контроля товаров, перемещаемых в рамках электронного документооборота:

– повышение управляемости данными в рамках осуществления таможенного контроля;

– интегрирование органов таможенного регулирования в торговый процесс;

– повышение качества и безопасности товаров, перемещаемых в рамках смарт-контрактов;

– повышение эффективности взаимодействия и сотрудничества между органами таможенного регулирования и органами налогового регулирования, а также другими субъектами взаимодействия;

– улучшение борьбы с финансовыми преступлениями в области таможенного контроля.

3. Среди информационных таможенных технологий автоматический выпуск товаров и автоматическая регистрация деклараций выступают одними из наиболее востребованными и эффективными. На наш взгляд, дальнейшее усовершенствование и распространение таких технологий интересно и для участников внешнеэкономической деятельности, и для органов таможенного регулирования. Таким образом, вектором развития системы органов таможенного регулирования в РФ считается практика использования технологий автоматического выпуска, автоматической регистрации и электронного декларирования при таможенном контроле товаров, перемещаемых в рамках смарт-контрактов.

4. Как следует подчеркнуть, блокчейн-технологии подразумевают априори надежность информационных сведений и невозможность их изменений. Именно поэтому органы таможенного регулирования могут использовать данные технологии для осуществления между органами таможенного регулирования и участниками внешнеэкономической деятельности надежного электронного документооборота при таможенном контроле перемещаемых товаров.

Дудченко Ю.Л.,
кандидат юридических наук, доцент кафедры общетеоретических правовых дисциплин, СКФ ФГБОУВО «РГУП»
г. Краснодар

Ковалева В.В.,
кандидат юридических наук, доцент, заведующий кафедрой общетеоретических правовых дисциплин, старший научный сотрудник, СКФ ФГБОУВО «РГУП»
г. Краснодар

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВЫХ ИННОВАЦИЙ: ПРОБЛЕМЫ И ТЕНДЕНЦИИ

Интенсивное развитие цифровых технологий детерминируют постановку вопроса о пределах, возможностях и средствах правового регулирования возникающих ввиду этого правоотношений, которые, безусловно, обладают своеобразной природой вследствие появления не только их новых объектов, но и субъектов взаимодействия. В научной литературе пишут, что современный человек одновременно существует по крайней мере в двух ипостасях – как реальный материальный объект, наделенный сознанием в природном (реальном) мире, и как аватар, виртуальная (электронная) личность, обладающая возможностью выбора внешности, возраста, возможностей в создаваемых им самим обстоятельствах жизни) в киберпространстве, созданном исключительно сознанием самого индивида, исходя из его собственных желаний и предпочтений, но обязательно при помощи искусственного интеллекта, коим могут быть наделены различные технологические объекты[1].

Анализ юридической литературы позволил прийти к выводу, что современные исследователи констатируют факт колоссальной трансформации общества, например, отмечается, что происходящие изменения можно рассматривать как исторический вызов, т.к. наступает новый этап – этап «неомодернизации», который отразится и на глобальном информационном обществе, и, конечно, на трансформации правовой системы[2]. Следует согласиться с тем, что современные вызовы позволяют признать наступление

---

[1] Попова А.В. Правовые аспекты онтологии искусственного интеллекта / А.В. Попова // Государство и право. – 2020. – № 11. – С. 115–127.

[2] Кроткова Н.В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации / Н.В. Кроткова, А.В. Минбалеев, Т.А. Полякова // Государство и право. – 2020. – № 5. – С. 75–87.

нового цивилизационного этапа, который требует переосмысления многих правовых вопросов, включая развитие системы информационного права, активного внедрения «цифры» как формы объективизации, бытия информации. Перед юридической научной общественностью ставятся вопросы о том, как соотносится в сегодняшнем информационном пространстве информационное право и цифровое, что такое «цифра» не только с технической точки зрения, но и с правовой. Важно юридическое осмысление «цифрового инструментария» и фундаментальные междисциплинарные исследования в государственном управлении и в экономике для использования его как на национальном, так и на глобальном уровне[1]. Перечисленные выше вопросы актуализируют существующую повестку дня, научное сообщество должно найти ответы, от которые зависит не только эффективность правового регулирования, но и судьба права в целом, как регулятора.

Следует отметить, что происходящие изменения затронули практически все существующие правоотношения, являющиеся предметом регулирования различных отраслей права. Так, например, специалисты в области трудового права отмечают, что: «Цифровая экономика имеет несколько специфических черт, которые отличают её от «аналоговой» и непосредственно влияют на трудовые отношения и труд в целом и на свободу труда, в частности. Сущность всех промышленных революций – замена труда человека на «труд» машины. В первые три ничего глобально-ужасного для человечества не произошло, мы выжили и приспособились. В новой digital economy происходит замещение человека более продвинутыми искусственными системами: роботами, компьютерными программами, алгоритмами, нейросетями, киберфизическими системами, искусственным интеллектом и т.п.[2] Необходимо отметить, что данная проблема сегодня является одной из ключевым, так как мы имеем дело с двумя процессами: с одной стороны, рост населения планеты и, как следствие, усиление конкуренции между людьми, с другой, возрастающее количество систем, программного обеспечения заменяющего человека как работника. Такая ситуация требует изменения правового регулирования, использования новых юридических конструкция, иных правовых средств.

Еще одной яркой иллюстрацией происходящих преобразований является исследование в уголовном праве, в научной литературе, в частности отмечается, что проблему трансформирующего влияния цифровых технологий на институт уголовного наказания можно представить двумя основными сценариями (вероятностными направлениями), которые заслуживают пристального внимания и проработки с целью обеспечения соответствия практики применения наказания ожиданиям и вызовам информационного

---

[1] Кроткова Н.В. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации / Н.В. Кроткова, А.В. Минбалеев, Т.А. Полякова // Государство и право. – 2020. – № 5. – С. 75–87.

[2] Шавин В.А. Трансформация принципа свободы труда в цифровую эпоху / В.А. Шавин // Государство и право. – 2021. – № 2. – С. 104–113.

общества. В зависимости от глубины модифицирующего воздействия на уголовное наказание, по мнению Е.А. Русскевича, можно выделить умеренный (адаптивно-линейный) сценарий эволюции наказания и взрывной (революционный). Умеренный сценарий цифровизации уголовного наказания предполагает поступательное внедрение информационно-коммуникационной инфраструктуры непосредственно в процесс исполнения имеющихся видов наказания в целях предупреждения десоциализации осуждённых[1]. Вызывает безусловный интерес, вывод автора о том, что в перспективным видится дополнение уголовного законодательства новым видом наказания – снижение рейтинга общественной благонадежности. Необходимо отметить, в этом случае речь идет о рецепции опыта КНР, правительство которого приняло решение «О планировании строительства системы социального кредита (2014–2020)». Е.А. Русскевич, пишет, что очевидно, что такая форма уголовной репрессии имеет много общего с такими традиционными видами уголовного наказания как лишение права занимать определенные должности и заниматься определенной деятельностью, а также ограничение свободы. Вместе с тем, отмечает автор, если данные виды наказания имеют срочный характер и предполагают установление конкретных ограничений в отношении осужденного, понижение лица в рейтинге общественной благонадёжности фактически представляет собой одномоментное общее ограничение субъекта в правоспособности. Учитывая всеобъемлющий характер такого ограничения, полагаем, что понижение лица в рейтинге общественной благонадежности (например, на одну, две, три категории) будет представлять собой более строгое наказание, чем лишение права занимать определенные должности и заниматься определенной деятельностью, а также ограничение свободы[2]. Данный пример показывает какие новые юридические средства можно использовать в процессе охранительного регулирования, хотя, и это не вызывает сомнение, предложение автора требует глубокого обдумывания, так как это существенное ограничение правоспособности, которое, может быть, не совместимо с ценностными основаниями права, не случайно приведенный опыт Китая, многие называют «цифровой диктатурой»[3].

Следует отметить, что происходящие изменения, затронули и вопросы безопасности, как отмечается в юридической литературе: «Риски и вызовы национальной безопасности в эпоху цифрового мира становятся особенно явными в контексте цифровой глобализации, под которой следует понимать формирование нового миропорядка, конструируемого и управляемого с помощью цифровых технологий в единстве сетевой,

---

[1] Русскевич Е.А. Уголовное наказание и цифровые технологии: точка бифуркации / Е.А. Русскевич // Государство и право. – 2020. – № 7. – С. 77–84.

[2] Там же.

[3] Разумов Е.А. Цифровое диктаторство: особенности системы социального кредита в китайской народной республике / Е.А. Разумов // Труды ИИАЭ ДВО РАН. – 2019. – № 3. – Т. 24. – С. 86–97.

коммуникационной и мировоззренческо-смысловой структуры. Представляется правильным говорить в таком случае о цифровой безопасности как важнейшем элементе национальной безопасности, но не в смысле технологической защиты информации. Понятие «цифровая безопасность» значительно шире, чем его часто понимают технические специалисты[1]. Мы солидарны с автором в том, что цифровая, как и любой вид безопасности требует правовой регламентации, отсюда непродуктивно рассматривать ее только с технической точки зрения, хотя и без нее невозможно, полагаем, здесь необходима «коллаборация» правового и технического, так как технологические изменения меняют бытие субъектов как участников правоотношений.

Приведенные выше примеры ярко иллюстрируют происходящие изменения во всех отраслях права, поэтому можно констатировать, что происходящие изменения являются фундаментальными и связанные с изменения технологического уклада. Как справедливо отмечается в научной литературе: «Модель правового развития с позиции теории технологических укладов можно определить либо как догоняющую, либо как опережающую. В России преобладала догоняющая модель, более эффективной представляется вторая возможная модель, при которой применяется опережающее регулирование. Право в этом случае принимается для отношений, которые еще только формируются, которые связаны с новыми технологиями, еще не получившими широкого распространения»[2]. Данное утверждение не лишено оснований, вместе с тем необходимо отметить, что опережающие правовое регулирование также может приводить к негативным последствиям, например, если выбраны не надлежащие средства правового регулирования. Ввиду этого считаем позитивным шагом принятие Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» от 31.07.2020 № 258-ФЗ[3], который дает возможность проверить вводимое специальное регулирование, которое впоследствии может стать всеобщим.

Как отмечает профессор Ю.А. Тихомирова, пишет, что: «Так, юристы рассуждают: хорошо, когда правил много, и плохо, когда правил мало. Но эта мера тоже не совсем удачная, если не сказать, что она подвержена критическому восприятию. На примере отечественного бизнеса видно, что нормативные излишества губительны. Сейчас картина правового развития в стране не кажется радужной. Не менее, если не более сложна картина мирового правового развития»[4]. Об этом пишет и Е.Е. Никитина, которая пишет, что разрыв между появлением и дальнейшим усовершенствованием

---

[1] Овчинников А.И. Безопасность личности и государства в цифровую эпоху: политико-правовой аспект / А.И. Овчинников // Журнал российского права. – 2020. – № 6. – С. 6.

[2] Пашенцев Д.А. Смена технологических укладов и правовое развитие России : монография / Д.А. Пашенцев, М.В. Залоило, А.А. Дорская. – М. : ИЗиСП : Норма : ИНФРА-М, 2021. – С. 165.

[3] Российская газета. – 2020. – 06 августа.

[4] Тихомиров Ю.А. Право: момент покоя или опережающее воздействие на социальные процессы / Ю.А. Тихомиров // Журнал российского права. – 2020. – № 4. – С. 7.

новейших технологий и темпами социальных изменений продолжает углубляться, что является проблемой для нахождения консенсусных социальных норм, оценки их обществом и формулирования их в качестве норм законодательства. В этих условиях сложно выработать эффективное правовое регулирование возникающих общественных отношений. При этом необходимо соблюдать баланс между определенной широтой границ регулирования для свободного развития технологий и обеспечивающих их научных исследований и нормативным закреплением ограничений и запретов для предотвращения рисков и угроз человеческой личности, ее достоинству и правам[1].

Подводя итоги, необходимо отметить, что происходящие изменения носят глубинный характер, цифровизация – это не только форма уже существующих правоотношений, это процесс, который определяет изменения правового регулирования, начиная с принципов, заканчивая формами права, так как только оптимальное сочетание средств регулирования позволит осуществить требуемые преобразования, и соответствие правового регулирования и общественного развития.

Королев М.П.,
кандидат юридических наук,
старший преподаватель кафедры
гражданского процессуального права,
ПФ ФГБОУВО «РГУП»
г. Нижний Новгород

ИНФОРМАЦИОННЫЙ ТЕХНОЛОГИИ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ МЕХАНИЗМА ПРИНУДИТЕЛЬНОГО ИСПОЛНЕНИЯ АКТОВ СУДОВ И ИНЫХ ЮРИСДИКЦИОННЫХ ОРГАНОВ

Развитие информационных технологий стремительно преображает общественные отношения во всех сферах: экономической, политической, технологической, не является исключением, и юридическая сфера внутренних связей социума. Становится общепризнанным, что цифровизация определяет переход к новому жизненному укладу, в числе прочего и в правовом механизме восстановления нарушенных прав и законных интересов граждан и юридических лиц.

Рассмотрение и разрешение споров в судах общей юрисдикции и арбитражных судах является основным способом дачи правовой оценки тем

[1] Никитина Е.Е. Система прав и свобод человека в условиях технологической революции / Е.Е. Никитина // Журнал российского права. – 2020. – № 8. – С. 27–44; – С. 8.

или иным действиям участников общественных отношений, фактам и событиям. Помимо констатации наличия или отсутствия нарушений одной из сторон спора, суды определяют меру воздействия на причинителя вреда или иным образом нарушившего закон субъекта, а также способ восстановления нарушенного права.

Для тех случаев, когда субъект, обязанный судебным вердиктом к совершению тех или иных действий, не исполняет акт суда, правовая система предусматривает институт исполнительного производства, реализуемый уполномоченными на то представителями государства, а именно судебными приставами-исполнителями Федеральной службы судебных приставов РФ.

В настоящее время система органов принудительного исполнения претерпевает существенные изменения, касающиеся как структурно-кадрового аппарата, так и организационного и правового инструментария, который может и должен быть использован в рамках процедуры по исполнению судебных актов и актов иных юрисдикционных органов.

Итоги деятельности ФССП РФ за последние годы не позволяют дать удовлетворительную оценку общему состоянию такого направления деятельности государства как исполнение решений судов (и актов иных юрисдикционных органов). Согласно итоговому докладу ФССП РФ за 2020 год в этот период на исполнении службы находилось более 100 млн производств, из которых более половины – это акты несудебных органов. Нагрузка на одного пристава-исполнителя превысила нормативную более чем в 17 раз. От общего числа находящихся в работе производств исполняется лишь 50 %, причем по судебным актам исполняемость еще ниже и составляет 47 %. Такие показатели не оставляют сомнений в необходимости серьезного повышения эффективности механизма принудительного исполнения, поиска новых инструментов и методов воздействия на должников и оптимизации действий всех участников этих отношений и проводимых при этом процедур.

В этой связи директор ФССП Д. В. Аристов озвучил позицию службы по этому вопросу, заявив, что видит решение проблемы в цифровизации всех процессов ведения исполнительного производства, его учета и контроля1. В условиях современной действительности такой подход представляется весьма перспективным.

Какова же ситуация в контексте использования информационных технологий в механизме принудительного исполнения на текущий момент. Положение в последние годы меняется к лучшему, совершенствуется нормативно-правовая база, оптимизируется организационная структура обмена информацией, обновляется и расширяется технологическая база.

Работа по использованию преимуществ информационных технологий ведется в рамках федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской

[1] Доклад директора ФССП РФ Д.В. Аристова в Совете Федерации Федерального Собрания РФ. – URL : https://youtu.be/fes-2jFmg5o

Федерации». Данный проект предусматривает введение суперсервиса «Цифровое исполнительное производство». Кроме того, продолжает реализовываться такой проект Российской Федерации и Нового банка развития как «Содействие развитию судебной системы Российской Федерации», в ходе которого заключаются государственные контракты на проектирование и внедрение информационных систем ФССП РФ.

Проводимые мероприятия направлены на создание и функционирование механизма взаимодействия граждан и организаций с органами принудительного исполнение посредством Единого портала государственных услуг. Так, в настоящее время установлен порядок получения участниками исполнительного производства сведений о ходе такого производства, подачи ходатайств в рамках производства[1], реализуется возможность исполнения актов о привлечении к административной ответственности путем оплаты штрафов.

Размещенный на официальном сайте ФССП РФ ресурс «Банк данных исполнительных производств» демонстрирует свою востребованность, в 2020г. на него было направлено 584 млн запросов, что почти в два раза больше нежели в 2019 г.[2].

Отдельным направлением использования компьютерных и сетевых технологий является обмен сведениями ФССП РФ с судебными учреждениями; такими государственными органами как ГИБДД, федеральная налоговая служба, регистрационные органы; банками и кредитными учреждениями. В субъектах РФ проводится работа по внедрению механизма направления судами исполнительных документов в органы принудительного исполнения, в том числе мировыми судьями. По данным ФССП в 12 субъектах РФ таким способом в 2020 г. было направлено более 670 тысяч исполнительных документов[3].

Из последних изменений в нормативно-правовой базе следует назвать принятие Федерального закона № 168-ФЗ от 08.06.2020 г. «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации», которым, помимо прочего, органам принудительного исполнения предоставлено право пользоваться данным ресурсом.

Резюмируя изложенное, представляется обоснованным вывод о том, что информационные технологии являются одним из основных инструментов повышения эффективности механизма принудительного исполнения, возрастающее со стороны государства внимание к формированию и использованию таким технологий позволяет выражать сдержанный оптимизм в оценке перспектив развития института принудительного исполнения в Российской Федерации.

---

[1] Согласно итоговому докладу ФССП РФ о результатах деятельности в 2020 г. таких заявлений с начала функционирования ресурса в ноябре 2020 г. до конца 2020 г. было направлено 93 тыс. – URL : https://fssp.gov.ru/files/fssp/db/files/02021/itogovyjdoklad2020vizual20213221449.pdf (дата обращения 05.04.2021).

[2] Там же.

[3] Там же.

Малышева Е.Ю.,
кандидат юридических наук, доцент,
заведующий кафедрой гражданского права,
ПФ ФГБОУВО «РГУП»
г. Нижний Новгород

Фетисова Т.В.,
кандидат экономических наук, доцент,
доцент кафедры гражданского права,
ПФ ФГБОУВО «РГУП»
г. Нижний Новгород

К ВОПРОСУ О ЦЕЛЕСООБРАЗНОСТИ КВАЛИФИКАЦИИ НОВЫХ «ТЕХНОЛОГИЧЕСКИХ» ПРАВОВЫХ ЯВЛЕНИЙ В КАЧЕСТВЕ ОСОБЫХ РАЗНОВИДНОСТЕЙ ПРАВООТНОШЕНИЙ

В статье поставлены методологические и содержательные вопросы в отношении судьбы «технологических» правовых явлений и их возможной или нецелесообразной квалификации в качестве особой разновидности правоотношений.

Современная правовая система находится в состоянии трансформации составляющих ее институтов. Традиционные для государственно-правовой сферы категории не могут в настоящее время их в должной мере обслуживать. Это, в первую очередь, относится к доктринальным правовым категориям, которыми являются категории «механизм правового регулирования» и «правоотношение».

Очевидно, что прежде всего «цифровизация» государственной и правовой сферы объективно минимизирует использование традиционных правовых категорий либо потребует принципиального пересмотра и корректировки их содержательной части. Авторами ранее уже были исследованы вопросы объективного соотношения объектов права (вне отраслевой и даже дисциплинарной принадлежности), условно относимых к инновационным, с механизмами права (технологиями), а также возможной квалификации некоторых инновационных объектов в качестве собственно правовых механизмов (технологий). В частности, было предложено используя методы аналитической юриспруденции применить для инновационных объектов специальные правовые режимы, выделив сквозную «целевую» группу – «корпоративные» правоотношения.

В настоящей статье авторы хотели бы продолжить исследование инновационных процессов в праве и акцентировать внимание на более общем вопросе – вопросе квалификации правоотношений как «технологических» посредством выявления как положительных, так и отрицательных

индикаторов. Прежде всего считаем необходимым представить краткий обзор необходимых законодательных источников и соответствующей научной литературы.

В 2019–2020 гг. блок «цифровых законов» существенно пополнился: внесены изменения в ст. 128 ГК РФ[1], приняты законы о краудфандинге[2]; о цифровых финансовых активах и цифровой валюте[3]; об экспериментальных правовых режимах в сфере цифровых инноваций (далее – Закон об ЭПР)[4]; о финансовых маркетплейсах[5]. Несмотря на то, что теперь такие явления, как «цифровой финансовый актив», «цифровая валюта», утилитарные цифровые права, новый вид ценной бумаги – цифровые свидетельства – официально закреплены и определены, экспертное сообщество продолжает активно дискутировать по вопросу соответствия содержания принятых законодательных актов требованиям практики.

В контексте проблематики исследования особый интерес представляет Закон об ЭПР, предполагающий возможность установления особого (экспериментального) правового режима сроком до 3-х лет в ряде приоритетных сфер и отраслей (рис. 1).

Экспериментальный правовой режим предполагает применение в отношении определенного круга субъектов или одного субъекта в течение фиксированного периода времени и на конкретной территории специального регулирования. Такой правовой режим устанавливается на определенное направление разработки, апробации и внедрения цифровых инноваций. Условия конкретного экспериментального правового режима определяются актом специального регулирования – программой экспериментального правового режима. В качестве результата предполагается принятие решение об изменении общего регулирования.

---

1 Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей ГК РФ» // ИСС Гарант.

2 Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 20.07.2020) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // ИСС Гарант.

3 Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ». – URL : http://publication.pravo.gov.ru/Document/View/0001202007310056

4 Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в РФ». – URL : http://publication.pravo.gov.ru/Document/View/0001202007310024

5 Федеральный закон от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы». – URL : http://publication.pravo.gov.ru/Document/View/0001202007200033? index=1&rangeSize=1. Федеральный закон от 20.07.2020 №212-ФЗ «О внесении изменений в отдельные законодательные акты РФ по вопросам совершения финансовых сделок с использованием финансовой платформы». – URL : http://publication.pravo.gov.ru/Document/View/0001202007200055?index=0&rangeSize=1

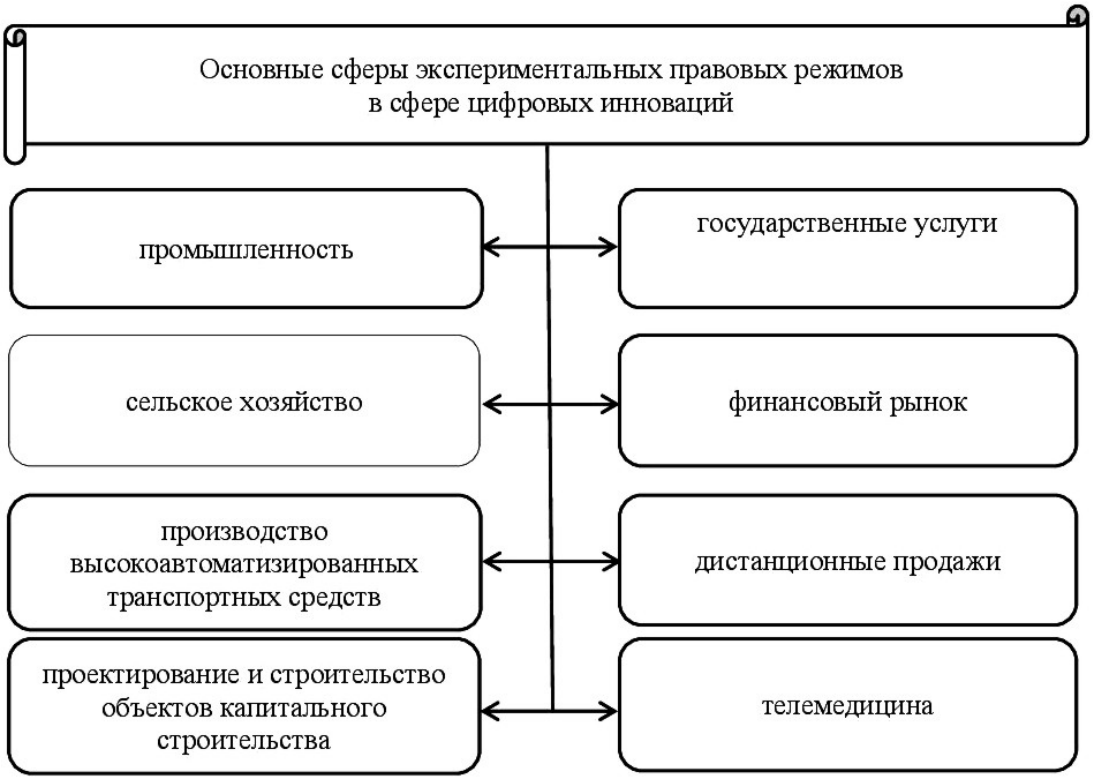

Рисунок 1 – Основные сферы экспериментальных правовых режимов в сфере цифровых инноваций

Алгоритм установления экспериментального правового режима реализуется в достаточно короткий срок (85 дней) и представлен на сайте Министерства экономического развития России (рис. 2).

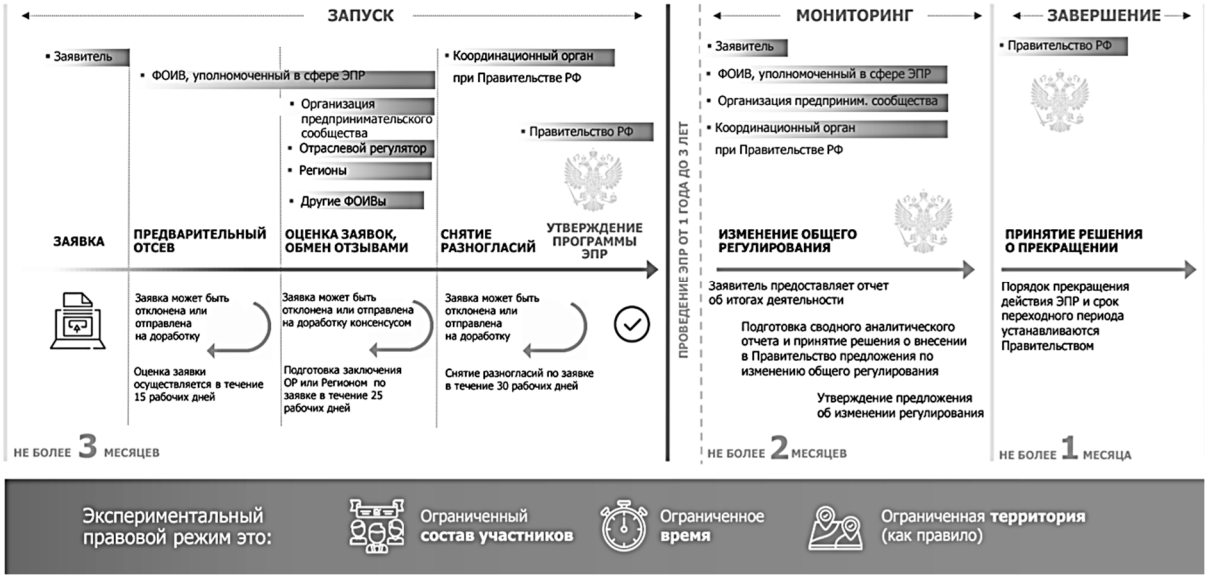

Рисунок 2 – Алгоритм установления экспериментального правового режима в сфере цифровых инноваций[1]

[1] URL : https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/eksperimentalnye_pravovye_rezhimy

«Цифровые законы» положили начало регламентации деятельности новых субъектов финансово-экономического оборота: операторов инвестиционных и цифровых платформ, операторов информационных систем (в которых осуществляется выпуск цифровых финансовых активов), операторов обмена цифровых финансовых активов, фактически включив их в круг особых цифровых субъектов.

Среди научных работ в сфере правовой регламентации технологической составляющей следует отметить работы, посвященные как глобальным изменениям права в условиях цифровизации, так и частным вопросам функционирования отдельных институтов, инструментов, технологий, в частности, цифровых финансовых активов, технологий распределенного реестра, краудфандинга, смарт-контрактов и т.д.

Вопросам инноваций в праве посвящен значительный ряд теоретических работ[1], в частности, в рамках обзора основных направлений инноваций в праве выделяются: предметно-правовое, методологически-правовое, программно-правовое, технико-правовое[2].

На данный момент позволим себе лишь ограничиться постановкой принципиальных и первоочередных, на наш взгляд, вопросов.

Ввиду понимания значимости исследования теории правоотношения, с точки зрения новых модернизированных форматов права, полагаем целесообразным и необходимым изначально дифференцировать вопросы методологического содержательного характера.

Вопросы методологического характера:

1. Будет ли зависеть «доктринальная» и «законодательная» судьба «технологических» правоотношений от вида правопонимания (к вечному вопросу об источниках (формах) права)?

2. Как быть с традиционной теоретической классификацией правоотношений на абсолютные и относительные и нахождением в ней достойного места для «технологических» правоотношений (к вопросу о соотношении статики и динамики)?

3. Впишутся ли «технологические» правоотношения в традиционный механизм правового регулирования (далее МПР) с его неизменной

---

[1] Городов О.А. Правовая инноватика: правовое регулирование инновационной деятельности. Юридическая книга. – 2008. – 408 с.; Волынкина М.В. Инновационное законодательство России. // Законодательство. – 2005. – № 10. URL : https://base.garant.ru/5204031/; Курышев Е.Ю. Направления инноваций в праве: перспективы развития. Международный научный журнал «Инновационная наука». – 2015. – № 12. – С. 138–139. – URL : https://cyberleninka.ru/article/n/napravleniya-innovatsiy-v-prave-perspektivy-razvitiya/viewer; Пашкова Д.А. К вопросу о понятии «инновация» в российском праве. Вопросы экономики и права. – 2017. – № 6. – С. 7–11. – URL : https://law-journal.ru/files/pdf/201706/201706_7.pdf (дата обращения 15.12.2020).

[2] Курышев Е.Ю. Направления инноваций в праве: перспективы развития. Международный научный журнал «Инновационная наука». – 2015. – № 12. – С. 138–139. – URL : https://cyberleninka.ru/article/n/napravleniya-innovatsiy-v-prave-perspektivy-razvitiya/viewer

структурой, либо необходим особый «техничный» МПР? А может вообще необходим пересмотр всей концепции МПР, вне зависимости от вхождения новых «составляющих» (к «любимому» многими исследователями вопросу, о так называемых, «субъективных правах» и определению их «истинного» места: внутри или за пределами собственно правоотношения)?

Вопросы содержательного характера:

1. Если «технологическим» правоотношениям быть, то так ли уж они однородны (к вопросу о возможной изначальной их дифференциации и одновременному выбору противоположных методов исследования (индукции или дедукции)?

2. Будет ли востребован для «технологических» правоотношений традиционный элементарный состав (и снова к вопросу о «субъективном» праве)?

3. И самый главный вопрос: что понимать под объектом «технологического» правоотношения (извечный и самый сложный вопрос даже для традиционных правоотношений и, соответственно, риторический вопрос и одновременное предложение о возобновлении дискуссии в отношении «монистической» и «плюралистической» теорий объекта правоотношения)?

На данный момент однозначное решение вопроса о «технологических» правоотношениях невозможно, и авторы позволяют себе предложить следующие тезисы-вопросы (положительные и отрицательные индикаторы) для дальнейшего обсуждения.

1. Если «технологическим» правоотношениям быть:

– они могут быть встроены в модернизированную модель «механизма правового регулирования» либо какого-либо его современного аналога;

– в силу неоднородности «технологических» правоотношений на первом этапе исследований предлагаем разработать «базовую» (возможно экспериментальную по аналогу «экспериментальных правовых режимов») модель условного «технологического» правоотношения.

2. Если рассматривать содержательный (элементарный состав) «технологических» правоотношений:

– единственный объект – это технологии (на данный момент универсального понимания «технологии» как объекта права нет и скорее всего в ближайшее время не будет (не решается принципиальная проблема «целесообразного конструктора» статьи 128 ГК РФ);

– субъекты «технологических» правоотношений: фиксируется множественная и неоднородная составляющая; замечены новые элементы фикционной составляющей, отличающиеся от обычного представления и понимания фикций в праве; увеличивается количество особых явлений по алгоритму «субъект-объект»; замечено появление «контекстных» субъектов;

– содержание «технологического» правоотношения: на данном этапе вынуждены признать нецелесообразность и преждевременность даже постановки вопроса о содержании в рамках традиционной корреляции

«права и обязанности сторон»; возможно содержание такого правоотношения будет находиться в плоскости исключительно технических и (или) процедурных действий.

Учитывая состояние современного «цифрового» законодательства и содержание доктринальных разработок по исследуемой проблематике, считаем, что рассматривать элементарный состав «технологических» правоотношений в традиционном контексте на данный период времени нецелесообразно и непродуктивно. Полагаем, прежде всего, следует определиться с методологическими принципами исследования правовых явлений с технологическими компонентами.

Мелоян В.Г.,
кандидат педагогических наук, доцент,
доцент кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

ФОРМИРОВАНИЕ ЭЛЕКТРОННОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ВУЗА: АНАЛИЗ ЭФФЕКТИВНОСТИ И РЕЗУЛЬТАТИВНОСТИ ФУНКЦИОНИРОВАНИЯ

При формировании электронной информационно-образовательной среды (ЭИОС) вузы самостоятельно определяют её структуру и составные элементы, чем и обусловлено наличие различных определений ЭИОС.

Следует отметить, что опыт создания и функционирования ЭИОС в российских вузах незначителен: от двух до десяти лет. В отечественной научной литературе мало информации, относящейся к анализу функционирования и эффективного использования ЭИОС в различных образовательных организациях.

Необходимость рассмотрения ЭИОС вуза как единой системы, обусловлена отсутствием единого алгоритма формирования ЭИОС в высшей школе в целом, и необходимостью создания унифицированного методологического подхода, к процессу создания и функционирования ЭИОС.

Внедрение глобальной вычислительной сети Интернет и ИКТ оказали огромное влияние на формирование ЭИОС, как одной из важных областей информационно-образовательной среды.

Это стало возможным благодаря доступности к электронным образовательным ресурсам и возможностью взаимодействия групп участников всех участников образовательного процесса через ИКТ. Применение информационных технологий в процессе обучения способствовало реализации

технологии дистанционного обеспечения в современном образовательном процессе.

Технология дистанционного обучения предусматривает развитие следующих видов технологий:

а) кейс-технологии, когда учебно-методические материалы комплектуются в специальный набор (кейс от англ. *case*) и передаются (пересылаются) обучаемому для самостоятельного изучения (с периодическими консультациями у назначенного ему руководителя (tutor);

б) TV-технологии, которая базируется на использовании телевизионных лекций с консультациями у тьюторов. TV-технологии, имитирует очную форму, способствуют расширению аудитории за счет удаленных студентов, с которыми преподаватель и студенты вступают в контакт (по типу телемоста). Данная модель обучения требует присутствия студентов (как и в очной форме) в данное время, в данном месте.

Использования TV-технологии разнообразны, к ним можно отнести:

– проведение лекционного и семинарского занятия преподавателем другого вуза;

– совместная работа над проектом исследователями из разных образовательных учреждений.

в) сетевые технологии, построенные на использовании сети Интернет, которые обеспечивают обучаемого учебно-методическим материалом, а также, интерактивное взаимодействие тьютора и обучаемого и обучаемых между собой.

Рассматривая управленческий аспект электронной информационно-образовательной среды необходимо выделить следующие четыре взаимосвязанных подсистем: техническая подсистема, информационная, кадровая и регламентная.

Техническая подсистема включает следующие компоненты технического обеспечения: серверы, компьютеры, локальная сеть, проекционное и телекоммуникационное оборудование.

Информационная подсистема предусматривает доступность обучающихся к необходимому программному обеспечению, медиатеке, электронным УМК дисциплин, информационному контенту сайтов вуза и преподавателей.

Кадровая подсистема объединяет преподавателей, студентов, руководство и сотрудников образовательного учреждения. Компоненты кадровой системы выступают в качестве субъектов ЭОИС.

Регламентная система на основе разработанных соответствующих регламентов, инструкций, положений, приказов, распоряжений и иных нормативных актов, в которых прописываются правила взаимодействия различных элементов в рамках ЭОИС, обеспечивает бесперебойная и качественную работу ЭОИС.

Автором под электронной информационно-образовательной средой (далее ЭИОС) понимается «совокупность информационно-телекоммуникационных технологий, включая электронные информационные и

образовательные ресурсы, которые позволяют студентам освоить образовательную программу, независимо от места нахождения обучающего.

Построение эффективно функционирующей ЭИОС невозможно без чётко сформулированных целей, задач и принципов её построения.

Принципы доступности, открытости, системности, многофункциональности, интеграции всех компонентов ЭИОС способствуют достижению таких целей как:

– создание на основе современных информационных технологий единого образовательного пространства;

– информационное обеспечение образовательного процесса в соответствии с требованиями к реализации образовательных программ Университета;

– создание на основе современных информационных технологий площадки для коммуникации между научно-педагогическими работниками и обучающимися.

Достижению сформулированных целей эффективного функционирования ЭИОС, способствуют решения следующих задач:

– организация доступа к основным профессиональным программам, учебным планам, рабочим программам дисциплин (модулей), практик, программам государственной итоговой аттестации, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах:

– фиксация хода образовательного процесса, результатов текущей, промежуточной аттестации и результатов освоения основной профессиональной образовательной программы;

– формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы;

– создание условий для организации взаимодействия между участниками образовательного процесса, в том числе синхронного и (или) асинхронного посредством сети «Интернет»:

– проведение всех видов занятий, процедур оценки результатов обучения, реализации которых предусматривает применение электронного обучения, дистанционных образовательных технологий.

Удовлетворение информационных потребностей всеми участниками взаимодействия с образовательной средой, выступает ключевым параметром качественного функционирования ЭИОС.

В статье рассмотрены следующие группы участников взаимодействия с ЭОИС[1].

Первую группу составляют студенты, которые в процессе освоения учебной программы активно используют издания электронных

[1] Прохоренков П.А. Этапы формирования электронной информационно-образовательной среды вуза / П.А. Прохоренков // Международный журнал экспериментального образования. – 2016. – № 2-2. – С. 291–294.

библиотечных систем и электронные образовательные ресурсы университета. Студенты активно используют дистанционные образовательные технологии в учебном процессе.

Вторая группа представлена профессорско-преподавательским составом, которые выступают как в роли создателей ЭИОС (готовят электронные материалы, разрабатывают учебные программы), так и потребителей данной среды в процессе преподавания дисциплин.

Для качественного использования возможностей ЭИОС необходимы мощные компьютеры, современные пакеты прикладных программ, обеспечивающие быстрый доступ к информационно-образовательным ресурсам.

Третью группу образуют сотрудники структурных подразделений университета, для которых качество ЭИОС определяется наличием в ее составе системы электронного документооборота, позволяющей автоматизировать процесс от приёма студентов до их выпуска.

Четвёртая группа включает внешних пользователей ЭИОС, прежде всего, абитуриентов, заинтересованных в информации об условиях приема и обучения и организации учебного процесса. Ещё одна подгруппа внешних пользователей выполняет функции контролирующих органов. Данная подгруппа проверяет открытость учебного заведения путем анализа материалов, размещенных на сайте вуза, а также, формирует разнообразные электронные отчеты по результатам деятельности учебного заведения.

На эффективность функционирования ЭИОС в вузе влияют множество факторов, выделим следующие из них:

– существование в учебном заведении технических и программных средств информатизации рабочих процессов и практического опыта их эксплуатации;

– наличие эффективной системы научного и методически – организационного процесса информатизации;

– возможность в учебном заведении прохождения подготовки и переподготовки преподавателей в области информационных технологий.

На основе вышесказанного, сформулирован вывод о том, что:

– появление открытых образовательных ресурсов, применение технологий дистанционного обучения, использование облачных сервисов, будет положительно влиять на эффективность и результативность функционирования ЭИОС учебного заведения;

– процесс преподавание с использованием технологии дистанционного обучения сопровождается такими явлениями как отсутствие у ППС строго регламентированных норм и оплаты труда, так и минимизацией воспитательной функции.

Уварова А.В.,
старший преподаватель кафедры
информационных технологий,
ФГБОУ ВО «КубГУ»
г. Краснодар

НЕЙРОННАЯ СЕТЬ ДЛЯ СИТУАЦИОННОГО МОДЕЛИРОВАНИЯ ПРАВОНАРУШЕНИЙ

Эмоции и чувства — это психические процессы, отражающие личную значимость внешних и внутренних ситуаций для жизнедеятельности человека в форме переживаний. Эмоции и чувства включаются во все психические процессы и состояния человека, в частности эмоции проявляются через мимику, движение мышц лица. Так как, в состоянии аффекта или стресса, мимика не контролируема, её распознавание может способствовать более точному определению состояния человека в момент преступления, на допросе или в суде[1].

Эмоция и мимика людей имеет общие особенности независимые от культурного происхождения, расы и пола, поэтому общие черты поддаются генерализации и существует возможность обучить нейронную сеть намного точнее распознавать эмоции, чем это делают люди. Проблемы обучения включают в себя: необходимость высоких вычислительных мощностей, так как обработка изображений требовательный процесс, относительно большое количество времени обучения и сложность сбора обучающих входных данных[2].

Для реализации искусственной нейронной сети решающую поставленную задачу был выбран язык Python. Сеть имеет структуру свёрточной сети и перцептрона, в которой обучение происходит с помощью метода обратного распространения ошибки. Для реализации также необходимы обучающие входные данные. Они должны состоять из фотографий людей, изображающих определённую эмоцию. Решено использовать готовый набор Cohn-Kanade Dataset (CK+48) – набор из 974 черно-белых фотографий людей, размера 48 на 48 пикселя, показывающих 7 эмоций: злость, презрение, отвращение, страх, радость, грусть, удивление.

Первый слой – слой свёртки состоит из шести нейронов – оригинального изображения, который обрабатывается ядром размера 5 на 5. Затем происходит выборка – группа пикселей 2 на 2 уплотняется до одного пикселя, выбирая максимальное значение функции активации среди них.

---

1 Изард К.Э. Психология эмоций. – СПб., 1999.

2 Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. – М., 2015.

Второй слой свёртки состоит из 16 нейронов размера 64 на 64 пикселя с ядром 5 на 5. Затем идёт аналогичный предыдущему слой выборки. Третий слой свёртки состоит из 64 нейрона размера 16 на 16 с ядром 3 на 3. Затем идёт слой выборки переводящий свёрточную нейронную сеть к полносвязной – перцептрону, у которого всего два скрытых слоя, 128 и 7 нейронов соответственно.

Структура такой нейронной сети представлена на рисунке 1.

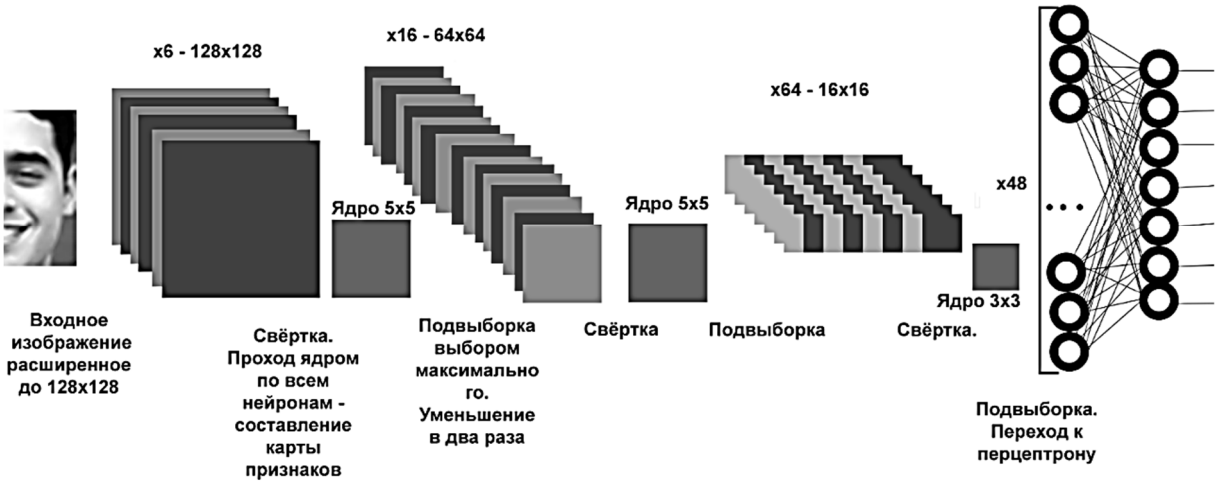

Рисунок 1 – Модель реализуемой свёрточной нейронной сети

После обучения нейронная сеть была использована для распознавания мимики добровольцев и некоторых общедоступных изображений.

При результатах работы на тестовой выборке, составленной из части изображений входных данных, не используемых при обучении, и на новых данных была достигнута точность 97 %. График изменения точности от количества прогонок данных представлен на рисунке 2.

На рисунке 3 представлен результат работы программы по распознаванию эмоций. Программа по загруженной фотографии классифицирует эмоцию одним из 7 классов. В данном случае результат работы нейронной сети это эмоция «Злость». Результат совпадает с ожидаемым.

Таким образом, была получена нейронная сеть и приложение на ее основе, распознающее эмоции человека с высокой точностью. Точность работы на реальных данных будет ниже, так как требуется больше входных данных для обучения. Объединив данную сеть с системой распознавания лиц и видеокамерами, можно получить инструмент, позволяющий поднять качество работы психологов в области правоведения и юриспруденции, в частности, улучшить распознавание состояния аффекта или лжи у подозреваемых и свидетелей, а соответственно уменьшить количество несправедливо вынесенных приговоров.

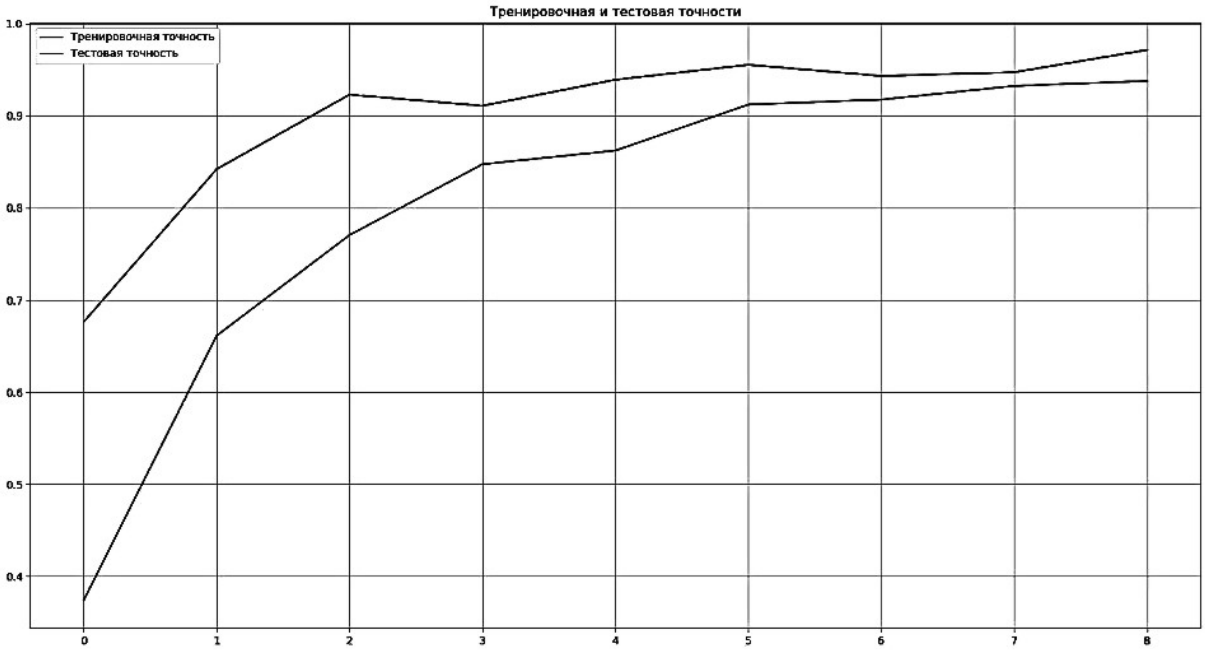

Рисунок 2 – График изменения точности вычислений

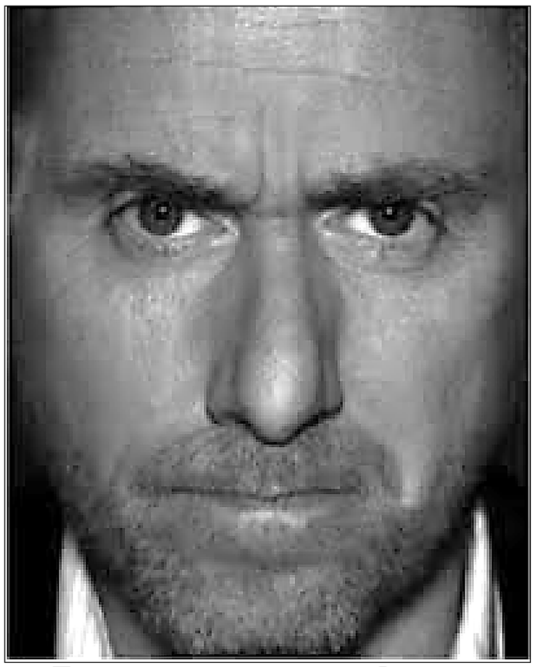

Рисунок 3 – Тестовое изображение и результат работы сети

Паршинцев А.А.,
научный сотрудник,
кафедра атомной физики,
физики плазмы и микроэлектроники,
«МГУ имени М.В. Ломоносова»
г. Москва

РОЛЬ ИНТЕЛЛЕКТУАЛЬНОГО КАПИТАЛА В СИСТЕМЕ УПРАВЛЕНИЯ ЗНАНИЯМИ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРОЕКТНО-ОРИЕНТИРОВАННЫХ КОМПАНИЙ КАК ФАКТОРА ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ СТРАНЫ В УСЛОВИЯХ ИНФОРМАТИЗАЦИИ ЭКОНОМИКИ

В настоящее время в условиях глобализации и возрастающей роли информации и ее потоков в экономике, управлении и обществе важнейшее значение приобретают знания. Как отмечается в Системе национальных счетов: «Приобретение знаний, навыков и квалификации повышает производительный потенциал соответствующих людей и является для них источником будущих экономических выгод»[1].

Следует отметить, что эффективность производственных процессов напрямую зависит от человеческого капитала, то есть знаний, которые люди привносят в процесс производства. При этом в экономической теории человеческий капитал не принято относить к активам предприятий, что подразумевает собой необходимость учета при выработке совокупности управленческих мероприятий в отношении человеческого капитала репутационного фактора и привлекательности для высококвалифицированных специалистов как отдельно взятого предприятия, так и отрасли, региона, и страны в целом[2].

Знания создаются, в частности, в процессе научных исследований, разработок, изучения или инноваций. При этом использование знаний может быть ограничено с помощью юридической или другой защиты. В этом случае знания приобретают форму интеллектуальной собственности.

С учетом того, что в основе интеллектуального капитала лежат знания в различных их проявлениях и формах, а также с учетом отраслевых особенностей в структуре интеллектуального капитала в высокотехнологичных проектно-ориентированных компаниях можно выделить человеческий

---

1 Система национальных счетов 2008. – URL : https://unstats.un.org/unsd/nationalaccount/docs/SNA2008RussianWC.pdf

2 Полякова М.С. Анализ методов оценки интеллектуального капитала / М.С. Полякова, А.С. Новоселов, Е.С. Каплун // Инновации и инвестиции. – 2020. – № 4. – С. 13–17.

капитал, информационно-репутационный капитал и капитал достижений интеллектуального труда[1].

Исходя из вышесказанного, были отобраны индивидуальные показатели, характеризующие основные аспекты интеллектуального капитала в высокотехнологичных проектно-ориентированных компаниях, и оценена степень тесноты их взаимосвязи с уровнем конкурентоспособности стран мира с помощью принятого на международном уровне индекса глобальной конкурентоспособности Всемирного экономического форума.

Среди показателей для проведения корреляционного анализа были отобраны следующие индикаторы:

– численность обучающихся по программам третичного образования на 1000 жителей;

– средняя продолжительность обучения;

– удельный вес работников промышленных предприятий с высшим образованием;

– результаты интеллектуальной собственности на одного жителя;

– объем экспорта высоких технологий в процентах к импорту высоких технологий.

Оценка проводилась с использованием коэффициента корреляции рангов Спирмена за 2017–2019 гг. по 50 странам мира, включая Россию. Расчеты проводились по данным[2].

В результате выполненного корреляционного анализа была установлена достаточно тесная взаимосвязь между уровнем конкурентоспособности страны и ее основными показателями интеллектуального капитала в высокотехнологичных проектно-ориентированных компаниях на протяжении рассматриваемого периода. Так, за рассматриваемый период значение коэффициента корреляции рангов Спирмена варьировалось в пределах от 0,856 с объемом экспорта высоких технологий в процентах к импорту высоких технологий в 2017 году до 0,951 со средней продолжительностью обучения в 2018 году.

Таким образом, можно утверждать, что формирование показателей конкурентоспособности страны происходит под непосредственным влиянием интеллектуального капитала в высокотехнологичных проектно-ориентированных компаниях на мезоуровне как важнейшей совокупности отраслей народного хозяйства[3].

---

[1] Богданова М.В. Анализ интеллектуального капитала: источники информации и система показателей / М.В. Богданова, А.А. Паршинцев // Научное обозрение. Серия 1. Экономика и право. – 2020. – № 5. С. 80–90.

[2] URL : https://www.weforum.org/reports/how-to-end-a-decade-of-lost-productivity-growth/in-full; http://data.un.org/en/iso/ru.html , https://data.worldbank.org/indicator

[3] Рогов А.И. Инвестиции в человеческий капитал как фактор успешного развития организаций и общества в эпоху цифровой экономики / А.И. Рогов, Е.С. Бакина, К.А. Ледовская // Стратегии бизнеса. – 2020 – Т. 8. – № 1(69). – С. 27–30.

Петрушкина А.В.,
старший преподаватель
кафедры государственно-правовых дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

К ВОПРОСУ РЕАЛИЗАЦИИ ПРАВА НА ИНФОРМАЦИЮ В СФЕРЕ ТРУДОВЫХ ОТНОШЕНИЙ

В современной России большое внимание уделяется вопросу информации. В первую очередь такой вывод модно сделать по тому, сколько за последнее время принято нормативно-правовых актов на эту тему. К примеру, Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»[1], Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2], а также множество подзаконных нормативных актов.

Информация в трудовом праве имеет большое значение. Поскольку реализация права на информацию представляет собой правомерную деятельность субъектов правоотношения, которая не противоречит требованиям, установленным нормами информационного права, а также выражается в создании и использовании прописанных законодательством прав и выполнении обязанностей[3]. Следовательно, насколько своевременно, достоверно и в полном объеме будет представлена работником и работодателем информация, будет зависеть законность отношение, которые возникают между субъектами, а также отсутствие конфликтных ситуаций. Кроме того, работник и работодатель, обладая достаточным количеством информации могут минимизировать финансовые издержки, возникающие в связи с недостатком информации. Но независимо от этого необходимо признать, что вопрос реализации права в трудовых отношениях является открытым, и требует дополнительное законодательное регулирование.

В статье 21 Трудового кодекса Российской Федерации установлено, что к основным правам работника относится право на полную достоверную информацию об условиях труда и требованиях охраны труда на рабочем

---

1 Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». – URL : http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения 19.11.2020).

2 Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL : http://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения 19.11.2020).

3 Попов Л.Л. Информационное право : учебник / Л.Л. Попов, Ю.И. Мигачев, С.В. Тихомиров. – М. : Норма : ИНФРА-М, 2010. – С. 58.

месте, а также право на участие в управлении организацией[1]. Данное право урегулировано главой 8 Трудового кодекса Российской Федерации. Также согласно статье 209 Трудового кодекса Российской Федерации условия труда – совокупность факторов производственной среды и трудового процесса, оказывающих влияние на работоспособность и здоровье работника[2]. Исходя из этого, на основании статьи 21 Кодекса работодатель обязан предоставить работнику информацию только по указанному кругу вопросов, то есть работодатель вправе не предоставлять информацию о планируемых изменениях его режима работы, не разъяснять положения локальных нормативных актов, в которых закреплено информация об оплате труда, аттестации и так далее.

Таким образом, необходимо внести в правки в статью 21 Трудового кодекса Российской Федерации о том, что работник имеет право на получение от работодателя информации, которая непосредственно связана с его трудовой деятельностью у конкретного работодателя.

Следующей проблемой исследователи считают то, что в трудовом законодательстве отсутствует четкая информация о предоставлении работником работодателю информации при трудоустройстве. На данный момент в статье 22 Трудового кодекса Российской Федерации не установлено право на требование работодателем от работника определённых документов для существования трудовых отношений.

В статье 65 ТК РФ перечислены документы, которые необходимо предоставить лицу, которое устраивается на работу, для заключения трудового договора. Но в то же время нет разъяснений о том, можно ли отказать в приеме на работу, если у работника отсутствуют документы, которые указаны в списке. К примеру, у работника нет трудовой книжки. Согласно части 5 статьи 65 ТК РФ, работодатель не имеет права отказать в приеме на работу, так как «в случае отсутствия у лица, поступающего на работу, трудовой книжки в связи с ее утратой, повреждением или по иной причине работодатель обязан по письменному заявлению этого лица оформить новую трудовую книжку». Однако данное положение порождает как минимум два вопроса.

Во-первых, как быть, если работник отказывается написать такое заявление? Статья 65 Кодекса не дает права на оформление трудовой книжки в одностороннем порядке. Также в статье 66 Трудового Кодекса Российской Федерации установлено, что работодатель обязан вести трудовую книжку работника, которые проработал у работодателя более 5 дней. А так как норма обязывающая, следовательно, работодатель может быть привлечен к административной ответственности.

---

[1] Трудовой кодекс Российской Федерации: Федеральный закон от 30.12.2001 г. № 197-ФЗ (в ред. от 09.11.2020 г.) // Собрание законодательства РФ. 2001. № 18.

[2] Трудовой кодекс Российской Федерации: Федеральный закон от 30.12.2001 г. № 197-ФЗ (в ред. от 09.11.2020 г.) // Собрание законодательства РФ. 2001. № 18.

Во-вторых, трудовая книжка является документом, который содержит информацию о трудовой деятельности и трудовом стаже работника. С помощью трудовой книжки работодатель может получить достоверную информацию о опыте работника, должностях, которые он занимал ранее, а также применялись ли к нему какие-либо меры поощрения. Если работник указал в резюме информацию о своем трудовом стаже, а затем сообщает информацию об отсутствии трудовой книжке, то работодатель может подвергнуть сомнению данную информацию и в дальнейшем отказать в приеме на работу. Такие случаи очень часто встречаются на практике.

Для урегулирования данного вопроса необходимо закрепить в Трудовом кодексе перечень документов, которые работник должен предоставить работодателю, в случае отсутствия трудовой книжки по какой-либо причине. К таким документам можно отнести, к примеру, копии кадровых приказов, рекомендации и другие.

В современном мире самой основной проблемой в теории и практике реализации информации в сфере трудового права является персонализации данных. Авторы считают информационное право самостоятельной отраслью права в системе российского права. Предметом отрасли информационного права являются общественные отношения, которые связаны с правовым регулированием оборота информации, создание, формирование, хранение и обработка, распространение, использование информационных ресурсов. Исследователи считают, что предмет информационного права неоднородный, то есть информация в определённой мере входит в любые правоотношения: государственные, административные, трудовые и другие1.

Относительно информационных отношений в трудовом праве, хотелось бы отметить, что право на информацию в сфере труда включает в себя целый ряд правомочий:

1. Право на получение информации, перечень которой определяется для конкретного случая;
2. Право на доступ к информации, которая уже имеется у субъекта;
3. Право на иную обработку информации, именно хранение, передачу, распространение и так далее.

Работник имеет право только на получение и доступ к информации, а все остальное является правомочием работодателя. Отдельно выделяется правомочие на защиту трудовой информации, в том числе персональных данных работников, сюда же относятся претенденты на вакансии и бывшие работники.

В трудовом законодательстве закреплено, что работодатель имеет право требовать от работников обеспечение сохранности информации конфиденциального характера – это является государственной, коммерческой,

---

[1] Волков Ю.В. Информационное право. Информация как правовая категория: учебное пособие для бакалавриата и магистратуры / Ю.В. Волков. – 2-е изд., стер. – М. : Издательство Юрайт, 2019. – С. 89.

служебной и иными видами тайн, которые чаще всего носят профессиональный характер[1].

Персональные данные относятся к служебной тайне и могут быть связаны не только с работниками, но и с лицами, которые ищут работу, либо являются бывшими работниками.

Несмотря на большое количество исследований в области персональных данных работников, в законодательстве все равно существуют некоторые пробелы.

Согласно статье 3 Федерального закона Российской Федерации «О персональных данных», к персональным данным является любая информация, которая прямо или косвенно относится к определенной физическому лицу[2].

В статье 2 Федерального закона Российской Федерации «Об информации, информационных технологиях и защите информации» дается определение конфиденциальной информации – это обязательное для выполнения лицом, получившим доступ к такой информации, требование не передавать такую информацию третьим лицам без согласи ее обладателя. В отношении определенных категорий работников приняты положения о персональных данных, которые утверждены специальными нормативно-правовыми актами[3].

Согласно статье 85 Трудового кодекса Российской Федерации персональные данные работника – это информация, которая необходима работодателю в связи с трудовыми отношениями и касается конкретного работника. Исходя из вышесказанного, можно выделить признаки персональных данных работника:

1. Это информация, которая необходима работнику в связи с трудовыми отношениями. Объем и содержание такой информации зависят от специфики работы и видов, выполняемых раб, статус работодателя и работника. Таким образом, информация может различаться в зависимости от обстоятельств, но в любом случае такая информация должна вытекать из потребностей работодателя как со стороны трудового отношения. Следовательно, необходимо в локальных нормативных актах уточнить какие данные не являются необходимыми для данного работодателя и постараться максимально исключить их из обрабатываемой информации.

---

[1] Федеральный закон от 29.07.2004 г. № 98-ФЗ (ред. от 18.04.2018 г.) «О коммерческой тайне» // СПС «КонсультантПлюс». – URL : http://www.consultant.ru/document/cons_doc_LAW_48699 (дата обращения 20.11.2021).

[2] Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». – URL : http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения 19.11.2021).

[3] Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС ««КонсультантПлюс». – URL : http://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения 19.11.2021).

2. Информация должна касаться физического лица в качестве работника и должна быть связана с его профессиональными характеристиками. То есть работодатель имеет право запросить только ту информацию, которая характеризует работника как сторону трудового договора, но не как личность. Таким образом, работодатель не может требовать информацию о хобби, привычках, политических взглядах и так далее.

Итак, российское законодательство имеет некоторые пробелы, которые подтверждаются на практике. Для их устранения необходимо внести изменения в трудовое законодательство. Во-первых, в Трудовом кодексе Российской Федерации необходимо установить, что работник имеет право на получение любой информации, которая непосредственно связана с его трудовой деятельностью у работодателя, а он обязан такую информацию предоставить. Во-вторых, необходимо установить последствия непредоставления информации при трудоустройстве, либо ее частичное предоставление. В-третьих, необходимо устранить некоторые противоречия норма Трудового кодекса Российской Федерации и специальных федеральных законов о персональных данных, а также создание конкретных локальных нормативных актов, которые будут регулировать вопросы персональной информации в трудовых отношениях.

Хуноян А.С.,
аспирант кафедры информационного права,
информатики и математики,
ФГБОУВО «РГУП»
г. Москва

ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БАНКОВСКОЙ СФЕРЕ

По мере того, как меняются традиционные формы финансовой деятельности, технологии знаменуют важный переход для финансовых учреждений от финансовых услуг, ориентированных на человека, к финансовым услугам, ориентированным на компьютеры[1]. Постепенный переход к финансовой индустрии, основанной на компьютерах и данных, уже можно увидеть в быстром росте сектора финансовых технологий (FinTech). Этот переход также означает, что финансовые учреждения должны адаптировать

[1] A Digital Tsunami: FinTech and Crowdfunding, International Scientific Conference on Digital Intelligence / R.M. Lacasse – Quebec City, Canada, April 4–6, 2016. – URL : http://fintechlab.ca/wp-content/uploads/2016/11/Digital-Tsunami-Site-Web.pdf (date of application 07.03.2021).

свои бизнес-модели, компьютерные системы и распределительные сети к новым реалиям.

Банковская отрасль является одной из наиболее быстро развивающихся, но при этом и подверженных самым различным рискам и опасностям. Одним из ключевых направлений развития общественных отношений в сфере банковской деятельности в период цифровизации экономики, безусловно, является внедрение новейших финансовых технологий, которые должны способствовать достижению самых различных задач.

Одной из наиболее перспективных, но пока слабо урегулированных финансовых технологий является технология искусственного интеллекта и сопутствующие технологии, которые открывают широкие горизонты как непосредственно в сфере банковской деятельности, так и в принципе для общего развития информационной среды[1].

Активное внедрение технологий искусственного интеллекта и робототехники во все сферы жизнедеятельности человека поставило целый ряд вопросов перед регулятором. Как следствие, к настоящему моменту в мире уже накоплен определенный опыт не только идентификации, но и решения отдельных правовых проблем в этой сфере, однако неопределённость правового регулирования по большому количеству ситуаций все ещё остается. Технологии искусственного интеллекта и машинного обучения относительно новы и какие-либо международные стандарты, и правила в этой области только вырабатываются.

Существует достаточно большое количество ситуаций, в которых те или иные аспекты применения технологий искусственного интеллекта потребуют корректировки правового регулирования. Вот некоторые из них: проблема алгоритмической прозрачности, проблема использования данных, проблема ответственности, проблема интеллектуальной собственности, проблема дискриминации и этики, проблема трансграничности финансовых рынков и др.

В финансовом секторе технологии искусственного интеллекта имеют широкие возможности для применения. Сюда можно отнести правовое регулирование инвестиционной деятельности с использованием искусственного интеллекта, в том числе для осуществления алгоритмической торговли («торговые роботы»), применение технологий искусственного интеллекта кредитными организациями для клиентского обслуживания и для осуществления деятельности, напрямую не связанной с обслуживанием клиентов (правовой статус ИИ – чат-боты, финансовые консультанты, прием заявок на кредиты), правовые последствия принятия носителем искусственного интеллекта неверных решений или ошибок, повлекших нанесение вреда, обработка различного рода финансовых данных, в том числе большого массива

[1] Ручкина Г.Ф. Финансовые технологии в России и за рубежом: тенденции правового регулирования создания и использования / Г.Ф. Ручкина, В.К. Шайдуллина // Банковское право. – 2018. – № 2. – С. 7–8.

данных о банковских операциях, анализа рынков и рыночной информации, финансовой отчетности[1].

Также необходимо отметить, что наиболее важными для регулирования являются те сферы применения искусственного интеллекта, которые, во-первых, позволяют максимально сократить издержки и потери (антифрод, противодействие легализации доходов, полученных преступным путем), и во-вторых, применяются напрямую при оказании банковских и иных финансовых услуг кредитными организациями (кредитный скоринг, инвестиционный консалтинг).

Таким образом, каждая сфера применения технологий искусственного интеллекта в финансовом секторе предполагает специфическое регулирование в зависимости от конкретных условий их внедрения.

Столкнувшись с возможностями и проблемами, создаваемыми искусственным интеллектом, банки и другие финансовые игроки сталкиваются с медленным, длительным, рискованным и потенциально очень дорогостоящим процессом перехода и интеграции новой технологии в свою деятельность[2].

Государствам необходимо будет разработать и принять нормы и правила, чтобы облегчить этот важный переход. Создание регулирующей инфраструктуры требует, чтобы регулирующие органы работали с экспертами по технологиям, чтобы понимать, управлять и контролировать риски, связанные с искусственным интеллектом в цифровой, физической, экономической и политической сферах[3].

Суммируя всё вышесказанное, необходимо подчеркнуть, что развитие технологии за последние несколько лет во всём мире поражает, а правовое регулирование формируется уже постфактум, потому необходимо учитывать тот небольшой опыт зарубежных государств, который уже сформировался, для эффективного правового регулирования применения технологии искусственного интеллекта не только в банковской, но и во всех финансовых отраслях.

---

[1] Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года». – URL : http://www.pravo.gov.ru

[2] Bharadwaj R. AI for Cybersecurity in Finance – Current Applications, Emerj. – URL : https://emerj.com/ai-sector-overviews/ai-cybersecurity-finance-current-applications/ (date of application 07.03.2021).

[3] Newman J.C. Toward AI Security: Global Aspirations for a More Resilient Future, CLTC White Paper Series. – URL : https://cltc.berkeley.edu/wp-content/uploads/2019/02/CLTC_Cussins_Toward_AI_Security.pdf (date of application 07.03.2021).

Чеботарева И.Ю.,
кандидат юридических наук,
доцент кафедры гуманитарно-правовых дисциплин,
филиал ФГБОУ ВО
«Адыгейский государственный университет»
г. Белореченск

ЭФФЕКТИВНОЕ ЗАКОНОДАТЕЛЬСТВО КАК ЗАДАЧА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Поток информации в настоящее время неумолимо растет и развивает информационное общество. Соответственно, актуальность вопросов обеспечения информационного поля безопасностью различными средствами становиться все более значимыми. Это в первую очередь вызвано технологиями, которые постоянно совершенствуются и дорабатываются, а также внедрением новых возможностей в систему взаимодействия общества.

Как указано в Доктрине информационной безопасности Российской Федерации, информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

Напомним, что информационная безопасность – это практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности в экономическом плане – это сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности ее применения и без какого-либо ущерба.

Но каково положение информационной безопасности в правовом поле?

Законодательные основы любого государства в области информационной безопасности являются необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, геополитических, военных и иных направлений функционирования этого государства. Сегодня информационная безопасность становится базовым элементом системы национальной безопасности России, что обусловлено быстро растущими технологическими возможностями современных информационных систем, влияющих на хозяйственно-

экономическую жизнь, духовно-идеологическую сферу и умонастроения людей[1].

Нормативная база по вопросам информационной безопасности России включает Конституцию Российской Федерации, федеральные законы; кодексы Российской Федерации; постановления Правительства Российской Федерации; ведомственные нормативные акты. Правовой основой обеспечения информационной безопасности является Федеральный закон от 27.07.2006 г. № 149-ФЗ (в редакции от 29.12.2020 г.) «Об информации, информационных технологиях и о защите информации». Важным документом является Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации». Основополагающим документом в области информационной безопасности является утвержденная 5 декабря 2016 г. Президентом Российской Федерации Доктрина информационной безопасности, представляющая совокупность целей, задач, принципов, основных направлений обеспечения информационной безопасности Российской Федерации. Доктрина служит основой для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации, подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации, разработки целевых программ обеспечения информационной безопасности Российской Федерации. Таким образом, непосредственно нормативно-правового акта о правовых основах, формах и методах информационной безопасности сегодня не принято. Однако, несколько компенсировалась ситуация в связи с принятием в 2017 году и вступлением в силу в 2018 году нового федерального закона о безопасности критической информационной инфраструктуры России.

Так, обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

---

[1] Михнев И.П. Природные радионуклиды как источник фонового облучения населения Нижневолжского региона / И.П. Михнев, С.В. Михнева; Гл. ред. О.Н. Широков // Образование и наука: современные тренды : колл. монография. Сер. «Научно-методическая библиотека». – Чебоксары, 2018. – С. 151–166.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

Все это перечислено в Доктрине информационной безопасности, но необходимого конкретизирующего законодательства пока не создано. Также важно при всем этом учитывать, что деятельность в области «информационной безопасности» – это не защита информации, т.к. такого объекта прав в российском законодательстве не существует, следовательно, отсутствуют основания использовать предусмотренные законом способы защиты прав (статья 12 ГК РФ). Информационная безопасность с юридической точки зрения – это профессиональная деятельность, заключающаяся не в защите информации, а в защите прав и законных интересов лиц, возникающих в связи с обменом информацией (т.е. сведениями, сообщениями, данными не зависимо от формы их представления), ее обработкой, передачей и хранением.

В связи с чем, анализ правовых основ в этой деятельности должен опираться на положения ныне действующего законодательства. Необходимость принятия официального законодательного документа об информационной безопасности продиктована современными угрозами информационным ресурсам. Поэтому, учитывая сформированные в России органы государственной власти и местного самоуправления требуется предусмотреть информационную безопасность как для физических лиц и частных юридических лиц, а также для органов власти – публично-правовых субъектов права. И приоритетным направление должно является эффективное законодательство, работающее и действующее в правовом регулировании информационной безопасности.

Черных А.М.,
кандидат технических наук,
доцент кафедры информационного права,
информатики и математики,
ФГБОУВО «РГУП»
г. Москва

ПРОЦЕССЫ СИТУАЦИОННОГО УПРАВЛЕНИЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБУЧЕНИЯ

В современных условиях юридическая, экономическая и управленческая профессиональная деятельность интенсивно изменяется в связи с внедрением информационных и коммуникационных технологий. Широкое создание и внедрение информационных систем, технологий хранения и обработки информационных массивов различного назначения требует определённых знаний основ информологии, информационных систем и технологий.

Изучение студентами Российского государственного университета правосудия (РГУП) материала дисциплин в рамках профессиональных образовательных программ связано с использованием различных информационных ресурсов университета. Подготовка специалистов включает необходимость переработки и анализа больших массивов научной, учебной и аналитической информации в области юриспруденции. В системе получения знаний студентами университета широко используется сеть библиотек, как обычных, так и электронных, структурированные базы данных и знаний, электронные книги и учебные пособия, распределённые информационные системы (сети Internet, Intranet), содержащие учебную, научную и специальную информацию (рис. 1). Существующая информационная система представляет собой автоматизированную систему обучения (АСО).

В централизованных интегрированных больших информационных системах, к которым относится автоматизированная система обучения высшего учебного заведения, обеспечение безопасности информации относится к наиболее актуальным задачам. Эффективное обеспечение защищённости учебно-методической информации в динамике реального времени функционирования АСО, с учетом сложившейся ситуации при нарушении безопасности информации, возможно с позиций ситуационного подхода. Синтез и оптимизация процессов обеспечения защищённости информации происходит в подсистеме контроля и защиты информации (КЗИ) в реальном времени функционирования АСО и реализуются в ходе ситуационного управления.

Рисунок 1 – Структура информационного ресурса университета

Под термином «ситуационное управление» защищённостью учебно-методической информации понимается процесс оперативного управления защищённостью информации и выработки организационно-технических решений, за основу которого принимаются ситуации, возникающие в процессе целевого функционирования подсистемы КЗИ (процесса) АСО и решения им соответствующие. При этом ситуация – есть описание состояний подсистемы КЗИ и элементов АСО на определенный момент времени меняющейся обстановки[1].

Обеспечение эффективности функционирования подсистемы КЗИ по ситуационному управлению осуществляется администратором защиты информации или лицом, принимающим решения (ЛПР). Сопровождение программного обеспечения подсистемы КЗИ сводится к совершенствованию и пополнению системы понятий защищённости информации в процессе обучения слушателей и функций предметной области по результатам анализа

[1] Ловцов Д.А. Введение в информационную теорию АСУ. ВА им. Ф.Э. Дзержинского 1996; Ловцов Д.А. Информационная теория эргасистем. Тезаурус. – М. : Наука, 2005. Ловцов Д.А. Управление безопасностью эргасистем / Д.А. Ловцов, Н.А. Сергеев. – М. : РАУ-Университет, 2001.

потребностей для защиты информации. Наличие у администратора защиты информации, ЛПР формализованных структурированных данных в области защиты информации даёт возможность, заполняя или модифицируя данные о состоянии подсистемы КЗИ, изменять взаимосвязанную работу программ-функций обеспечения конфиденциальности, сохранности, достоверности информации на различных периодах подготовки специалистов юриспруденции и в условиях информационного соперничества.

Специфику ситуационного управления защищённостью информации обусловливает наличие у ЛПР логико-лингвистических средств переработки качественной информации о состоянии подсистемы КЗИ и возникающих в реальной обстановке угрозах защищённости учебно-методической информации. Использование информационно-кибернетического системного подхода к задачам ситуационного управления защищённостью информации дает возможность рассматривать его в АСО на уровне абстракции, как организованную совокупность технологических процессов переработки информации и позволяет оптимизировать процедуры обеспечения защищённости учебно-методической информации.

Функции перехода между информационными процессами при подготовке студентов в высшем учебном заведении, отражают сущность переработки учебно-методической информации в данном виде подготовки слушателей и программируются для подсистемы КЗИ АСО[1]. Создание функциональной базы данных и знаний (БДЗ) подсистемы КЗИ заключается в заполнении структуры данных соответствующими понятиями процесса подготовки студентов, требованиями к защищённости учебно-методической информации, данными, определяющими информационные угрозы, фактами нарушений защищённости информации и способами их устранения. Данный подход к задаче обеспечения защищённости информации позволяет использовать информационно-математическое обеспечение (ИМО) подсистемы КЗИ при изменении требований образовательных стандартов и форм обучения, для различных форм представления учебной информации и категорий конфиденциальности.

Особенностями автоматизации ситуационного управления защищённостью информации в АСО в постановке задачи обеспечения защищённости информации, выражается в соответствующей системе понятий в области защиты информации и рассматривается, как система понятий формальной модели АСО, используемая для автоматизации процесса обеспечения защищённости информации. Это позволяет устранить затруднения, возникающие при взаимодействии администратора защиты информации с комплексном средств автоматизации (ЭВМ) подсистемы КЗИ в процессе решения

---

[1] Злобин С.М. Эффективность образовательного процесса и информационные технологии / С.М. Злобин, А.М. Черных; РАН // Труды V Межведом. науч.-техн. конф. «Проблемы совершенствования систем защиты информации и образовательных технологий подготовки специалистов в области информационной безопасности» (14–16 сентября 2005 г.). – Краснодар : КВИ, 2005. – С. 99–109.

функциональных задач АСО с учётом требований защищённости информации[1].

На основе анализа известных АСО и интеллектуальных систем управления определяются общие требования и базисная структура экспертной информационной системы (ЭИС) подсистемы КЗИ, согласно которой ЭИС позволяет администратору защиты информации исследовать ситуации нарушения защищённости информации в АСО, решение которых проводится на основе прикладных алгоритмов ситуационного управления защищённостью информации подсистемы КЗИ. Если такие алгоритмы не существуют, то путем логического вывода или аргументированного обоснования администратором (экспертом) защиты информации они вырабатываются с учётом конкретной ситуации.

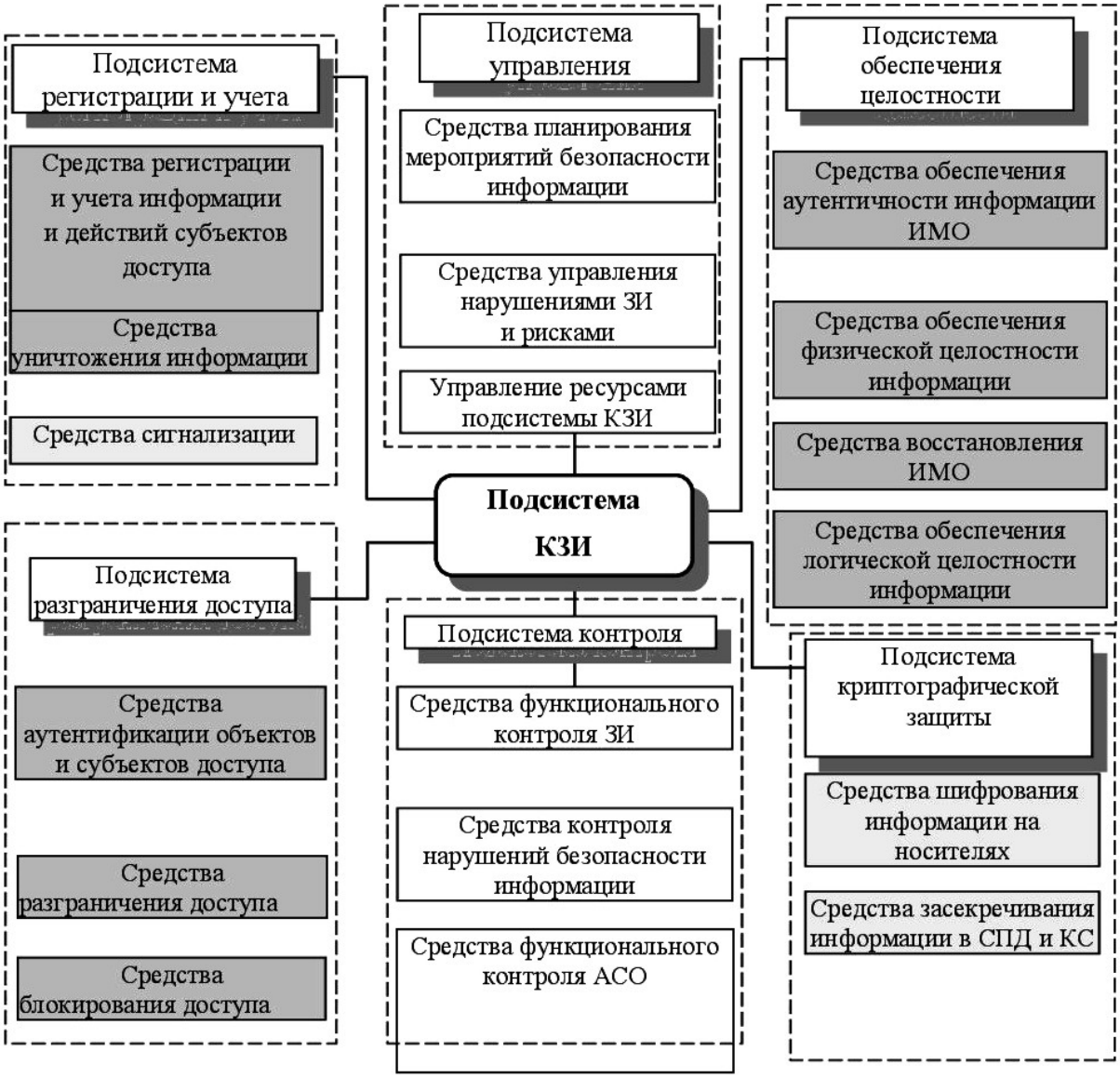

Рисунок 2 – Обобщенная структурная схема подсистемы КЗИ АСО

[1] Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

В последнем случае решение задач обеспечения защищённости информации подсистемой КЗИ АСО обеспечивается способностью ИМО ЭИС формировать логические выводы и обоснованные рекомендации на основе знаний в области защиты информации. ЭИС обеспечивает информационные процессы накопления, интеграции, уточнения, поиска, извлечения, интерпретации, знаний об АСО и образовательном процессе, угрозах защищённости информации и изъянах в подсистеме КЗИ, реорганизацию БДЗ с учётом нарушений защищённости информации в АСО.

Структура данных ЭИС подсистемы КЗИ описывает систему понятий защиты информации в АСО в процессе обучения и определяет начальные, промежуточные, целевые лингвистические показатели.

Структура математической модели ситуационного управления защищённостью информации подсистемы КЗИ АСО состоит из трёх основных компонентов:

S – множество средств автоматизации *g* – типов расположенных в различных Z – элементах системы АСПС; *R* – множество ресурсов, используемых для защиты информации подсистемой КЗИ; *A*(*p*) – множество ЗИ, подлежащих реализации подсистемой КЗИ АСПС при существующих ограничениях.

$$Z\ g\ l(g),$$

$$L = \Sigma\ \Sigma\ \Sigma\ S_{zce},$$

$$z = 1,\ c = 1,\ e = 1.$$

База данных знаний (БДЗ) подсистемы КЗИ с программами-функциями обеспечения защищённости информации, представляет собой знания о том, как использовать имеющиеся данные для достижения целей АСО.

Основным средством исчисления высказываний в алгоритме ЗИ подсистемы КЗИ являются семантические сети и фреймовые представления. При решении задач ситуационного управления защищённостью информации используются фреймовые модели, поскольку фрейм представляет собой модульную структуру данных со всей совокупностью включенных в нее процедур обеспечения защищённости информации для распознавания стереотипных ситуаций нарушений защищённости информации.

Язык фреймовых представлений относится к открытой системе, что позволяет оперативно добавлять новые компоненты КЗИ, для соединения фреймов (знаний) используется естественный язык. Фреймы подсистемы КЗИ представляют собой локальные многоуровневые семантические сети (графы, деревья, списки и т.д.) и являются синтаксическими и семантическими блоками информации. В них содержится декларативные и процедурные элементы, обеспечивающие конфиденциальность, достоверность и сохранность перерабатываемой в АСО информации, и связь с фреймами подсистемы КЗИ.

В процедурной и в декларативной части фреймов информация храниться в виде программ. Наличие в фреймах незаполненных участков, (слотов) позволяет заполнять их в процессе активизации функционирования

фрейма обеспечения защищённости информации в соответствии с ситуацией нарушения защищённости информации или предписаниями, которыми они сопровождаются. Данный подход позволяет фрейму настраиваться на модульном, уровне (слотов), и на уровне фреймов подсистемы КЗИ. Фреймовая логико-лингвистическая модель (ЛЛМ) процесса обеспечения защищённости информации строиться в виде совокупности определенным образом сформированных фреймов подсистемы КЗИ и множества фреймов данных пользователей АСО, представляющих собой описание типовых ситуаций нарушений защищённости информации.

Фрейм подсистемы КЗИ представляет не одну конкретную ситуацию нарушения защищённости информации, а наиболее характерные, принадлежащие определённому классу. Система таких фреймов используется при хранении данных нарушений защищённости информации в информационной базе подсистемы КЗИ обобщенной информации, характеризующей процессы защиты информации. Фреймовая ЛЛМ в виде программного комплекса применяется в подсистеме КЗИ АСО и обеспечивает диалоговый человеко-машинный режим, использованием языков программирования высокого уровня (Borland C, C + +, Delphi, СУБД и др.), позволяющих упростить обращение к ПЭВМ.

Таким образом, на основе анализа реальных процессов ситуационного управления защищённостью информации, задач обеспечения защищённости информации и нарушений защищённости информации, особенностей их организации в АСО, определяет содержание и функции моделей и алгоритмов оптимизации процесса ситуационного управления защищённостью информации и реализует их на средствах АСО.

Шиянов Г.П.,
кандидат педагогических наук,
доцент кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

Шиянов Б.Г.,
аспирант
ФГБОУВО «КГУФКСТ»
г. Краснодар

ЭЛЕКТРОННОЕ ПРАВОСУДИЕ ДЛЯ ИГРОВЫХ ВИДОВ СПОРТА В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Наступает новая эпоха в спортивном правосудии – это применение новейших технологий, таких как системы электронных видеоповторов.

Очевидно, что система видеоповторов в игровых видах спорта поможет судьям более точно и справедливо выносить решения по итогам соревнований[1].

В футболе система видео повторов используется для определения взятия ворот, фолов, рассмотрения мелких эпизодов, чтобы помогать бригаде судей в назначении штрафных, пенальти, отмены неверных решений, всесторонней помощи бригаде арбитров.

В хоккее видеоповтор используется только для определения правильности взятия ворот. При этом правила применения видео повтора в Национальной хоккейной лиге (НХЛ) и соревнованиях, проводящих под эгидой Международной федерации хоккея (МФХ).

Начиная с сезона 15/16 начал применяться так называемый тренерский челленджер. Это правило, по которому тренера команд могут объявлять тайм-аут, в любой промежуток игры, если команда сохранила этот самый тайм-аут и пропустила гол, если ошибка судьи доказана, то тайм-аут у команды сохраниться.

В НБА (национальная баскетбольная лига) ситуация с системой видеоповторов тоже крайне интересная, это один из самых ранних случаев, когда в большой спорт, впервые видеоповторы начали использовать в НБА еще в 2002 году в тех случаях, когда требовалось установить, уложился ли в игровое время спортсмен, проводящий бросок. В дальнейшем «полномочия» видеоповтора несколько раз расширялись, и сейчас его можно применять во многих спорных эпизодах, например, определяя в какой момент, до или после броска, случился фол.

С 2006 года данная система начала использоваться в международных баскетбольных соревнованиях. Появились новые нетрадиционные взгляды на подход к судейству. В ходе проведения научных наблюдений, на наш взгляд, самая интересная и самая правильная система видеоповторов «ястребный глаз».

Ястребиный глаз – программно-аппаратный комплекс, моделирующий траекторию игрового снаряда. Система была разработана компанией Roke Manor Research и впервые протестирована в реальных условиях спортивных соревнований в 2001 году. Система «ястребный глаз» стала неотъемлемой частью теннисной, крикетной и с нового сезона футбольной культуры, которая, по сути, стала прародителем футбольной системы VAR, добавила соревновательному процессу зрелищности и способствовала укреплению духа fair play (чистая игра) в ходе соревнований. Получила несколько наград за достижения в сфере развлечений. Хотя система имеет и немало критиков, которые считают, что автоматизация судейства в спорте лишает его человеческого фактора и особого соревновательного духа.

---

[1] Использование видеоповторов в различных видах спорта. – URL : https://sport.rambler.ru/other/37200730/?utm_content=sport_media&utm_medium=read_more&utm_source=copylink

В научно-практической литературе методике видеоповторов не уделяется должного внимания.

В условиях пандемии коронавируса система видеоповторов особенно важна в спорте, так как она может работать удаленно, что уже было применено в недавнем матче футбольной лиги чемпионов УЕФА между Испанской «Севильей» и лондонским «Челси», где бригада работала удалённо, что позволило обезопасить бригаду от заражения.

Специалистами осуществляется активная научно-исследовательская деятельность, направленная на поиск новых систем, которые могли бы стать основой коррекции игрового процесса.

Однако эта точка зрения в последнее время непопулярна среди спортивных боссов. Они считают, что скандалы, вызванные судейскими ошибками и подозрения, что ошибки были совершены намеренно, наносят организаторам соревнований слишком большой урон. А системы электронного судейства якобы способны минимизировать этот вред. Действительно – кто возьмется обвинять робота в симпатиях или антипатиях к одному из соперников?

И это тоже проблема. Можно обвинить машины, забывая, что принятие решения остается за судьей.

Каковы же главные последствия массового использования электронных средств судейства в профессиональном спорте и спорте высших достижений?

1. Электронные системы требуют дорогостоящего оборудования, технических специалистов и дополнительных судей, а это огромные деньги. В итоге на судейство по-новому могут претендовать только толстосумы и самые рейтинговые соревнования.

2. Обращение к электронным средствам пока не происходит в режиме онлайн, а требует дополнительного времени на просмотр повторов. Порой это сильно затягивает соревнования и сбивает их темп.

3. «Челленджи» – апелляции к электронным системам – становятся частью тактики. Иногда они, независимо от результата, способны сбить соперника, оказать давление на судей, дать время собраться и так далее. Тот, кто умеет использовать такие паузы, получает дополнительное преимущество.

4. Наличие электронных систем вовсе не исключает манипуляций. Например, известны случаи, когда в спорных эпизодах объявлялось, что техника дала сбой, и не может разрешить спор. Также камеру теоретически можно обмануть, как и судью-человека.

5. Видеоповторы не являются панацеей от конфликтов. Иногда судьи, находясь в стрессовой ситуации, не могут правильно трактовать какие-то кадры. Кроме того, вызывает вопросы и регламент использования или неиспользования видеоповторов. И тогда система электронного судейства становится бесполезной.

Итак, следует внести в правила соревнований, в которых используются видеоповторы, следующие положения:

1. Перенести судейскую бригаду, отвечающую за видеоповторы в удалённое место, что позволит оставить бригаду без давления главной судейской бригады, для более точного судейства.
2. Нужно ужесточить систему наказаний за предвзятое судейство.
3. Совершенствовать системы видеоповторов опираясь на самые современные технологии. Например, в теннисе сейчас система лучше, чем, например, в футболе, а многие виды спорта вообще остаются без систем видеоповторов. Требуется уравнять все виды спорта в этом отношении.

Раздел 3

Обеспечение информационной безопасности в правовом и образовательном пространстве

Аванесова Р.Р.,
кандидат экономических наук, доцент,
филиал ФГБОУ ВО
«Адыгейский государственный университет»
г. Белореченск

Слюсаренко Э.Е.,
кандидат биологических наук., доцент,
филиал ФГБОУ ВО
«Адыгейский государственный университет»
г. Белореченск

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО И ОРГАНИЗАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одним из важных направлений обеспечения устойчивого развития человечества в обозримом будущем является освоение результатов продолжающейся научно-технической революции, в том числе результатов, полученных в области автоматизации процессов получения, передачи, хранения и распространения информации, формирования глобального информационного пространства. Расширяется применение современных информационных и коммуникационных технологий, компьютерной техники в социально-экономической, политической и духовной сферах жизнедеятельности общества, в выполнении задач государственного управления. Потенциал информационно-коммуникационных технологий активно используется для повышения качества жизни граждан, содействия реализации ими конституционных прав и свобод человека и гражданина, формирования институтов гражданского общества, расширения участия граждан в решении их насущных проблем, повышении эффективности деятельности органов государственной власти и местного самоуправления.

Эти процессы с неизбежностью повышают зависимость человека, организаций, государственных органов и учреждений от устойчивости функционирования информационной инфраструктуры общества, безопасности ее использования для реализации основных прав и свобод, законных интересов граждан, интересов общества и государства.

Устойчивость функционирования и безопасность использования информационной инфраструктуры становятся важным фактором повышения

конкурентоспособности страны, обеспечения ее национальной безопасности. Влияние данного фактора на жизнь общества и государства становится особенно заметно в условиях обострения межгосударственных отношений, разработки методов и способов использования информационно-коммуникационных технологий для оказания «силового» давления на политическое руководство государства и население, для усиления потенциала вооруженных сил зарубежных государств, для нарушения социальной стабильности, вмешательства во внутренние дела других государств.

Проблема обеспечения информационной безопасности является на сегодня одной из самых острых не только у нас в стране, но и в развитых странах мира. Опыт эксплуатации информационных систем и ресурсов в различных сферах жизнедеятельности показывает, что существуют весьма реальные угрозы потери информации, приводящие к материальным и иным ущербам. При этом обеспечить на 100 % безопасность информации практически невозможно.

В связи с этим, в некоторых европейских государствах появилось законодательное закрепление понятия «информационная безопасность». Так в законодательстве Российской Федерации есть конкретное определение данного понятия, а именно: «под информационной безопасностью понимается состояние защищенности её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

Наиболее очевидными источниками информационных опасностей являются:

1) отсутствие единой государственной политики в области обеспечения информационной безопасности;

2) несовершенство нормативной правовой базы, регулирующие отношения в области обеспечения информационной безопасности, а также недостаточная правоприменительная практика;

3) недостаточный контроль за развитием информационного рынка со стороны государственных структур и общества;

4) низкий уровень информатизации государственных и коммерческих структур;

5) низкий уровень защищенности интересов физических и юридических лиц в информационной сфере;

6) сращивание государственных и коммерческих структур в области кредитно-финансовой сферы с криминальными структурами;

7) получение доступа криминальными структурами к конфиденциальной информации;

8) усиление влияния организованной преступности на жизнь общества;

9) контрабандный ввоз и незаконная продажа компьютерной техники и средств радиосвязи, получение неконтролируемой прибыли.

Государственная политика в Российской Федерации по обеспечению информационной безопасности реализуется через правотворчество,

правоприменение и участие государства в развитии правосознания и правовой культуры граждан.

За последние годы наблюдаются значительные сдвиги под влиянием реальных процессов информатизации. Правовой основой здесь является Федеральный закон «Об информации, информационных технологиях и о защите информации», которым наиболее детально урегулированы вопросы правового режима информационных ресурсов. На основе положений названного Закона создана нормативно-правовая база информатизации субъектов Российской Федерации. Информационные ресурсы обрели значительную основу для их организации и развития в региональных, территориальных, отраслевых и межотраслевых системах[1].

Нормативная правовая основа решения проблем информационной безопасности Российской Федерации базируется на соответствующей системе правовых норм, которые регулируют отношения в данной области. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации определены в утвержденной Президентом РФ «Доктрине информационной безопасности Российской Федерации»[2].

В данном документе определены правовые, организационно-технические и экономические методы обеспечения информационной безопасности Российской Федерации, приведены основные положения государственной политики и представлены организационные основы обеспечения информационной безопасности нашей страны. Он также предусматривает разработку последующих нормативных правовых документов, призванных регулировать отношения в сфере информационной безопасности.

Достаточно чувствительной стороной состояния законодательства в области информационной безопасности являются проблемы процессуального значения. Это огромная область науки и практики, так как необходимы новые решения в учете, фиксации, сборе доказательств, в выработке оценки юридических фактов и их слагаемых, в понимании тонкостей работы с информацией в разных областях жизни. Процедуры и правила работы с информацией в системах государственного управления и в деловой практике частного сектора, процессуальные правила правоохранительных органов — особая область законодательства.

Специфика сферы правового регулирования и обеспечения информационной безопасности заключается в том, что здесь возникает необходимость в обеспечении безопасных условий развития сферы информатизации.

---

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. – URL : //http://www.consultant.ru/document/cons_doc_LAW_61798

[2] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – URL : //http://www.consultant.ru/document/cons_doc_LAW_208191

Недоработки в области правового регулирования являются источником угроз в области информационной безопасности.

Собственно, сфера информационной безопасности в значительной мере связана с обеспечением учета, анализа причин возникновения конфликтов и угроз в сфере информатизации. Обеспечение безопасности основывается на профилактике и создании нормального течения этих процессов. Это важно в первую очередь для обеспечения нормотворческой деятельности соответствующих органов государственной власти.

Угрозами же безопасности информационных средств и систем могут являться:

1. Противоправный сбор и использование информации;
2. Разработка и распространение программ, нарушающих нормальное функционирование информационных систем, в том числе систем защиты информации;
3. Утечка информации по техническим каналам (визуально-оптические, акустические, электрические, радиотехнические, материально-вещественные);
4. Внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций, независимо от формы собственности;
5. Уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
6. Перехват информации в сетях передачи данных и на линиях связи;
7. Несанкционированный доступ к информации, находящейся в банках и базах данных (может быть целенаправленный и случайный);
8. Нарушение законных ограничений на распространение информации.

В каждом предметном направлении правового регулирования и формирования нормативно-правовой основы совмещаются задачи создания условий бесконфликтных отношений участников и одновременно условий предотвращения отступлении от нормы, выявления угроз и опасностей по каждому направлению, а также по формированию механизмов реагирования на реализуемые отступления от установленных правил. В законодательстве обозначить границу между актами и нормами, посвященными отдельно общему регулированию отношений и обеспечению безопасности в информационной сфере почти невозможно. Каждый нормативный акт содержит нормы, правила, порядок отношений, соблюдение которых создает состояние безопасности, а нарушение или отступление от них – условия угрозы или реального правонарушения.

Представляется, что каждый правовой акт может быть оценен не только с позиций позитивного установления правил поведения или отношений, но и с позиций его потенциала предотвращения нарушений. Для

достижения целей безопасности чаще применяются запретительные нормы, условия ограничения дозволенного. Известно, что состав правонарушений и санкции помещаются в соответствующие кодексы, нормы которых не всегда гармонизированы с нормами регулятивного характера.

Много проблем связано и с механизмами выявления, фиксации правонарушений, их расследования, с осуществлением экспертиз и судебного разрешения дел. Здесь формируется область ответственности, которую можно рассматривать как наиболее самостоятельную область правового обеспечения безопасности: пресечение нарушения, восстановление нарушенного права, выбор меры наказания и т.д. В связи с этим в области правового обеспечения информационной безопасности первостепенное значение приобретают нормы процессуального права.

Можно отметить, что эффективность законодательства определяется полноценностью его регулятивной части – той части норм, которые создают ясность у участников определенных отношений, как они должны действовать в той или иной ситуации, какими правами и обязанностями они наделены от имени государства или своего контрагента (партнера). В этих целях всякий раз необходимо знать о наличии нормативной основы для тех или иных отношений. Обращение практики к массиву действующего законодательства и подзаконных актов в информационной сфере часто завершается установлением неполноты, несогласованности, а порой и противоречивости нормативно-правовой основы.

Анализ информационного законодательства показывает, что с одной стороны, многие законы, международные соглашения направлены на снятие былых ограничений, поощрение конкуренции, создание условий, способствующих росту информационной индустрии. С другой стороны, эту свободу деятельности и самовыражения необходимо совместить с общественными интересами, что выражается в ограничениях на содержание, передаваемое в глобальных компьютерных сетях, защиту прав на неприкосновенность личной жизни, на интеллектуальную собственность.

В итоге представляется необходимым дальнейшее усовершенствование правовой базы, особое место в системе которой занимает уголовное право, и практики ее применения. При этом в первую очередь необходимо достижение единства норм различных отраслей права, максимальное уменьшение их несбалансированности.

В результате сопоставительного анализа области информационной безопасности информационной сферы с учетом положений Доктрины информационной безопасности и норм информационного законодательства в этой области можно выделить три основных направления правовой защиты объектов в информационной сфере (правового обеспечения информационной безопасности).

1. Первое направление. Защита чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности; нравственных и эстетических идеалов; стабильности и

устойчивости развития общества; информационного суверенитета и целостности государства от угроз воздействия вредной, опасной, недоброкачественной информации, недостоверной, ложной информации, дезинформации, от сокрытия информации об опасности для жизни личности, развития общества и государства, от нарушения порядка распространения информации.

2. Второе направление. Защита информации и информационных ресурсов прежде всего ограниченного доступа (все виды тайн, в том числе и личной тайны), а также информационных систем, информационных технологий, средств связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц.

3. Третье направление. Защита информационных прав и свобод личности (право на производство, распространение, поиск, получение, передачу и использование информации; права на интеллектуальную собственность; права собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии) в информационной сфере в условиях информатизации.

При этом главными направлениями совершенствования законодательства в этой области являются:

1. Разработка проектов федеральных законов, регулирующих отношения в области служебной, коммерческой, банковской и других видов тайн;

2. Усиление борьбы с правонарушениями в информационной сфере путем совершенствования норм, регулирующих ответственность физических и юридических лиц за несанкционированный доступ к информации, ее противоправное копирование, уничтожение, блокирование и модификацию;

3. Разработка нормативных правовых актов, регулирующих отношения в области противодействия техническим разведкам;

4. Совершенствование систем лицензирования и сертификации в различных сферах информационной безопасности;

5. Регулирование вопросов использования импортных аппаратных и программных средств, в том числе средств защиты информации;

6. Дальнейшее развитие законодательства в области государственной тайны и системы ее защиты;

7. Гармонизация стандартов Российской Федерации в области информационной безопасности с международными стандартами.

Последнее направление является особенно важным, поскольку принятие российского стандарта, аналогичного международному стандарту ISO 15408-99 («Общие критерии») позволит России не только выйти на международный уровень оценки безопасности информационных технологий, но и получить возможность создания нового поколения межведомственных нормативно-методических документов по оценке информационной безопасности на единой основе.

Такие межведомственные нормативные документы должны в определенной мере компенсировать имеющийся разрыв, отсутствие необходимой координации между деятельностью правоохранительных органов по

противодействию компьютерной преступности и мероприятиями, проводимыми службами информационной безопасности.

В заключении необходимо сказать, что информационная безопасность России является базовой составляющей национальной безопасности России. Она напрямую влияет на эффективную работу органов государственной власти, является неотъемлемым фактором в борьбе с организованной преступностью и мировым терроризмом. Совершенствование законодательной базы должно стать важным фактором правового и организационного обеспечения информационной безопасности России.

Акимжанов Т.К.,
Заслуженный работник МВД РК,
доктор юридических наук, профессор,
директор НИИ права,
профессор кафедры
юриспруденции и международного права,
Университет «Туран»,
полковник юстиции в отставке
г. Алматы

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – КАК ВИД НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН

В условиях всеобщей цифровизации, мировое сообщество осознало, что самой главной задачей для человечества в третьем тысячелетии является обеспечение информационной безопасности как части национальной безопасности в отдельно взятом государстве и, в целом, на всем мировом пространстве.

Неслучайно, в ст. 4 Закона Республики Казахстан от 06 января 2012 года «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 28 декабря 2018 года) к одному из видов национальной безопасности на ряду с общественной безопасностью, военной безопасностью, политической безопасностью, экономической безопасностью, экологической безопасностью отнесена информационная безопасность – как состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека, гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная безопасность страны[1].

[1] Закон Республики Казахстан «О национальной безопасности Республики Казахстан». Правоохранительные органы. Сборник законодательных актов. – Алматы : ЮРИСТ, 2019. – С. 52.

Роль информационной безопасности трудно переоценить. По мнению ученых, современный период развития можно охарактеризовать как переход от постиндустриального общества к информационному. Его невозможно сегодня представить без интенсивных информационных обменов и развивающихся информационных систем. Информационные потоки постепенно становятся рычагами управления информационными процессами[1].

Более детальную характеристику процессов, происходящих в информационном пространстве, дают ученые-криминологи. По их мнению, современный мир характеризуется стремительным развитием информационных отношений, информационно-телекоммуникационных систем, компьютерных устройств, социальных сетей, появлением новых средств создания, хранения, обработки и распространения электронно-цифровой информации, расширением киберпространства и тотальной компьютеризацией человеческого общества[2].

Чтобы полнее раскрыть содержание информационной безопасности как вида национальной безопасности, рассмотрим понятие самой национальной безопасности – как состояние защищенности национальных интересов Республики Казахстан от реальных и потенциальных угроз, обеспечивающих динамическое развитие человека и гражданина, общества и государства[3].

Первый Президент Казахстана Н.А. Назарбаев в своей книге «Критическое десятилетие», говоря о проблемах безопасности, отметил, что национальная безопасность призвана обеспечить гарантии неуязвимости основных, жизненно важных интересов страны – национального суверенитета, территориальной целостности, защиты населения. В этом смысле, национальная безопасность выступает как система жизнеобеспечения государства: нет национальной безопасности – нет государства[4].

Казахстан, являясь частью мирового сообщества, вносит большой вклад в решение данного вопроса. Развитие казахстанского общества на современном этапе тесно связано с возрастанием количества условий и обстоятельств, угрожающих жизни и здоровью людей, интересам общества и государства и достигло такого уровня существования, когда обеспечение безопасности, самосохранения, выживания, как отдельного человека, так и мирового сообщества в целом превращается в проблему, необходимость решения которой не оставляет сомнений.

---

1 Информационное право : учебник для бакалавров / Отв. ред. И.М. Рассолов. – М. : Проспект, 2016. – С. 13.

2 Теоретические основы предупреждения преступности на современном этапе развития российского общества : монография / П.В. Агапов, Г.В. Антонов-Романовский, В.К. Артеменков [и др.]; Под общ. Ред. Р.В. Журбина; Академия Генеральной прокуратуры Российской Федерации. – М. : Проспект, 2018. – С. 383.

3 Закон Республики Казахстан «О национальной безопасности Республики Казахстан». Правоохранительные органы. Сборник законодательных актов. – Алматы : ЮРИСТ, 2019. – С. 50.

4 Назарбаев Н.А. Критическое десятилетие. – Алматы : Атамура, 2003. – С. 202.

Заслуживает внимания описанная известным ученым криминологом В.Н. Кудрявцевым в своей книге «Стратегия борьбы с преступностью» – стратегия безопасности. Цитируемый автор предлагает меры безопасности определять, как предпринимаемые в целях защиты людей, промышленных, военных, научных и иных объектов от преступных посягательств неустановленных (неопределенных) лиц.

При этом центр тяжести перемещается с превентивной, и поэтому незаконной, репрессии в отношении «подозреваемых» или «неблагонадежных» элементов на осуществление мер по охране и защите государственных и общественных объектов, а также граждан, от возможных преступных посягательств. По сути, речь идет об устранении условий, способствующих совершению преступлений[1].

В свою очередь будет интересным исследование общей дефиниции безопасности, в структуру которого входит и само понятие национальной безопасности.

Как известно, понятие безопасности с позиции различных наук, как правило, трактуется неоднозначно. Психология безопасность представляет как ощущение, восприятие и переживание необходимости в защите жизненных (духовных и материальных) потребностей и интересов людей. Философия и социология рассматривают безопасность как состояние, тенденции развития и условия жизнедеятельности общества, его структур, институтов и порядков, при которых обеспечивается сохранение оптимального соотношения различных категорий и противоположностей. С позиций юридических наук безопасность рассматривается как система установления правовых гарантий защищенности личности и общества, обеспечения их нормальной жизнедеятельности, прав и свобод.

Например, по мнению С.В. Степашина безопасность есть состояние, тенденции развития (в том числе латентные) и условия жизнедеятельности социума, его структур, институтов и установлений, при которых обеспечивается сохранение их качественной определенности с объективно обусловленными инновациями в ней и свободное, соответствующее собственной природе и ею, определяемой функционирование[2].

Н.Д. Казаков определяет безопасность как «динамически устойчивое состояние по отношению к неблагоприятным воздействиям и деятельность по защите от внутренних и внешних угроз, по обеспечению таких внутренних и внешних условий существования государства, которые гарантируют возможность стабильного всестороннего прогресса общества и его граждан»[3].

---

[1] Кудрявцев В.Н. Стратегия борьбы с преступностью. – М. : Юрист, 2003.

[2] Степашин С.В. Безопасность человека и общества (политико-правовые вопросы) : монография. – СПб. : СПб. ЮИ МВД России, 1994.

[3] Казаков Н.Д. Безопасность и синергетика (опыт философского осмысления) / Н.Д. Казаков // Безопасность. Информационный сборник Фонда национальной и международной безопасности. – 1994. – № 4. – С. 62.

М.А. Лесков безопасность рассматривает как явление, тождественное гомеостазису системы, «под которым принято понимать тип динамического равновесия, характерный для сложных саморегулирующихся систем и состояний в поддержании существенно важных для сохранения системы параметров в допустимых пределах»[1].

В.И. Митрохин, считает, что безопасность есть мера защищенности среды жизнебытия, чести, достоинства, ценностей личности, социальных групп, государства, общества, цивилизации в целом[2].

Обобщая приведенные выше дефиниции безопасности, можно сделать обобщенный вывод, что безопасность есть результат социальной деятельности по обеспечению безопасности личности, общества, государства.

В качестве предмета деятельности выступают конкретные угрозы опасности (информационные, экологические, военные, политические, экономические и пр.), а также отдельные материальные носители этих угроз (природные и социально-общественные явления и т.д.).

По мнению российских ученых С.В. Степашина и В.С. Комисарова, угрозы могут классифицироваться по различным основаниям[3].

В ст. 6 Закона Республики Казахстан «О национальной безопасности Республики Казахстан» закреплен перечень основных угроз национальной безопасности, среди которых применительно к рассматриваемой нами проблеме информационной безопасности относятся: п. 16) снижение уровня защищенности информационного пространства страны, а также национальных информационных ресурсов от несанкционированного доступа, а также п. 17) информационное воздействие на общественное и индивидуальное сознание, связанное с преднамеренным искажением и распространением недостоверной информации в ущерб национальной безопасности[4].

Как нам представляется, информационная безопасность должна охватывать следующие основные направления деятельности.

Первое. Это всеобщая цифровизация. Создание информационной базы о всех направлениях развития современного общества. Только наличие желаемого информационного пространства того или иного государства, может обеспечить его поступательное и развитие, и безопасность.

Второе. Это обеспечение доступа граждан к любой интересующей их информации открытого характера. В ч. 3 ст. 18 Конституции Республики Казахстан закреплена норма, что государственные органы, общественные

---

[1] Лесков М.А. Гомеостатические процессы и теория безопасности / М.А. Лесков // Безопасность. Информационный сборник. – 1994. – № 4(20).

[2] Митрохин В.И. Концептуальные основы стратегии национальной безопасности России / В.И. Митрохин // Социально-политический журнал. – 1995. – № 6.

[3] См., напр.: Степашин С.В. Безопасность человека и общества (политико-правовые вопросы). – СПб. : СПб ЮИ МВД России, 1994. – С. 19.; Комиссаров В.С. Преступления, нарушающие общие правила безопасности (понятия, система, общая характеристика) : автореф. дис. … д-ра юрид. наук. – М. : МГУ, 1997.

[4] Закон Республики Казахстан «О национальной безопасности Республики Казахстан». Правоохранительные органы. Сборник законодательных актов. – Алматы : ЮРИСТ, 2019.

объединения, должностные лица и средства массовой информации обязаны обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации[1].

Третье. Обеспечение безопасности всех источников информации, в том числе и отдельных граждан, имеющейся в Республике Казахстан, то есть информационной базы. Когда обеспечена полная информационная безопасность в обществе, можно говорить о состоянии защищенности данного общества и его граждан.

Следует отметить, что информатизация, кроме позитивного имеет и негативные свойства. Так, по мнению ученых, информационные технологии – это своеобразный «ящик Пандоры», который несет обществу не только блага, но и различные трудности, проблемы, испытания. Расплатой за «технологические блага» стали изменения в социальной культуре людей: информационная сеть Интернет заменила большинству театры, филармонии, консерватории, библиотеки, музеи, книги; общение в социальных сетях – «Живое» общение со знакомыми, друзьями, родственниками и другими людьми, люди становятся психологически интернет-зависимыми[2].

Кроме этого, негативные свойства цифровизации связаны напрямую с преступной деятельностью, то есть с криминальным миром.

Об этом описано в работе известного российского ученого криминолога В.С. Овчинского «Криминология цифрового мира»[3], по мнению которого стратегия информационного общества понимает само это общество в широком смысле – как общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан[4]. В.С. Овчинский достаточно точно изложил и аргументировал всю процедуру и механизм цифровизации криминального мира в современных условиях всеобщей цифровизации.

В современной научной литературе и публицистике, в официальных документах и нормативных актах, посвященных противостоянию преступности, используются разнообразный понятийный аппарат и терминология. Они заимствованы из различных областей научных знаний и призваны по возможности наиболее емко выражать сущность данной деятельности. Это и уголовная политика, и борьба (война) с преступностью (с ее концепциями и стратегиями), и контроль над преступностью, реагирование, воздействие на нее, противодействие преступности и т.п. Однако, с позиции угроз

---

[1] Конституция Республики Казахстан : практ. пособие. – Алматы : ТОО «Издательство «Норма-К», 2019.

[2] Теоретические основы предупреждения преступности на современном этапе развития российского общества : монография / П.В. Агапов, Г.В. Антонов-Романовский, В.К. Артеменков [и др.]; Под общ. Ред. Р.В. Журбина; Академия Генеральной прокуратуры Российской Федерации. – М. : Проспект, 2018.

[3] Овчинский В.С. Криминология цифрового мира : учебник для магистратуры. – М. : Норма : ИНФРА М, 2018.

[4] Овчинский В.С. Криминология цифрового мира : учебник для магистратуры. – М. : Норма : ИНФРА М, 2018.

национальной безопасности, в том числе и информационной безопасности, преступность самостоятельно не рассматривалась.

Разграничение различных терминов и понятий, обозначающих определенный вид деятельности, имеет не только теоретическое, но и прикладное значение, в особенности для нормотворчества, для организации работы по противостоянию преступности, разграничению компетенции субъектов, осуществляющих эту задачу, по устранению их смешения и дублирования их функций.

Поэтому казахстанский законодатель при разработке нового УК РК 2014 года предусмотрел новую главу 7 «Уголовные правонарушения в сфере информатизации и связи» УК РК, в которую включил наиболее опасные виды посягательств на эти отношения:

а) неправомерный доступ к информации, в информационную систему или сеть телекоммуникации (ст. 205 УК РК);

б) неправомерное уничтожение или модификация информации (ст. 206 УК РК);

в) нарушение работы информационной системы или сетей телекоммуникации (ст. 207 УК РК);

г) неправомерное завладение информацией (ст. 208 УК РК);

д) принуждение к передаче информации (ст. 209 УК РК);

е) создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК РК);

ж) неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211 УК РК);

з) предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК РК);

и) неправомерные изменения идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213 УК РК).

По мнению казахстанских и российских ученых, все уголовные правонарушения, входящие в Главу 7 УК РК, можно классифицировать на группы:

а) уголовные правонарушения, посягающие на конфиденциальность, целостность и доступность охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникативной сети (ст. 205–211 УК РК);

б) иные виды уголовных правонарушений в сфере информатизации и связи (ст. 212 и 213 УК РК)[1].

И так, подводя итог рассмотрению понятия информационной безопасности как одного из видонациональной безопасности можно сделать следующие выводы.

---

[1] Уголовное право Республики Казахстан: Особенная часть : в 2-т. : учебник для вузов. Отв. ред. И.И. Рогов, К.Ж. Балтабаев, А.И. Коробеев. – Алматы : Жеті Жарғы, 2016.

Первое. В связи с всеобщей информатизацией всех жизненно важных и жизненно обеспечивающих процессов, как нам представляется, информационной безопасности по праву принадлежит в настоящее время ведущее место, среди других видов национальной безопасности.

Второе. Обеспечение информационной безопасности направлено на охрану конституционных прав граждан, общественных организаций, государственных органов и, в целом, всего государства.

Третье. В связи с активной цифровизацией криминального мира, информационная безопасность должна охватить деятельность всех правоохранительных и специальных органов Республики Казахстан, призванных обеспечивать правопорядок и общественную безопасность в Республике Казахстан.

С учетом вышеперечисленных обстоятельств можно констатировать, что обеспечение информационной безопасности в стране – есть мера по укреплению правопорядка, общественной безопасности, стабильности в обществе, а также обеспечению прав и законных интересов граждан страны.

Такая стратегия исходит из определенной политической идеологии и предполагает наличие общей концепции, определение не только ближайших, но и отдаленных целей и способов их достижения, разнообразных мер различных субъектов антикриминального воздействия, пригодных для применения в различных, изменяющихся условиях.

При этом дальнейшее развитие информационной безопасности в Республике Казахстан должна предполагать планирование и осуществление научно обоснованной системы антикриминальных мероприятий на всех уровнях социальной организации и найти свое достойное место в новой Концепции правовой политики Республики Казахстан на период с 2021 по 2030 годы, разработка которой ведется в настоящее время.

Бочкарева Е.А.,
доктор юридических наук, доцент,
заведующий кафедрой административного
и финансового права,
СКФ ФГБОУВО «РГУП»
г. Краснодар

Кривцов А.С.,
судья Краснодарского краевого Суда,
преподаватель кафедры административного
и финансового права,
СКФ ФГБОУВО «РГУП»
г. Краснодар

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА: ПРАВОВЫЕ АСПЕКТЫ

В условиях повышения рисков национальной безопасности не первый год в повестке дня науки финансового права – правовые аспекты

обеспечения финансовой устойчивости государства и его финансовой безопасности, теоретические вопросы разработки финансово-правовых механизмов противодействия геополитическим вызовам, системные исследования финансового суверенитета государства.

Последний, по мнению Н.В. Омелехиной, представляет собой часть экономического суверенитета и проявляется во вне как независимость государства во взаимоотношениях с другими государствами в части реализации своей фискальной компетенции и материального обеспечения международных обязательств. В самом государстве финансовый суверенитет предполагает «…право государства устанавливать и взимать денежные платежи с населения в пределах своей территории, получать иные доходы, аккумулировать их в определенных фондах и перераспределять для материального обеспечения задач и функций государства, выраженных в предметах ведения соответствующего публично-правового образования и закрепленных в составе полномочий его органов»[1].

В условиях инновационного развития современного государства переход от архаичных систем управления к аналитическим информационным системам в сфере финансовой деятельности сопровождается глобализацией процессов получения и обработки финансово-значимой информации. Возникающая потребность в рассмотрении динамики развития важнейших институтов финансового права в условиях формирования цифровой экономики обеспечивается научными разработками, предметом которых является чрезвычайно широкий круг проблем.

Необходимость разработки финансово-правовых механизмов, позволяющих противодействовать финансовым рискам в условиях экономической турбулентности, обусловливает потребность их исследования в качестве правовой категории[2]. В течение всего современного периода развития науки финансового права широко обсуждаются вопросы совершенствования правовых средств оптимизации публичных расходов и их перераспределения, финансово-правовые механизмы обеспечения делегированных полномочий. В качестве примера достаточно сослаться на работы Е.М. Андреевой, в которых не только поднимаются все перечисленные проблемы, но и обосновывается комплекс мер по их минимизации[3].

Исследователи работают над формированием и совершенствованием понятийно-категориальный аппарат в области цифровой экономики,

---

[1] Омелехина Н.В. Финансовый суверенитет государства: к постановке проблемы исследования правовой идентификации / Н.В. Омелехина // Финансовое право. – 2017. – № 4. – С. 21.

[2] Омелёхина Н.В Финансовые риски в бюджетной сфере: доктринальное понимание сущности и видового разнообразия / Н.В. Омелехина // Журнал российского права. – 2018. – № 8. – С. 77–88.

[3] Андреева Е.М. К вопросу о порядке оценки потребностей в финансовых ресурсах на исполнение переданных полномочий субъектов публичной власти / Е.М. Андреева // Современное общество и право. – 2019. – № 1(38). – С. 53–60.

гармонизацией подходов к ее нормативному правовому регулированию, в том числе с учетом опыта зарубежных стран.

Ученые предпринимают попытки научного осмысления таких явлений, как цифровая экономика, цифровые финансовые рынки, электронный бюджет, электронные денежные средства, криптовалюта, блокчейн, аудиторская тайна, налоговая тайна; исследуют правовые режимы конфиденциальность информации при «амнистии капиталов», международный обмен налоговой информацией, информационные системы и технологии в финансовом (бюджетном) контроле, правовой режим государственной информационной системы в бюджетных отношениях, внедрение в бюджетные отношения информационно-телекоммуникационных технологий; оценивают цифровизацию налогового контроля и цифровые технологии в финансово-банковской сфере; анализируют эффективность правовой защиты информации в национальной платежной системе.

Большинство из перечисленных явлений находится в объективе научного интереса гражданского, корпоративного, информационного, а также уголовного права. Однако несомненную ценность имеют и финансово-правовые исследования, которые могут быть востребованы в других отраслевых юридических науках. Отметим работы И.И. Кучерова, посвященные анализу криптовалюты как правовой категории. Автор приходит к выводу о том, что «…криптовалюта является разновидностью электронных денег, которая представляет собой обусловленную использованием технологии распределенного реестра специфическую электронную форму частных денежных средств»[1].

Во взаимосвязи с вопросами обеспечения финансовой безопасности исследует криптовалюту Е.Г. Костикова, которая выделяет две группы рисков: риски публичного и риски частного характера, и полагает важным «…рассмотреть и оценить возможность и механизмы дозволительного правового регулирования эмиссии и обращения кибервалюты»[2].

Продуктивным является рассмотрение криптовалюты в сравнительном аспекте, как объекта финансово-правового и гражданско-правового регулирования[3]; также активно исследуются вопросы налогообложения и налогового контроля ее оборота[4].

---

[1] Кучеров И.И. Криптовалюта как правовая категория / И.И. Кучеров // Финансовое право. – 2018. – № 5. – С. 8.

[2] Костикова Е.Г. Кибервалюта: вопросы правового обеспечения финансовой безопасности / Е.Г. Костикова; Под ред. И.А. Цинделиани // Избранные труды кафедры финансового права Российского государственного университета правосудия. Сборник статей. – М. : Проспект, 2018. – С. 150–159.

[3] Затулина Т.Н. Институт «криптовалюта» как объект финансового и гражданского правового регулирования в Российской Федерации: постановка проблемы правореализации / Т.Н. Затулина, В.В. Низовцев, О.А. Подобина // Финансовое право. – 2019. – № 6. – С. 9–12.

[4] Ступаченко Е.В. Проблемы правового регулирования налогообложения и налогового контроля оборота криптовалют / Е.В. Ступаченко // Право и цифровая экономика. – 2019. – № 4. – С. 10–13.

Анализируя влияние цифровых технологий на финансовое право, А.А. Ситник обоснованно отмечает: «…в условиях цифровизации экономики новые технологии, с одной стороны, ведут к расширению предмета правового регулирования, а с другой – являются инструментом, способствующим регулированию, администрированию, финансовому контролю и надзору»[1].

Представляется, что правы авторы, по мнению которых «В складывающихся условиях всеобъемлющей цифровизации важно понимать, что правильно организованные финансово-правовые отношения в цифровую эпоху может предоставить большие возможности для увеличения благосостояния людей, лишь находясь в надежном правовом поле»[2].

Финансовая безопасность, как представляется, охватывает совокупность несколько взаимосвязанных сфер, содержательно совпадающих с элементами финансовой системы, и включает в себя: бюджетную, налоговую, банковскую, валютную, и т.д. безопасность. При этом каждая из перечисленных сфер чрезвычайно насыщенна с информационной точки зрения. И не только насыщенна, но и чрезвычайно уязвима. В частности, защита информационной безопасности в финансовой сфере правовыми средствами предполагает поиск баланса интересов кредитных организаций, их клиентов, налоговых и иных органов государственной власти, других лиц, претендующих, в силу различных обстоятельств, на доступ к тем или иным конфиденциальным сведениям.

Сказанное подтверждается разнообразной судебной практикой.

Так, например, с отказом налоговых органов предоставить информацию о счетах и транзакциях обанкротившихся клиентов сталкиваются арбитражные, а равно – финансовые управляющие, приступившие к выполнению своих обязанностей. При этом суды занимают противоположные позиции по вопросу о праве указанных лиц на доступ к сведениям, с одной стороны, необходимым управляющим для выполнения своей миссии, а с другой – защищенных грифом «тайны».

В частности, Арбитражный суд Волго-Вятского округа оставил без изменения решения нижестоящих судов, признавших неправомерным отказ налогового органа в предоставлении финансовому управляющему копий налоговых деклараций должников, сведений о видах и суммах налогов, уплаченных, а также подлежащих уплате, о проверках и их результатах, и др. В своем решении суд подчеркнул, что данные сведения, составляющие налоговую тайну, необходимы «для принятия финансовым управляющим решения об обжаловании сделок должника по выбытию имущества

---

[1] Ситник А.А. Финансовые технологии: понятие и виды / А.А. Ситник // Актуальные проблемы российского права. – 2019. – № 6. – С. 27–31; – С. 27. – URL : https://doi.org/10.17803/1994-1471.2019.103.6.027-031

[2] Боташева Л.Э. Трансформация финансово-правовых отношений в условиях цифровой экономики / Л.Э. Боташева, Д.А. Смирнов // Гуманитарные и юридические исследования. – 2019. – № 2. – С. 182.

(имущественных прав) с целью поступления денежных средств в конкурсную массу должника и удовлетворения требований кредиторов, а также для проверки наличия признаков преднамеренного и фиктивного банкротства»[1].

Арбитражный суд Московского округа, рассматривая в чем-то похожий спор, но с участием пенсионного фонда и по поводу персональной информации застрахованных лиц – субъектов банкротного дела, пришел к аналогичному выводу о том, что «арбитражному управляющему предоставлено право запрашивать необходимые сведения, в том числе составляющие служебную, коммерческую и банковскую тайну; запрошенные конкурсным управляющим у пенсионного фонда документы являются информацией, при отсутствии которой невозможно надлежащим образом исполнить обязанности конкурсного управляющего, предусмотренные действующим законодательством, и предпринять все необходимые меры в рамках процедуры банкротства должника»[2].

Однако Арбитражный суд Восточно-Сибирского округа посчитал правильными выводы судов об обоснованности отказа налоговой инспекции в предоставлении конкурсному управляющему сведений о доходах должника и удержанных суммах налогов, согласившись с тем, что «Перечень информации, которую финансовый управляющий имеет право получать …определен в статьях 20.3 и 213.9 Закона о банкротстве и является исчерпывающим. При этом указание на возможность финансового управляющего истребовать сведения, составляющие налоговую тайну, в законе отсутствует»[3].

Получается, что предоставлять сведения о себе должен сам должник, а финансовый управляющий может обратиться к нему с таким требованием. И вот только если должник отказывается «поделиться» необходимой информацией с финансовым управляющим, у последнего появляется право подать в арбитражный суд ходатайство об истребовании доказательств. Иными словами, обращаться в налоговую инспекцию за сведениями о должнике, составляющими налоговую тайну, управляющий просто не имеет права.

Равным образом, с позиции буквального толкования законодательных положений, был разрешен спор о штрафе банка за отказ от предоставления Управлению Федеральной антимонопольной службы информации о наличии банковских транзакций по счетам клиента. Арбитражный суд Северо-Западного округа оставил без изменения решения судов и отказал в жалобе антимонопольному органу, указав на то, что действующее законодательство не содержит положений, обязывающих банк представлять в антимонопольный орган по его мотивированному требованию документы и сведения,

---

[1] Постановление Арбитражного суда Волго-Вятского округа от 05.03.2020 № Ф01-8762/2020 по делу № А82-8719/2019 // СПС «КонсультантПлюс».

[2] Постановление Арбитражного суда Московского округа от 19.12.2019 № Ф05-19318/2019 по делу № А40-5993/2019 // СПС «КонсультантПлюс».

[3] Постановление Арбитражного суда Восточно-Сибирского округа от 07.11.2019 № Ф02-5314/2019 по делу № А19-7444/2019 // СПС «КонсультантПлюс».

составляющие банковскую тайну, и «суды первой и апелляционной инстанций пришли к правомерному выводу об отсутствии у Банка обязанности исполнять направленный запрос антимонопольного органа, вследствие чего указали на отсутствие в его действиях состава административного правонарушения, предусмотренного частью 5 статьи 19.8 КоАП РФ»[1].

На наш взгляд, приведенные примеры судебной практики свидетельствуют о необходимости конкретизации действующего законодательства в части положений, устанавливающих объем сведений, составляющих финансовую тайну, и круга субъектов, имущих право на доступ к таким сведениям.

Соответственно, мы можем предположить, что в научном осмыслении нуждается особая инфраструктурная область финансовой деятельности – правовые режимы конфиденциальной информации[2].

Полагаем, что главная цель обеспечения экономической безопасности в целом, и финансовой – в частности, состоит в создании подкрепленного правовыми гарантиями эффективного, постоянно действующего механизма противодействия внешним угрозам, способного «здесь и сейчас» обеспечить финансовой системе государства максимальный набор функций, отвечающий потребностям и запросам общественного развития.

Совершенствуя правовые механизмы финансовой безопасности, необходимо находить слабые места и потенциальные угрозы, анализировать ситуацию не только в своей стране, но и за ее пределами, что подразумевает трансформацию национального мониторинга и создание препятствий от действий нерезидентов и спекулятивного иностранного капитала[3].

Итак, в современных условиях всеобщей цифровизации обеспечение экономической безопасности особенно актуально в аспекте достижения финансовой устойчивости государства и его территорий, сбалансированности бюджетной системы, соблюдения прав и законных интересов участников финансовых отношений.

В связи с глобализацией экономического пространства возникает большое количество различных угроз финансовой самодостаточности публично-территориальных образований. Сегодня и перед учеными, и перед практиками стоит важнейшая задача – найти механизмы обеспечения безопасности финансовой деятельности, предложить пути совершенствования законодательства и способы использования существующей правовой базы в интересах защиты личности, общества, государства.

---

[1] Постановление Арбитражного суда Северо-Западного округа от 12.03.2020 № Ф07-1619/2020 по делу № А56-74329/2019 // СПС «КонсультантПлюс».

[2] Бегларов Н.А. Информационные технологии и финансовая тайна / Н.А. Бегларов, Х.В. Мамакаев // Судебные ведомости. – 2019. – № 1–2 (71–72). – С. 12–14.

[3] Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». – URL : http://base.garant.ru/71296054/#ixzz6juxcZv3u (дата обращения 14.11.2020).

Жанузакова Л.Т.,
доктор юридических наук, профессор,
заместитель директора НИИ права,
Университет «Туран»,
главный научный сотрудник,
отдел конституционного,
административного права
и государственного управления,
Институт законодательства
и правовой информации
г. Алматы

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Становление системы обеспечения информационной безопасности личности пришлось на середину XX века, с принятием ООН целого ряда международных документов в области прав человека.

Само понятие «информационная безопасность личности» можно рассматривать как состояние защищенности человека, его прав и свобод от реальных и потенциальных угроз в сфере информационного пространства. Правовые основы информационной безопасности личности закреплены законодательством Республики: Конституцией, законами «О доступе к информации», «О средствах массовой информации», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О государственных услугах», Административным процедурно-процессуальном кодексом. Ст. 18 Конституция закрепляет право каждого на неприкосновенность частной жизни, личную и семейную тайну, тайну личных вкладов, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; обязанность государственных органов, общественных объединений, должностных лиц и средства массовой информации обеспечить каждому гражданину возможность ознакомиться с затрагивающими его права и интересы документами, решениями и источниками информации. Ст. 20 устанавливает право свободно получать и распространять информацию любым, не запрещенным законом способом[1].

Кроме того, право на получение информации, сохранности конфиденциальной информации о человеке в отдельных сферах жизни или отдельных категорий лиц регулируется отраслевыми законами: кодексами «О здоровье

[1] Конституция Республики Казахстан. Принята 30 августа 1995 г. на республиканском референдуме. С изменениями и дополнениями, внесенными законами РК от 07 октября 1998 г., от 21 мая 2007 г., от 02 февраля 2011 г., от 10 марта 2017 г., от 23 марта 2019 г. // Ведомости Парламента РК. 1996. № 4. Ст. 217; 1998. № 20. Ст. 245; 2007. № 10. Ст. 68; 2011. № 3. Ст. 29; 2017. № 5. Ст. 9; 2019. № 5–6. Ст. 28.

народа и системе здравоохранения» и «О браке (супружестве) и семье», Законом «О защите детей от информации, причиняющей вред их здоровью и развитию» и иными нормативными правовыми актами.

Содержание информационной безопасности личности охватывает достаточно широкий спектр прав и гарантий. Одним из них является право на защиту персональных данных.

В последнее время участились случаи сбора, обработки и распространения персональных данных без разрешения на то их обладателей. Практически каждый сталкивался с тем, что получал рекламу на сотовый телефон или звонок от компании с предложениями о товарах или услугах. При этом свой номер телефона данной компании мы не оставляли, либо оставляли, но совсем не для получения рекламы. Это один из типичных примеров неправомерного использования персональных данных.

Ранее регулирование правоотношений в сфере сбора и обработки персональных данных было хаотичным, отсутствовало определение основных терминов, одно и то же понятие могло иметь разное значение в различных нормативных актах. Это усложняло применение законодательства. Сейчас понятие «персональные данные» единое для всех отраслей права. Персональными данными являются любые сведения о человеке, на основе которых можно определить конкретного субъекта персональных данных, зафиксированные на любом носителе.

Закон РК от 21 мая 2013 г. «О персональных данных и их защите» устанавливает механизмы, препятствующие неправомерному использованию персональной информации, регламентирует процедуры сбора, обработки, хранения персональных данных с разрешения граждан.

Согласно этому нормативному правовому акту, персональные данные – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

Разновидностью персональных данных являются биометрические данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность[1].

Исчерпывающего перечня персональных данных в Законе нет. Однако несколькими подзаконными нормативными правовыми актами во главе с постановлением Правительства РК от 12 ноября 2013 г. № 1214 «Об утверждении Правил определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач», был в свое время установлен базовый перечень персональных данных[2]. Поскольку их количество достаточно большое, указанное постановление содержит ссылку на специальные перечни, где с ними можно ознакомиться.

---

[1] Ведомости Парламента РК. 2013. № 7. Ст. 35.

[2] Собрание актов Президента и Правительства РК. 2013. № 65. Ст. 884.

Итак, персональными данными человека считаются: фамилия, имя и отчество, пол, дата и место рождения, гражданство, национальность, индивидуальный идентификационный номер, семейное положение, имущественное состояние, адресные сведения о месте жительства, данные документа, удостоверяющего личность; контактные телефоны; электронный адрес; подпись; портретное изображение (фотография) и другая информация, идентифицирующая конкретного человека либо относящаяся к нему.

В специальных нормативных правовых актах могут устанавливаться дополнительные сведения, относящиеся к персональным данным. Например, о наличии или отсутствии судимости, признании потерпевшим; сведения о заработной плате; сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса); сведения об имуществе и т.д.[1]

Персональные данные делятся на общедоступные и с ограниченным доступом. Общедоступные персональные данные – персональные данные, доступ к которым является свободным с согласия субъекта или на которые в соответствии с законодательством РК не распространяются требования соблюдения конфиденциальности[2]. Однако Закон приводит лишь примеры источников общедоступных данных, но не перечисляет такие данные.

К источникам общедоступных данных отнесены библиографические справочники, телефонные и адресные книги, общедоступные электронные информационные ресурсы, средства массовой информации[3]. Можно полагать, что к общедоступным данным относятся, в частности, имя, фамилия, адрес, номер стационарного телефона. При этом нужно отметить, что объем информации, который предоставляют справочники и адресные книги, может разниться. Сами субъекты персональных данных могут быть против включения той или иной информации в адресные книги и справочники.

В этой связи целесообразно именно на уровне закона закрепить перечень общедоступных персональных данных.

Персональные данные ограниченного доступа – персональные данные, доступ к которым ограничен законодательством.

Разрешение на сбор и обработку персональных данных может дать только сам владелец этих данных – собственник. Это касается и отзыва такого согласия. Закон не предоставляет возможность третьим лицам осуществлять эти действия по доверенности. Такое право дается только законному представителю – то есть лицу, которое представляет интересы субъекта перед государственными органами, организациями, гражданами в силу

---

[1] Приказ Министра внутренних дел РК от 12 августа 2013 г. № 493 «Об утверждении перечня персональных данных, необходимого и достаточного для выполнения осуществляемых задач» //Информационно-правовая система нормативных правовых актов РК «Әділет». – URL : adilet.zan/kz

[2] Ведомости Парламента РК. 2013. № 7. Ст. 35.

[3] Ведомости Парламента РК. 2013. № 7. Ст. 35.

того, что опекаемый не может самостоятельно осуществлять свои права и выполнять обязанности по причине малолетства или физического состояния. Работодателям и государственным органам следует учитывать эту особенность закона при сборе персональных данных.

Субъект, осуществляющий сбор, обработку и защиту персональных данных, – это оператор. Так вот, эти две категории субъектов могут накапливать, хранить, изменять, дополнять, использовать, распространять, обезличивать, блокировать и уничтожать персональные данные, а также передавать их третьим лицам.

Сбор, обработка и защита персональных данных осуществляются в соответствии с принципами соблюдения конституционных прав и свобод человека и гражданина; законности; конфиденциальности персональных данных ограниченного доступа; равенства прав субъектов, собственников и операторов; обеспечения безопасности личности, общества и государства. Так, принцип конфиденциальности выражается в том, что собственники и (или) операторы, а также третьи лица, получающие доступ к персональным данным ограниченного доступа, обеспечивают их конфиденциальность путем соблюдения требований не допускать их распространения без согласия субъекта или его законного представителя либо наличия иного законного основания. Лица, которым стали известны персональные данные ограниченного доступа в связи с профессиональной, служебной необходимостью, а также трудовыми отношениями, обязаны обеспечивать их конфиденциальность[1]. Утверждается, что оператор должен собирать только то количество информации, которое необходимо для выполнения его деятельности. Важно с точки зрения безопасности, что физически базы с такими данными должны находиться на территории Казахстана.

Как справедливо отмечает А. Жатканбаева, поводом для обсуждения является «целесообразность создания всевозможных банков персональных данных, полнота их наполнения, а также порядок и процедура отнесения этих сведений к защищаемым, особо защищаемым либо общедоступным». «Основным правилом для оператора по сбору и управлению персональными данными, – по ее мнению, – должно стать четкое понимание целесообразности и ответственности при организации своей деятельности»[2].

Вместе с тем, можно отметить, что, несмотря на общее правило по использованию и распространению персональных данных с согласия собственника, в некоторых случаях наличие такого согласия не требуется. Например, на публикацию фотографии лица, занимающего государственную должность. Недавно во Франции предпринималась попытка принятия закона, запрещающего публиковать фото и видеоизображения полицейских при выполнении их служебных обязанностей, например, при разгоне

---

[1] Ведомости Парламента РК. 2013. № 7. Ст. 35.

[2] Жатканбаева А. Е. Конституционно-правовые аспекты информационной безопасности в Республике Казахстан. – Алматы, 2009. – С. 196.

митинга, демонстрации с применением силы. Демократическая общественность страны подвергла резкой критике это положение закона, как посягательство на свободу слова и прессы. В Казахстане журналистские расследования о коррупционных схемах чиновников (например, приводятся сведения о счетах и недвижимости членов семьи) зачастую приводят к судебным разбирательствам за посягательство на честь и достоинство этих чиновников и преследованию журналистов.

Персональные данные подлежат уничтожению собственником и (или) оператором, а также третьим лицом: по истечении срока хранения; при прекращении правоотношений между субъектом, собственником и (или) оператором, третьим лицом; при вступлении в законную силу решения суда; в иных случаях, установленных законодательством РК[1].

Важный момент связан с условиями удаления персональных данных. Пока в Казахстане не реализовано так называемое «право на забвение». В 2014 году Европейский суд постановил, что поисковые системы, в том числе Google, должны рассмотреть возможность удаления из поисковых результатов информации, которая будет признана судом «неадекватной, устаревшей или чрезмерной». Этот вопрос поднимался в Мажилисе Парламента Казахстана, однако общественные организации и СМИ подвергли это предложение критике, в связи с тем, что правом удалить о себе информацию будут пользоваться чиновники, а сама мера будет новым шагом по усилению цензуры в Казахстане[2].

Защита персональных данных осуществляется путем применения комплекса правовых, организационных и технических мер. Собственник, оператор, третье лицо обязаны принимать меры по защите персональных данных, обеспечивающие: предотвращение несанкционированного доступа к персональным данным; своевременное обнаружение фактов несанкционированного доступа, если такой несанкционированный доступ не удалось предотвратить; минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным.

Особенности защиты электронных информационных ресурсов, содержащих персональные данные, устанавливаются в соответствии с Законом РК «Об информатизации».

Нарушение законодательство о персональных данных влечет за собой гражданскую, административную и уголовную ответственность.

К сожалению, несмотря на принятые законодательные меры по защите персональных данных, все еще остро стоит проблема их охраны в киберпространстве. Сегодня граждане совершают покупки, оплачивают коммунальные расходы, налоги и штрафы через интернет. Через web-портал «электронного правительства» можно получить государственные услуги. И

---

[1] Ведомости Парламента РК. 2013. № 7. Ст. 35.

[2] Д. Сабитов. Информационная безопасность Казахстана: защита данных и смыслов. – Астана – Алматы : Институт мировой экономики и политики (ИМЭП) при Фонде Первого Президента РК – Лидера Нации, 2016. – С. 34.

хотя государство, банки и иные структуры делают все возможное для создания защищенных серверов, опасность хищения данных платежных карт, сведений из документов, удостоверяющих личность, сохраняется. В печати нередко приводились факты, когда персональные данные граждан незаконно использовались работниками банков, хакерами и другими лицами для кражи денег с банковских счетов, оформления кредитов, проведения сделок с недвижимостью без ведома собственника и прочих противоправных действий, совершаемых из корыстных целей. Нередко и сами граждане провоцируют совершение преступлений, выкладывая в социальные сети широкий спектр сведений о себе, необдуманно передавая по электронной почте или незащищенным каналам мобильной связи копии своих документов. В этой связи должна быть обеспечена усиленная система внутренней безопасности с постоянным обучением сотрудников организации, проведением профилактических бесед по вопросам административной и уголовной ответственности за правонарушения в данной сфере. Следует также осуществлять разъяснительную работу среди населения о нецелесообразности таких действий.

Еще один аспект информационной безопасности личности касается морально-психологической защиты человека от информации, наносящей вред или создающей угрозу для жизни, здоровья, имущества, психики человека. Речь идет о воздействии на сознание человека путем размещения в сети видеороликов, разного рода постов, фотографий, статей, обращений, иной информации с использованием приемов нейролингвистического программирования и других психотехник, разжигающих национальную и расовую рознь, призывающих к суициду, благотворительности, оказанию финансовой помощи больным детям и социально незащищенным лицам, обещающих легкие заработки в интернете и т.д. Брачные аферисты – также частые гости Интернета, через который они заводят знакомства с одинокими женщинами. Через Интернет сегодня можно купить наркотики, различные поддельные документы, получить доступ к закрытой информации и пр. Особенно подвержены деструктивному влиянию таких сайтов дети, подростки, пожилые люди, лица с низким уровнем образования и невысокими доходами, неустойчивой психикой. Таких людей легко обмануть, ими легче манипулировать.

Во избежание подобного негативного воздействия становится очевидным, что одной воспитательно-разъяснительной работы среди школьников и молодежи недостаточно. Необходимо вводить в обучение дисциплину «Информационная безопасность», если не отдельным спецкурсом, то хотя бы отдельным разделом или отдельными темами при преподавании таких дисциплин, как «Основы безопасности жизнедеятельности», «Информатика», «Основы государства и права» и т.д. Во многих юридических вузах или на юридических факультетах университетов уже преподается курс «Информационное право», где в числе прочих рассматриваются вопросы информационной безопасности личности.

Институт защиты персональных данных является одним из важнейших институтов гражданского общества. В нашей стране он достаточно молодой, и еще должным образом не изучен. Особенно актуальными сейчас являются нюансы сбора, обработки и защиты персональных данных работодателем при приеме на работу наемных работников, тонкости обмена персональными данными во время заключения договоров, защита личных данных в сети Интернет, а также вопросы хранения, использования и уничтожения персональных данных.

Лузин А.И.,
старший преподаватель
кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУ ВО «РГУП»
г. Краснодар

ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ СФЕРЕ

Образовательный процесс в настоящее время касается наименее защищенных от пропаганды членов общества – детей и подростков. Поэтому система информационной безопасности образовательного учреждения должна обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений и гарантировать ограниченный доступ в стены образовательного учреждения деструктивной пропаганды, как незаконного характера, так и безобидной, но предполагающей воздействие на сознание учащихся в заведениях среднего полного общего и высшего образования.

Под информационной безопасностью с одной стороны рассматривается комплекс организационно-технических мероприятий, обеспечивающих целостность и конфиденциальность информации в сочетании с её доступностью для пользователей, с другой – это показатель, отражающий статус защищенности информационной системы. Защищенность информационной системы организации достигается за счет реализации комплекса мероприятий и средств защиты, основанных на локальной политике безопасности и анализе рисков, допустимых для образовательной структуры в период её деятельности. Сферы образовательной деятельности, системы государственного регулирования, информационные сети, банки и т.п. требуют специальных мер обеспечения информационной безопасности и предъявляют особые требования к надежности функционирования хозяйственных систем в соответствии с характером и важностью решаемых задач в образовательной системе. Образовательная безопасность как комплекс организационно-технических мероприятий создает условия предотвращения утечки

конфиденциальной информации, обучающихся из баз данных, а также предотвращает внедрение антисоциальных информационных потоков в учебный процесс. Процесс защиты информации осуществляется за счет недопущения нарушения локальной политики информационной безопасности, предотвращения диверсий, устранения причин возникновения ущерба. В условиях недостаточной защиты информации образование находится в условиях неопределенности и риска воздействия со стороны третьих сил.

В понятие информационной безопасности образовательного учреждения также входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы. Вторым аспектом понятия станет защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

В настоящее время в системе образовательной деятельности недостаточно внимания уделяется безопасности информации и её защите. В основном безопасность рассматривается, как перечень основных показателей, по которым делается оценка о ее защищенности. В этом случае, для реализации грамотной политики экономической безопасности предприятия, необходимо учитывать такой немаловажный фактор, как поступающая информация и принимаемые на её основе управленческие решения. Для того чтобы решить эти проблемы необходимо изучить специфику и проанализировать основные направления и информационные потоки создания и использования информации в образовательном процессе.

В системе охраняемой законом информации, находящейся в распоряжении образовательного учреждения, можно выделить основные группы, представленные на рисунке 1.

Рисунок 1 – Основные группы охраняемой законом информации

Представленные сведения могут стать объектом возникновения внешней угрозы. Проникновение может нарушить сохранность оцифрованных книг, уничтожить хранилища знаний, внести изменения в структуру программ, используемых для обучения.

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность подростков, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус.

Можно выделить основные группы объектов, которые вероятно подвергнуться намеренному или ненамеренному воздействию представлены на рисунке 2.

Рисунок 2 – Объекты, которые могут подвергнуться воздействию

Обучающиеся, подверженные внешнему агрессивному информационному влиянию и способные создать в школе криминальную ситуацию, также можно выделит в отдельную категорию группы риска. В последнее время перечень таких ситуаций существенно расширился, что говорит о возможной целенаправленной психологической атаке на сознание детей и подростков. Угрозы, направленные на повреждение любого из компонентов

системы, могут носить как случайный, так и осознанный преднамеренный характер.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть спрогнозированы. Их виновниками могут оказаться учащиеся, служащие, конкуренты, третьи лица с намерением на совершение киберпреступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию при работе с компьютерными системами и программами. Наибольшей опасности подвергаются компьютерные сети, доступ к которым может быть получен извне. Определенной проблемой также является нарушение авторских прав, намеренное хищение чужих разработок. Следует также отметить риск использование учебного оборудования и образовательного процесса для создания условий вовлечения ребенка в криминал и терроризм.

В России принята «Национальная стратегия действий в интересах детей»[1], определяющая степень угроз и меры защиты их безопасности. В связи с чем необходимо координировать действия по ограничению агрессивного воздействия на сознание ребенка, которые должны стать основными. На втором месте должно оказаться обеспечение безопасности цифровой инфраструктуры.

Представляется целесообразным придерживаться мнения о том, что: «информационное обеспечение образовательной деятельности, как метода контроля и защиты необходимо рассматривать в аспекте качественного информирования лиц, принимающих решения»[2].

Защита информации опирается на действующие в этой сфере законы, определяющие отдельные ее массивы как подлежащие защите. Они выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна).

Также необходимо в образовательном процессе учитывать роль морально-этических ценностей, на которых должна основываться система мер, защищающих обучающихся от деструктивной, этически некорректной, незаконной информации.

Необходимо выработать ряд внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями в рамках образовательного учреждения, а также внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни сведений, не подлежащих передаче. Дополнительно необходимо разработать политику безопасности, определяющую порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и

---

[1] Распоряжение Правительства РФ от 18 марта 2021 г. № 656-р «О внесении изменений в распоряжение Правительства РФ» от 22 марта 2017 г. № 520-р. – URL : https://www.garant.ru/products/ipo/prime/doc/400371751/ (дата обращения 12.09.2021).

[2] Там же.

документов. Эта политика должна определять порядок доступа студентов к сети Интернет в компьютерных классах, возможность защиты от антисоциальных электронных ресурсов, запрет на пользование собственными носителями информации.

Разработать регламент доступа к электронной почте, к которой имеют доступ сотрудники и учащиеся, чтобы избежать угроз заражения вирусами и получения некорректной информации. Также, должно быть использовано программное обеспечение, ограничивающее несанкционированный доступ обучающихся на определенные сайты.

Итоги проводимых исследований показывают, что они определяются способами осуществления мер информационной безопасности, в которой важнейшим элементом выступает реструктуризация информационно-управленческой системы образовательной организации. В настоящее время, создание различных информационных сетей, компьютерных систем с целью оперативной реализации организационно-управленческих функций требует много внимания для их информационной защищенности и безопасности. Очень часто руководители стараются сэкономить на средствах защиты, что приводит к утечке конфиденциальной информации, потере важных сведений и утрате данных. Для реализации политики информационной безопасности в образовательной сфере необходимо организовать структуризацию информационных потоков по определенным алгоритмам, представленным на рисунке 3.

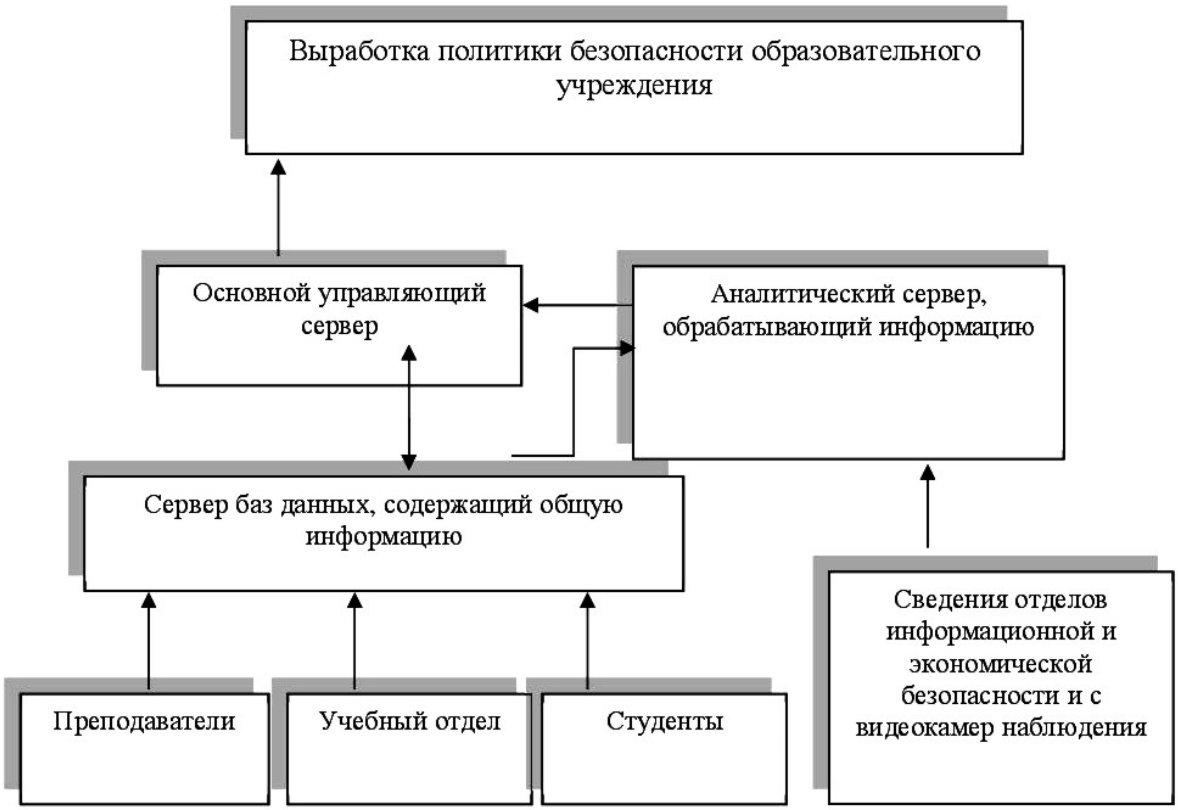

Рисунок 3 – Информационных потоки в системе безопасности образовательной среды

Все меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности. Также для реализации концепции безопасности необходимо привлечение родителей студентов, в ряде случаев они помогут провести реализацию мер обеспечения информационной безопасности и определение мер по ограничению информации, которую студент может получить дома. Таким образом комплексная реализация мер по защите информационного поля в образовательной сфере позволит свести к минимуму возможные риски, которые могут возникнуть в ходе учебного процесса и обезопасить не только преподавательский состав, но и студентов, за которых несет ответственность образовательное учреждение в период нахождения его на территории организации.

Петухов А.Ю.,
кандидат педагогических наук,
доцент кафедры оперативно-розыскной деятельности
в органах внутренних дел,
«Краснодарский Университет МВД России»
г. Краснодар

ПРОБЛЕМЫ ОПЕРАТИВНО-РОЗЫСКНОГО ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Быстроразвивающаяся компьютерная сеть Интернет сочетает в себе не только достоинства, но и значительные недостатки, способствующие использованию возможностей информационных и коммуникационных технологий в преступной деятельности. Преступления, совершаемые с помощью информационных технологий, являются совершенно новым видом преступности. А, потому, криминогенные процессы, которые сегодня существуют в сети, представляют достаточно большую угрозу, как для отдельно взятого человека, так и для государства в целом.

За первое полугодие 2020 года в России почти двукратно выросло количество преступлений в сфере компьютерной информации. Об этом говорится в сообщении, опубликованном на сайте МВД России: «Существенным фактором, оказывающим негативное влияние на криминогенную ситуацию в стране, продолжает оставаться рост IT-преступности. За январь-июнь 2020 года он составил 91,7 % по сравнению с аналогичным периодом прошлого года, а удельный вес указанных противоправных деяний в общей структуре преступности достиг 22,3 %»[1].

[1] О состоянии преступности в Российской Федерации в 1-м полугодии 2020 года // Официальный сайт МВД России. – URL : https://мвд.рф/news/item/20580266 (дата обращения 12.09.2020).

Таким образом, мы можем сделать вывод о том, что информационные технологии стали использоваться при совершении различных преступлений, это и незаконный оборот наркотиков, оружия и боеприпасов, мошеннические действия в сети Интернет, преступления, связанные с террористической и экстремистской деятельностью. Именно поэтому, уже в конце 2019 года Министр внутренних дел Российской Федерации Владимир Колокольцев принял решение о создании специальных подразделений, которые будут специализироваться на противодействии преступлениям, совершаемым с использованием IT-технологий[1]. В декабре 2020 года МВД России было анонсировано создание специализированного подразделения «киберполиции».

Сегодня, киберпреступники преследуют разные цели, это могут быть прямые атаки на компьютеры или другие устройства с целью вывода их из строя, распространение вредоносных программных кодов, получение личной и иной значимой информации, торговля запрещенными предметами и веществами. В рамках статьи мы не разделяем преступления, непосредственно связанные с посягательством на информацию и иные виды преступлений, совершаемые с использованием информационных технологий, так как целью настоящего исследования, является поиск алгоритмов и методов выявления лиц их совершивших. Поэтому преступления, совершенные с использованием информационно-коммуникационных технологий, можно разделить на следующие виды[2]:

– неправомерное подключение к информационно-телекоммуникационной сети Интернет;

– создание, использование и распространение сетевых вредоносных программ;

– незаконное изготовление, хранение, распространение, рекламирование и (или) публичная демонстрация информации, запрещённой к свободному обороту, совершённое с использованием сети Интернет;

– нарушение авторских и смежных прав, а также незаконное использование чужого товарного знака, совершённые с использованием сети Интернет;

– мошенничество, совершенное с использованием сети Интернет;

– хищение электронных реквизитов и сбыт поддельных кредитных, либо расчётных карт;

– вымогательство, совершённое с использованием сети Интернет;

– сбыт наркотиков и иных запрещенных предметов;

– кибертерроризм.

---

[1] В МВД России будут созданы новые подразделения по борьбе с преступностью в сфере высоких технологий // Официальный сайт МВД России. – URL : https://мвд.рф/news/item/18809813 (дата обращения 12.09.2020).

[2] Кибертерроризм // Официальный сайт научного журнала «Мир народов». – URL : http://mirnarodov.ru/2018/04/19/kiberterrorizm-ugroza-21-veka/ (дата обращения 17.09.2020).

В настоящее время, классические возможности оперативно-розыскной деятельности не позволяют в полной мере осуществлять эффективное противодействие рассматриваемым нами преступлений. Причинами такого положения дел, являются отсутствие достаточных у оперативных сотрудников знаний в IT-сфере, недостаточная оснащенность оперативных подразделений, отсутствие действенных алгоритмов оперативно-розыскного документирования рассматриваемых преступлений.

Сегодня многие авторы исследующие вопросы теории и практики оперативно-розыскной деятельности указывают на необходимость широкого использования и внедрения возможностей искусственного интеллекта в оперативно-розыскную деятельность, внедрения систем анализа больших данных. На наш взгляд, это возможности будущего. На текущий момент, таких реализованных систем в правоохранительной деятельности просто нет. Да и появившись, они будут решать несколько иные задачи, прежде всего аналитические. А, оперативному сотруднику, уже сегодня требуется вполне простой и понятный алгоритм действий, а также понятные и доступные средства для решения поставленных перед ним задач.

Решение вышеназванных проблем, кроется, на наш взгляд, в широком внедрении в профессиональную деятельность оперативных подразделений методов использования компьютерной разведки на базе открытых источников информации. Собственно, как и в привычной нам форме осуществления оперативно-розыскной деятельности, где основной и первоначальной задачей любого оперативного сотрудника, является сбор первичной информации о событии или объекте оперативной заинтересованности, раскрытие преступлений, совершенных посредством использования современных информационных технологий, либо лиц, их совершивших начинается со сбора доступной информации и ее последующая проверка. Компьютерная разведка выступает здесь совокупностью методов и используемых приемов, которые применяются оперативным сотрудником для получения необходимых массивов данных с целью последующего их анализа. Следует сказать, что, как и в классических ситуациях, порой для раскрытия преступления достаточно лишь одного незаметного факта, так и для компьютерных преступлений, для установления личности преступника бывает достаточно одного особенного фона на размещенной фотографии в сети Интернет, определенного высказывания, оставленного преступником в социальной сети или чате.

Одним из основных методов ведения такой разведки, основанной на поиске, сборе и анализе информации, направленной на решение разведывательных задач по поиску киберпреступников и раскрытия киберпреступлений, выступает OSINT. Технология компьютерной разведки (OSINT – Open Source Intelligence) – это разведка на базе открытых источников информации и доступных каждому пользователю. Иными словами, это первоначальный сбор информации на открытых ресурсах сети и последующий ее анализ.

Однако, такая разведка позволяет осуществлять поиск необходимой информации не только на поверхности открытых данных сетевого пространства, но и той, которая ввиду длительного отсутствия ее использования была скрыта в архивы или хранится в информационных системах со слабой защитой. Поэтому, область действия интернет-разведки охватывает не только Интернет, но ещё и иные доступные источники оперативно-значимой информации, это традиционные средства массовой информации, специализированные издания, фотографии, видео, метаданные и многое другое.

В этой связи, компьютерная разведка предполагает два основных способа сбора информации. Пассивный способ сбора информации обеспечивает сбор сведений в сети при котором лицо, осуществляющее поиск, никак не выдает себя, иными словами, поиск осуществляется только в пределах легальной, общедоступной, незащищенной информации. Активный способ предполагает активные действия, направленные на прямое или опосредованное (посредством использования специализированных программ) взаимодействие с исследуемым компьютером или информационной системой. Это могут быть прямые подключения к открытым портам, сканирование уязвимостей информационной системы или компьютерной защиты и многое другое. Следует отметить, что при использовании активного способа поиска информации, вероятность обнаружения лица, осуществляющего поиск достаточно велика.

Вышеперечисленные факторы позволяют нам предложить типовой алгоритм поиска и сбора информации с помощью технологии OSINT для целей оперативно-розыскной деятельности. На наш взгляд, предлагаемый алгоритм реализуется посредством выполнения следующих действий:

1. Систематизация имеющейся первичной оперативно-значимой информации об интересующем объекте;
2. Определение ее структуры и полноты (это могут быть вполне разрозненные сведения об объекте поиска: ФИО, номер телефона, адрес электронной почты, логины и другое);
3. Выбор направления поиска недостающей информации по конкретным структурным элементам имеющейся первичной информации;
4. На основании выделенных направлений поиска осуществляется выбор перечня открытых программно-поисковых комплексов, доступных оперативному сотруднику;
5. Планирование процесса поиска, исходя их выделенных направлений и имеющихся программных ресурсов для осуществления поиска;
6. Обобщение и последующий анализ полученных в ходе поиска сведений и выявление недостающей информации;
7. Повторный выбор направлений и средств поиска, с учетом полученной информации.

Таким образом, завершение процесса поиска интересующей оперативного сотрудника информации наступает в двух случаях:

1) получение исчерпывающей информации об объекте поиска;
2) использование всех доступных средств поиска.

Естественно, что такой алгоритм должен быть снабжен соответствующим инструментарием. Именно использование специализированных программ вызывает порой главную сложность в оперативно-розыскной деятельности, ввиду их незначительного количества и высокой стоимости коммерческих продуктов. Особенностью, рассматриваемой нами технологии OSINT, являет то, что она фактически бесплатна. Для сбора информации в сети используются открытые и общедоступные ресурсы сети. Определенные функции этих систем предполагают незначительную плату за их использованием, но это незначительные суммы. Как правило, для использования этих ресурсов достаточно регистрации на сервисе.

Подводя итог, можно сделать следующие выводы. Неоспоримым преимуществом рассматриваемой нами методики, является то, что в отличие от классических возможностей оперативно-розыскной деятельности, OSINT благодаря своей низкой стоимости, повсеместной доступности, отсутствием ограничений, связанных с соблюдением режима секретности, надёжности и в силу работы с информацией в режиме реального времени, всегда доступна оперативному сотруднику. Полагаем, что использование этой технологии, в случае противодействия киберпреступности, преступлений, связанных незаконным оборотом наркотиков, осуществляемых в теневом Интернете, преступлений связанных с экстремистской деятельностью лиц, должно всегда предшествовать проведению классических оперативно-розыскных мероприятий и являться одним из действенных способов проверки первичной оперативной информации и установлению личности преступника.

Технология компьютерной разведки, являясь одной из важнейших технологий «глубинного сбора» разноформатной информации, позволит сосредоточить усилия оперативных подразделений на выполнении более сложных и «узких» задач, не привлекая силы специальных подразделений на добывание того, что можно получить из открытых источников. Полагаем, что активное использование этой технологии в оперативно-розыскной деятельности, позволит в значительной степени повысить эффективность работы оперативных подразделений в противодействии преступлений, совершаемых с использованием современных информационных технологий.

Сарина С.А.,
кандидат юридических наук,
ассоциированный профессор
кафедры юриспруденции и
международного права,
Университет «Туран»
г. Алматы

ВОПРОСЫ ПРИЗНАНИЯ И ПРИВЕДЕНИЯ В ИСПОЛНЕНИЕ РЕШЕНИЙ ИНОСТРАННЫХ АРБИТРАЖНЫХ СУДОВ В РЕСПУБЛИКЕ КАЗАХСТАН С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Рассматривая вопрос о признании и приведении в исполнение на территории Республики Казахстан арбитражных решений, необходимо четко разграничивать:

1) признание и приведение в исполнение в Республике Казахстан *иностранных арбитражных решений*;

2) исполнение в Республике Казахстан *решений международных коммерческих арбитражей*, вынесенных на ее территории.

К числу иностранных арбитражных решений относятся решения, вынесенные международными коммерческими арбитражами за пределами Республики Казахстан.

В условиях монополии государства на осуществление внешнеэкономической деятельности вопросы принудительного исполнения иностранных арбитражных решений возникали редко. Подавляющее большинство решений международных арбитражей исполнялось советскими внешнеторговыми организациями добровольно[1].

Не случайно поэтому, что в советском законодательстве вплоть до 1988 г. отсутствовал нормативный акт, предусматривавший порядок исполнения иностранных арбитражных решений. С выходом на международную экономическую арену большого количества казахстанских предприятий и организаций, ситуация резко изменилась и теперь можно сказать, что исключением является добровольное исполнение решений. Поэтому вопросы принудительного исполнения приобрели особую остроту.

В настоящее время признание и приведение в исполнение иностранных арбитражных решений осуществляется в Республике Казахстан на основании Закона о МКА, ГПК, Закона «Об исполнительном производстве и статусе судебных исполнителей» и Нью-Йоркской конвенции 1958 г.

В ст. 425 ГПК РК и ст. 80 Закона РК «Об исполнительном производстве и статусе судебных исполнителей» закреплено, что порядок

[1] Шишкин С.А. Признание и исполнение решений иностранных судов и арбитражей / С.А. Шишкин // Юридический мир. – 1997. – № 5. – С. 27–30.

исполнения в Республике Казахстан решений иностранных судов и арбитражей, помимо этих законодательных актов, определяется соответствующими международными договорами, в которых участвует Казахстан. Сюда, безусловно, включаются договоры и соглашения, которые были подписаны Республикой Казахстан. Наряду с Нью-Йоркской конвенцией, в этот перечень могут входить Конвенция стран СНГ о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (г. Кишинев, 07 октября 2002 г.), Соглашение стран СНГ о порядке разрешения споров, связанных с осуществлением хозяйственной деятельности (г. Киев, 20 марта 1992 г.)[1], Соглашение о порядке взаимного исполнения решений арбитражных, хозяйственных и экономических судов на территориях государств-участников СНГ (г. Москва, 06 марта 1998 г.)[2], а также ряд двусторонних соглашений о правовой помощи, о взаимной защите капиталовложений и др., включающих условия о взаимном признании и исполнении иностранных арбитражных решений.

К сожалению, Казахстан не является участником ряда важнейших международно-правовых актов, в частности: Конвенции по вопросам гражданского процесса (Гаага, 01 марта 1954 г.). СССР присоединился в свое время к данной Конвенции; Конвенции о вручении судебных и внесудебных документов за границей по гражданским и арбитражным вопросам (Гаага, 15 ноября 1965 г.); Брюссельской конвенции по вопросам юрисдикции и принудительного исполнения судебных решений в отношении гражданских и коммерческих споров (27 сентября 1968 г.); Конвенции о получении за границей доказательств по гражданским или торговым делам (Гаага, 18 марта 1970 г.); Конвенции по предоставлению показаний за пределами государств в рамках гражданских и арбитражных процессов (Гаагской конвенции по свидетельским показаниям) (Гаага, 18 марта 1970 г.); Конвенции о юрисдикции и приведении в исполнение судебных решений по гражданским и коммерческим делам (Лугано, 16 сентября 1988 г.)[3]. Это, конечно, вызывает сложности в решении вопроса о том, подлежат ли признанию и исполнению на территории РК решения судов тех государств, с которыми не установлены соответствующие договорные отношения об оказании правовой помощи.

Здесь следует еще раз напомнить о том, что Республика Казахстан присоединилась к Нью-Йоркской конвенции, а это означает исполнение в Республике Казахстан только тех арбитражных решений, которые были вынесены на территории других государств-участников этой Конвенции.

---

[1] Вестник Высшего Арбитражного Суда Российской Федерации. – 1992. – № 1. – С. 114–118. Вестник Высшего Арбитражного Суда Российской Федерации. – 1992. – № 1. – С. 114–118.

[2] Баймолдина З.Х. Гражданское процессуальное право Республики Казахстан : в 2-х томах. – Т. 2: Особенная часть. (Темы 16–30) : учебник. – Алматы : КазГЮА, 2001.

[3] Баймолдина З.Х. Признание и исполнение иностранных судебных решений. – URL : http://www.notariat.ru/bulletinarhiv/press_861_23.aspx/ (от 05.09.06). – 6 с.

В соответствии со ст. 3 Нью-Йоркской конвенции признание и приведение в исполнение иностранных арбитражных решений в странах-участницах не должно быть более обременительным, чем признание и приведение в исполнение их внутренних арбитражных решений. Это требование в Казахстане полностью соблюдено. Положения Закона о МКА в отношении порядка признания и исполнения иностранных арбитражных решений полностью соответствуют Нью-Йоркской конвенции.

Для признания и приведения в исполнение иностранного арбитражного решения в ст. 32 Закона о МКА предусмотрено предъявление кредитором решения в компетентный суд письменного ходатайства, сопровождаемого подлинниками или «должным образом» заверенными копиями арбитражного решения и арбитражного соглашения (в «должным образом» заверенном переводе на государственный или русский язык). Кроме того, в ст. 33 Закона о МКА перечислены основания, по которым компетентный суд может отказать в признании или приведении арбитражного решения в исполнение. Как уже говорилось, они соответствуют основаниям, предусмотренным в ст. 5 Нью-Йоркской конвенции.

Закон о МКА не затрагивает процессуальных аспектов и не упоминает о том, в каком именно порядке иностранное арбитражное решение приводится в исполнение на территории Республики Казахстан. Но ст. 32 Закона о МКА отсылает к «компетентному суду», т.е. суду судебной системы Республики Казахстан. Следовательно, арбитражное решение признается обязательным и приводится в исполнение при подаче в компетентный суд письменного ходатайства об этом.

В международных отношениях важно, чтобы решение по спору, вынесенное судом одного государства, имело юридические последствия в другом государстве. Однако акты юрисдикционных органов, по общему правилу, имеют территориальный характер действия. Юридическую силу в другом государстве они приобретают, если другое государство в какой-либо форме выразит на это свое согласие. Формы выражения такого согласия, а также способы признания и исполнения иностранных арбитражных решений могут быть различными. По общему правилу, они зависят от законов конкретной страны, а также от положений международных договоров, в которых страна участвует. Но вместе с тем общим требованием для признания и принудительного исполнения арбитражного решения является требование взаимности[1].

Приведение в исполнение решения производится по ходатайству заинтересованной стороны.

Установление в ГПК правила об обращении за принудительным исполнением решения в суд по месту рассмотрения спора арбитражем представляется неудачным в связи со следующим.

---

[1] Попондопуло В. Проблемы, связанные с принудительным исполнением решений третейских судов / В. Попондопуло, Е. Скороходов // Хозяйство и право. – 1999. – № 9. – С. 31–32.

Во-первых, в узком смысле этого выражения это может быть суд в том же помещении, на той же улице, в том же районе и в городе, а в широком – той же области, в стране и т.д. Во-вторых, по месту рассмотрения спора может быть несколько судов. Например, какой-либо арбитраж рассмотрел спор и вынес решение в г. Алматы. Если следовать норме ГПК, то исполнительный лист должен быть выдан судом по месту рассмотрения спора в г. Алматы, где на сегодняшний день, кроме Алматинского городского суда, приравненного к областному, имеются специализированный межрайонный экономический суд, специализированный межрайонный административный суд и порядка 11 (кроме военных) районных судов. Аналогичная ситуация имеется и в других крупных регионах страны[1].

На практике ходатайство о принудительном исполнении решения арбитража ни один суд не принимает к производству, ссылаясь на то, что он не является судом по месту рассмотрения спора.

Суд по месту рассмотрения спора отказывает в принятии ходатайства, указывая, что он не является компетентным судом, поскольку таковым по Закону о МКА является суд, которому был бы подсуден спор по первой инстанции в случае отсутствия соглашения сторон о рассмотрении дела в арбитраже. Счастливое же совпадение в одном лице суда по месту рассмотрения спора и компетентного суда иногда просто невозможно[2].

Вопрос о том, в каком порядке следует исполнять в Республике Казахстан арбитражные решения, вынесенные на территории других стран-членов СНГ, что представляет собой частный случай исполнения решений иностранных арбитражей, на практике поднимался неоднократно. Следует ли при этом применять Соглашение о порядке разрешения споров, связанных с осуществлением хозяйственной деятельности, или же Нью-Йоркскую конвенцию?

К решению проблемы исполнения арбитражных решений по спорам между сторонами из стран СНГ существует два подхода. Согласно одному из них, исполнение должно производиться на основании Соглашения, поскольку оно, будучи региональным международным договором, имеет приоритет перед Нью-Йоркской конвенцией[3].

Эта позиция основывается на следующем деле, ответчиком в котором являлось российское акционерное общество.

Суд общей юрисдикции РФ отказался исполнить арбитражное решение, вынесенное Международным коммерческим арбитражным судом при

---

1 Басин Ю.Г. Исполнение арбитражных решений по коммерческим спорам в Казахстане / Ю.Г. Басин // Гражданское законодательство Республики Казахстан. Статьи, комментарии, практика. – Алматы : ТОО Баспа, 2001. – № 10. – С. 36–47.

2 Ким В. Проблемы исполнения решений третейских судов и арбитражей / В. Ким // Юрист. – 2005. – № 6. – С. 30–32.

3 Нешатаева Т. О признании и исполнении решений по хозяйственным спорам стран СНГ на территории Российской Федерации / Т. Нешатаева // Закон. – 1998. – № 7. – С. 98–104.

ТПП Республики Беларусь по спору между белорусской и российской сторонами, посчитав, что его исполнение находится в компетенции государственных арбитражных судов. При этом суд сослался на то, что Российская Федерация и Республика Беларусь являются участницами Соглашения о порядке разрешения споров, связанных с осуществлением хозяйственной деятельности, от 20 марта 1992 г., которое в ст. 3 предусматривает, что «хозяйствующие субъекты каждого государства-участника СНГ имеют на территории других Независимых Государств право беспрепятственно обращаться в суды, арбитражные (хозяйственные) суды, третейские суды и другие органы, к компетенции которых относится разрешение дел...». Далее Соглашение устанавливает, что решения компетентных судов взаимно признаются и исполняются на территории государств-участников СНГ (ст. 7, 8). Механизм исполнения судебных решений определяется по праву страны, в которой решение подлежит исполнению.

Арбитражный суд выдал приказ на исполнение решения третейского суда иностранного государства, указав, что оснований для отказа в выдаче приказа за исполнение суд не усматривает, так как Россия и Беларусь участвуют в Соглашении 1992 г., предусматривающем «национальный порядок исполнения решений третейских судов».

Суд посчитал себя вправе выдать приказ на исполнение решения, вынесенного третейским судом государства-участника СНГ, исходя из того, что порядок исполнения решений таких судов на территории Российской Федерации определяется Временным положением о третейском суде для разрешения экономических споров 1992 г. и, согласно разделу 5 данного Положения, приказы на принудительное исполнение решений третейских судов выдаются арбитражным судом. Согласно другому подходу к решению той же самой проблемы арбитражные решения, вынесенные в государствах-участниках СНГ, исполняются на территории РК в порядке, предусмотренном Нью-Йоркской конвенцией. Если между Казахстаном и соответствующей страной заключен двусторонний договор, предусматривающий взаимное признание и исполнение арбитражных решений, то исполнение производится на основании этого договора.

Дело в том, что Соглашение, хотя и упоминает в ч. 2 ст. 3, что хозяйствующие субъекты каждого из государств-участников СНГ вправе на территории других государств-участников СНГ «беспрепятственно обращаться в суды, арбитражные (хозяйственные) суды, третейские суды...» для разрешения гражданско-правовых споров, в дальнейшем, однако, никак не регулирует порядок исполнения решений третейских судов и говорит исключительно о признании и исполнении решений государственных судов. Статья 8 Соглашения предусматривает представление в компетентный суд «исполнительного документа», выданного судом, разрешившим дело по существу. Третейские суды таких документов не выдают. На эти обстоятельства обратил внимание Высший Арбитражный Суд РФ, который в своем Письме от

01 марта 1996 г. № ОМ-37 «О решении вопросов об исполнении решений арбитражных судов одного государства на территории другого государства», отметил: «Соглашение о порядке разрешения споров, связанных с осуществлением хозяйственной деятельности, от 20.03.1992 г. и Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22.01.1993 г. предусматривают взаимное признание и исполнение решений судов по гражданским и семейным делам одного государства на территории другого. При этом под судами понимаются государственные (а не третейские) суды, которые правомочны принимать решения, получающие силу закона и подлежащие принудительному исполнению на территории государства, то есть суды общей компетенции и арбитражные (хозяйственные) суды»[1].

Автор придерживается второй позиции – о том, что исполнение решений арбитражных (третейских) судов, вынесенных по спорам между сторонами из стран СНГ, производится в общем порядке по правилам, предусмотренным Законом о МКА. Развитие судебной практики в РК показывает; что по второму пути.

Для подтверждения можно привести такой пример. Решением МКАС при ТПП РФ было удовлетворено исковое заявление АО «Красноярские авиалинии» и на ЗАО Авиакомпания «Гиацинт-Рахат» (Республика Казахстан) была возложена обязанность уплатить истцу задолженность по арендной плате авиатранспортного средства в сумме 200836,78 долларов и арбитражного сбора в размере 8552 долларов. В виду уклонения должника от добровольного исполнения решения третейского суда, взыскатель обратился в Алматинский городской суд с ходатайством о выдаче исполнительного документа для принудительного исполнения решения третейского суда. Суд ходатайство отклонил, ссылаясь в определении от 18 октября 2000 г. на необходимость представления заинтересованным лицом исполнительного документа, выданного компетентным судом РФ, для решения судом РК вопроса о принудительном исполнении решения суда независимого государства в соответствии с требованиями Киевского соглашения от 23 марта 1992 г. Коллегия по хозяйственным делам Верховного Суда РК определение городского суда отменила и частную жалобу АО «Красноярские авиалинии» удовлетворила, поскольку ссылка на Киевское соглашение, по мнению коллегии, является неправомерной в виду того, что этим международным договором регламентирована процедура разрешения экономических споров компетентными судами государств СНГ, к каковым не относятся третейские суды и арбитражные комиссии, применимым правом в данном случае является Нью-Йоркская Конвенция, в ст. 3 которой закреплено, что к признанию и приведению к исполнению решений иностранных арбитражей не должны применяться существенно более обременительные условия, или более

[1] Вестник Высшего Арбитражного Суда Российской Федерации. – 1996. – № 12.

высокие пошлины и сборы, чем те, которые существуют для признания и приведения в исполнение решений[1].

Вопрос о возможности исполнения в Республике Казахстан арбитражного решения, вынесенного в государстве СНГ, которое не участвует ни в Нью-Йоркской конвенции, ни в Соглашении 1992 г., в принципе остается открытым. По мнению Е.А. Виноградовой, ответ на этот вопрос «будет, скорее всего, отрицательным»[2]. Мы считаем, что он может быть решен положительно. Закон о МКА не содержит норм в отношении его применения только к арбитражным решениям, вынесенным на территории государств-участников Нью-Йоркской конвенции или иного международного соглашения, либо только на основании взаимности. Более того, ст. 7 Нью-Йоркской конвенции «не лишает никакую заинтересованную сторону права воспользоваться любым арбитражным решением в том порядке и в тех пределах, которые допускаются законом... страны, где испрашивается признание и приведение в исполнение такого арбитражного решения». Как показывает зарубежная практика, применение внутреннего законодательства о признании и исполнении иностранных арбитражных решений к решениям, вынесенным на территории государств, не участвующих в Нью-Йоркской конвенции, отнюдь не является исключением (хотя не является и общепринятым правилом). Так что все будет зависеть от того, какую позицию займут суды Республики Казахстан, столкнувшись с подобной ситуацией.

Решения международных коммерческих арбитражей, вынесенные на территории Республики Казахстан и направленные против казахстанского юридического или физического лица, совместного предприятия либо иностранного лица, имеющего на территории Республики Казахстан имущество, не нуждаются в признании и исполняются в порядке, предусмотренном ГПК РК и Законом «Об исполнительном производстве и статусе судебных исполнителей». Согласно п. 4 ст. 5 этого Закона исполнительными документами, в частности, являются «исполнительные листы, выдаваемые на основании решений международных и иностранных судов и арбитражей». К их числу относятся арбитражи ad hoc и постоянно действующие арбитражи, созданные на территории Республики Казахстан на основании Законов о МКА и о третейском суде.

Исполнение на территории Республики Казахстан арбитражного решения, вынесенного на основании Закона о МКА, производится по определению компетентного суда о его принудительном исполнении. Сторона, ходатайствующая о выдаче исполнительного листа, должна приложить к ходатайству документы, предусмотренные ст. 32 Закона о МКА. Суд может отказать в выдаче исполнительного листа только по ограниченным основаниям, предусмотренным в ст. 33 Закона о МКА.

---

[1] Определение Коллегии по хозяйственным делам Верховного Суда РК от 21 февраля 2001 г. № 1к-87-01145 // сайт Верховного Суда РК. – URL : http://www.supcourt.kz

[2] Виноградова Е.А. Третейский суд. – М. : Инфра, 1997.

Как уже говорилось, на основании Закона о третейских судах действуют третейские суды, разрешающие внутренние экономические споры. Согласно ст. 1 этого Закона, он не применяется, когда хотя бы одна из сторон находится на территории другого государства либо является предприятием, организацией с иностранными инвестициями, если иное не установлено законодательными актами РК.

В цели настоящей диссертационной работы не входит подробный анализ самого процесса исполнительного производства, потому мы ограничимся только указанием на его основные вехи.

Принудительное исполнение решений международных коммерческих арбитражей, как вынесенных за рубежом, так и на территории Республики Казахстан, производится в соответствии с положениями Закона об исполнительном производстве и статусе судебных исполнителей.

В процессе исполнения арбитражного решения нередко встречаются затруднения, связанные с невозможностью немедленного взыскания с должника больших денежных сумм. Поскольку такие затруднения носят процессуальный характер, они должны преодолеваться по правилам судебного исполнительного производства, действующим в стране исполнения[1]. В ст. 13 Закона РК «Об исполнительном производстве и статусе судебных исполнителей» предусмотрено, что «при наличии обстоятельств, делающих совершение исполнительных действий затруднительным или невозможным, судебный исполнитель, взыскатель или должник вправе поставить перед судом по месту исполнения вопрос об отсрочке или рассрочке исполнения, а также от индексации присужденных сумм»[2].

Так, в казахстанской судебной практике был случай, когда городской суд г. Астаны, выдавший приказ об исполнении решения международного арбитражного суда о взыскании с казахстанского ответчика значительной суммы в иностранной валюте в пользу английского взыскателя, отсрочил начало взыскания до 2002 г. и установил рассрочку взыскания продолжительностью в пять лет. На взыскиваемые суммы по мере погашения долга начисляются пять процентов годовых.

Исполнение судебного решения требует денежных расходов. На кого они должны возлагаться: на лицо, обращающееся в государственный суд за исполнением, либо на должника? Возможны требования уплаты определенной суммы в виде государственной пошлины.

В казахстанском законодательстве эти вопросы также не нашли пока достаточно полного решения. Нередко казахстанские государственные

---

[1] Определение Коллегии по хозяйственным делам Верховного Суда РК от 21 февраля 2001 г. № 1к-87-01145 // сайт Верховного Суда РК. – URL : http://www.supcourt.kz

[2] Закон Республики Казахстан «Об исполнительном производстве и статусе судебных исполнителей» от 30 июня 1998 г. // Нормативные акты. Законы Республики Казахстан. – Алматы : ТОО «Аян Эдет», 2000.

суды требуют от лица, обратившегося за получением приказа на исполнение, уплаты государственной пошлины в размере, установленном законом для случаев предъявления в суд искового заявления. Такие требования лишены всякого обоснования[1].

Теоретически, производство по исполнению арбитражных решений в Республике Казахстан (будь то решения иностранных арбитражей или, например, МАС при ТПП РК) немногим отличается от того, что принято в большинстве стран Запада. К сожалению, на практике эта система не работает. Это относится как к исполнению решений судов общей юрисдикции, так и решений международных коммерческих арбитражей. Как отмечает Е.А. Суханов: «в нынешних условиях общепринятая мировая практика добровольного исполнения арбитражных решений под страхом оказаться в деловой и моральной изоляции отсутствует, ибо недобросовестность контрагента никого не смущает и становится, чуть ли не нормой»[2].

Таким образом, получение на руки исполнительного листа еще не гарантирует исполнение арбитражного решения. Существует много способов, которые недобросовестная сторона может применить для того, чтобы избежать исполнения решения. К ним относятся «увод» денежных средств с банковских счетов, сокрытие имущества, ликвидация предприятия должника, а также возбуждение дел о банкротстве. В соответствии с п. 1 ст. 22 Закона об исполнительном производстве исполнительное производство приостанавливается в случае возбуждения государственным арбитражным судом производства по делу о несостоятельности должника до принятия решения по указанному делу. Если имущества должника недостаточно для удовлетворения требований взыскателя, то исполнительное производство прекращается (п. 4 ст. 23). При той возможности маневров, которую предоставляет действующее законодательство о банкротстве, исполнение иностранного арбитражного решения может оказаться невыполнимой задачей, как о том неоднократно свидетельствовали иностранные компании, предпринимавшие попытки добиться исполнения решений международных арбитражей в Республике Казахстан. Можно только надеяться, что в будущем ситуация изменится к лучшему.

---

[1] Право и внешнеэкономическая деятельность / Отв. ред. Сулейменов М.К. – Алматы : Жеті Жарғы, 2001.

[2] Суханов Е. Третейские суды и предпринимательские споры / Е. Суханов // Право и экономика. – 1998. – № 2. – С. 89–91.

Соловьева С.В.,
кандидат юридических наук,
доцент кафедры административного
и финансового права,
СКФ ФГБОУВО «РГУП»
г. Краснодар

ОГРАНИЧЕНИЕ ПРАВА НА ДОСТУП К ИНФОРМАЦИИ – КАК СПОСОБ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Развитие цифровых технологий, имеющие место в настоящее время, отражается в разных сферах общественной жизни и не может не сказаться на состоянии правового регулирования, особенно если это затрагивает право граждан на свободный доступ к информации и право на информационную безопасность. Во исполнение положения статьи 29 Конституции РФ о праве на свободный поиск, получение, передачу, производство и распространение информации любым законным способом, федеральным законодательством определяется порядок правового регулирования производства, распространения и использования информации.

Основным федеральным законом, раскрывающим понятие информации и информационной безопасности, а также порядок ее обеспечения, является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1]. В данном законе информация, в зависимости от категории доступа к ней, подразделяется на общедоступную информацию и информацию, доступ к которой ограничен федеральными законами, то есть информация ограниченного доступа.

К общедоступной информации федеральный закон относит общеизвестные сведения и иную информацию. Понятие «иной информации» в законе не раскрывается, но указывается, что эта информация определяется в федеральных законах, касающихся некоторых специфических сфер деятельности, доступ к которой не ограничен. Кроме того, к общедоступной информации, относится информация доступ, к которой нельзя ограничить. В основном это информация, которая затрагивает права и свободы граждан, а также информация, определяющая правовое положение организаций, полномочия и деятельность органов государственной власти и местного самоуправления, информация о состоянии окружающей среды, информация, накапливаемая в открытых фондах и иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

В сфере обеспечения информационной безопасности наиболее неоднозначным является правовой режим информации ограниченного доступа,

---

[1] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 31.07.2006. № 31 (Ч. 1). Ст. 3448.

основное содержание данной информации раскрывается в указанном федеральном законе. В статье 9 Федерального закона об информации и ее защите сформулирован общий принцип ограничения доступа к информации. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства, при этом, обязательным требованием является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Данная правовая норма устанавливает, во-первых, в каких случаях может быть ограничено право на доступ к информации, а во-вторых, определяет, что ограничения вводятся только федеральным законом.

Информация ограниченного доступа подразделяется на два вида: информацию, отнесенную к государственной тайне, и сведения конфиденциального характера, причем, соблюдение конфиденциальности информации, является обязательным и в отношении первой, и в отношении второй.

Правовое регулирование информации, содержащей государственную тайну, осуществляется в соответствии с Законом Российской Федерации «О государственной тайне»[1], в котором определяется понятие и перечень сведений, относящихся к государственной тайне. Информация, характеризующаяся как государственная тайна, является закрытой с ограниченным доступом. Определенных критериев отнесения информации к сведениям, составляющим государственную тайну, кроме как обеспечения безопасности (в широком ее понимании, относящейся ко всем сферам общества и государства, правам и свободам человека) нет.

Что же касается, такой информации ограниченного доступа, содержащую сведения конфиденциального характера, то ее правовой режим не является таким однозначным, как государственная тайна, поскольку регулируется разными нормативными правовыми актами.

К конфиденциальной информации могут относиться любые сведения, доступ к которым ограничен законодательством: охраняемая законом тайна, персональные данные, профессиональная тайна, коммерческая тайна, служебная тайна. В целом, для придания информации статуса конфиденциальности необходимо установление правового режима, то есть издание соответствующего нормативного правового акта.

Так, понятие «охраняемая законом тайна» в законодательстве не раскрывается и не содержится перечень информации, который может составлять сведения «охраняемые законом тайны». Фактически к такой информации отнести любую информацию, в отношении которой законодатель установил режим тайны.

Например, в Трудовом кодексе РФ указывается на охраняемую законом тайну, к которой законодатель относит государственную,

---

[1] Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 13.10.1997. – № 41. – С. 8220–8235.

коммерческую, служебную и иные тайны (п. «в» п. 6 ч. 1 ст. 81 ТК РФ),[1] в Налоговом кодексе РФ закон называет в качестве охраняемых законом – банковскую, налоговую и иные тайны (п. 3.1 ст. 100 НК РФ)[2].

Понятие «иной охраняемой законом тайны» в законодательстве также не раскрывается, это могут быть сведения, в отношении которых закон устанавливает режим тайны, но прямого правового регулирования (запрета на распространение либо каким-то иным образом использование такой информации) нет.

Так, например, правовой режим тайны устанавливается в отношении: тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (п. 1 ст. 63 Закона о связи);3 личной и семейной тайны (ч. 1 ст. 23 Конституции РФ); тайны совещания судей (ч. 3 ст. 167 АПК РФ, ч. 4 ст. 194 ГПК РФ); тайны усыновления (п. 1 ст. 139 СК РФ)[4].

В основном закон прямо не называет те или иные сведения тайной, но относит их к информации ограниченного доступа, с обязательным соблюдением конфиденциальности. Например, это касается персональных данных, причем законодательство[5] не содержит конкретного перечня персональных данных, к которым может быть отнесена любая информация о гражданах, но организации либо иные операторы, использующие персональные данные граждан, обязаны соблюдать режим конфиденциальности, и информация, содержащая персональные данные не должна быть в свободном доступе.

Под профессиональной тайной понимается охраняемая законом конфиденциальная информация, ставшая известной лицу в силу исполнения им профессиональных обязанностей. Понятие профессиональной тайны, также не раскрывается в законе. В отличие от персональных данных профессиональная тайна охватывает сведения, как о гражданах, так и о юридических лицах. Разновидностями профессиональной тайны являются: нотариальная тайна, адвокатская тайна, банковская тайна, аудиторская тайна, тайна страхования, тайна следственных действий и другие ее разновидности. Режим конфиденциальности в отношении указанных разновидностей профессиональной тайны определяется законодательством, путем наложения запрета на ее свободное распространение и свободного доступа к такой информации, под угрозой привлечения к административной либо уголовной ответственности.

---

1 Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Российская газета. № 256. 31.12.2001.

2 Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ // СЗ РФ. № 31. 03.08.1998. Ст. 3824.

3 Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Российская газета. № 135. 10.07.2003.

4 Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ // СЗ РФ. 01.01.1996. № 1. Ст. 16.

5 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 31.07.2006. № 31 (Ч. 1). Ст. 3451.

Самостоятельный правовой режим имеет коммерческая тайна, так как регулируется отдельным нормативным правовым актом[1]. К коммерческой тайне относится конфиденциальная информация, которая позволяет ее обладателю получить коммерческую выгоду (увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке и так далее), при этом, коммерческая тайна и конфиденциальная информация не являются тождественными понятиями.

Коммерческая тайна является разновидностью конфиденциальной информации, но в отношении сведений, составляющих коммерческую тайну, всегда действует режим конфиденциальности, причем исчерпывающего перечня сведений, которые могут составлять коммерческую тайну, нет.

Еще одна разновидность конфиденциальной информации, которая имеет самостоятельный правовой режим – это служебная тайна. К служебной тайне относятся сведения, доступ к которым ограничен органами государственной власти в соответствии с федеральными законами либо иными нормативными правовыми актами[2].

В целом, если говорить о конфиденциальности информации, и соответственно придание ей статуса ограниченного доступа, то данный правовой режим осуществляется путем установления запрета на свободное использование той либо иной информации.

Однако, бурное развитие цифровых технологий, отмечающееся в последние годы, имеет своим следствием трансформацию самых разнообразных слагаемых общественной жизни и не может не сказаться на состоянии правового регулирования обеспечения доступа к информации и ее безопасности, как об этом говориться в Доктрине информационной безопасности Российской Федерации,3 что расширение областей применения информационных технологий, порождает новые информационные угрозы.

В связи с чем, на сегодняшний день, наблюдается тенденция установления конфиденциальности в отношении сведений, составляющих разные сферы общественной жизни и деятельности органов государственной власти и их должностных лиц. Причем, не путем установления прямого запрета на получение той или иной информации, а ограничения доступа к такой информации, тем самым государство все больше осуществляет функцию «тотального» контроля за распространением, оборотом и использованием любой информации, что, в свою очередь, может создавать опасность замены запретительного принципа права разрешительным, когда основные информационные права и свободы можно будет реализовать только в установленных государством случаях.

---

[1] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 09.08.2004. № 32. Ст. 3283.

[2] Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ. 10.03.1997. № 10. Ст. 1127.

[3] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 12.12.2016. № 50. Ст. 7074.

Отсюда вытекает потребность унифицировать перечень сведений, доступ к которым не может быть ограничен в соответствии с единым перечнем видов конфиденциальной информации и, исходя из необходимости минимизации подобных случаев, предусмотреть механизмы обязательного обнародования подпадающих под этот перечень сведений в средствах массовой информации.

Цимбал В.Н.,
кандидат юридических наук,
доцент кафедры специальных
информационных технологий
учебно-научного комплекса
информационных технологий,
«Московский Университет МВД России
имени В.Я. Кикотя»
г. Москва

ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопросы международной информационной безопасности на сегодняшний период времени стоят перед мировым сообществом достаточно актуально. Развитие информационных технологий, трансграничный обмен информацией, слабое регулирование приводит к реализации угроз в информационной сфере как на уровне отдельного государства, так и на межгосударственном уровне. В данной работе нами будут проанализированы вопросы международной информационной безопасности, которые отстаивает и продвигает Российская Федерация на международной арене.

Согласно действующим нормативным актам Российской Федерации, под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры[1].

В данном контексте, в нашей стране действует указ Президента РФ от 24 июля 2013 г. № Пр-1753 «Основы государственной политики Российской Федерации в области международной информационной безопасности на

[1] Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года: указ Президента РФ от 24.07.2013 № Пр-1753 п. 6. Доступ из справ.-правовой системы «Гарант».

период до 2020 года», определяющий основные угрозы в области международной информационной безопасности, цели, задачи и приоритетные направления государственной политики Российской Федерации в области международной информационной безопасности, а также механизмы их реализации[1].

Иным документом, затрагивающим аспекты рассматриваемой деятельности в нашей стране, является Доктрина информационной безопасности Российской Федерации, согласно которой одним из национальных интересов России в информационной сфере являются «…содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве[2]». Так в данном подзаконном акте отмечается, что «…отсутствуют международно-правовые нормы, регулирующие межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий[3]».

На международной арене Российская Федерация обращает внимание других государств на проблемы, возникающие в информационной сфере, в частности начиная с конца XX века, а именно с 1998 года, когда инициативно подняла данный вопрос на целенаправленное обсуждение в рамках ООН. В дальнейшем Россия неоднократно выдвигала различные предложения по организации и обеспечению международной информационной безопасности, рассмотрим, по нашему мнению, одни из важнейших из них.

В 1998 году Россия предложила США подписать заявление на уровне президентов[4]. Но имеющиеся противоречия между странами не позволили подписать данный документ, в свою очередь, некое взаимопонимание в области информационной безопасности была достигнута в «Совместном заявлении об общих вызовах безопасности на рубеже XXI века», подписанном президентами США и России в сентябре 1998 года[5].

12 мая 1999 года, Российской Федерацией предложен документ «Принципы, касающиеся международной информационной безопасности»,

---

1 Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года: указ Президента РФ от 24.07.2013 № Пр-1753 п. 6. Доступ из справ.-правовой системы «Гарант».

2 Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646 п. «д» ч. 8. Доступ из справ.-правовой системы «Гарант».

3 Там же. – Ч. 19.

4 Ромашкина Н.П. Проблемы международной информационной безопасности: компромисс между Россией и Западом? / Н.П. Ромашкина // Европейская безопасность: события, оценки, прогнозы. – 2016. – № 41(57). – С. 10.

5 Угрозы информационной безопасности в кризисах и конфликтах XXI века / Под ред. А.В. Загоровского, Н.П. Ромашкиной. – М. : ИМЭМО РАН, 2015. – С. 106.

который включал некоторое количество терминов: информационное пространство, информационная война, международная информационная безопасность, международная информационная преступность, терроризм и иное. Таким образом, была предпринята попытка привести понятийный аппарат к обобщенному виду[1].

На 55-й сессии Генеральной Ассамблеи ООН (декабрь 1999 г.) нашей страной был предложен и в дальнейшем принят обновленный проект резолюции, в которой был впервые обозначен военный аспект проблемы международной информационной безопасности.

В январе 2002 года на 56-й сессии Генеральной Ассамблеи ООН принята резолюция A/RES/56/19 «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»[2]. Важнейшим шагом вперед в рассматриваемой сфере явилось принятие в том же году Россией и США резолюции «Создание глобальной киберкультуры»[3].

В 2004 году создана Группа экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Заседания данной группы проходили в 2004, 2009, 2012, 2014, 2016 и 2017 годах.

В 2005 году по решению Генеральной Ассамблеи ООН была создана рабочая Группа экспертов для изучения проблематики международной информационной безопасности. Не решенной проблемой оставалось не достаточное регулирование международным правом безопасности отношений от возможного использования информационных технологий в достижении военно-политических целей.

В сентябре 2011 года Россия представила проект «Конвенции об обеспечении международной информационной безопасности»[4]. Основные положения документа были сжаты в список из 23 основных вопросов, представляющих интерес для России в информационном пространстве. В проекте конвенции речь шла о предотвращении военных конфликтов в киберпространстве, борьбе с кибертерроризмом и кибермошенничеством. К ней присоединились Китай и Индия. Негативную реакцию конвенция вызвала у

---

[1] Проблемы информационной безопасности в международных военно-политических отношениях / Под ред. А.В. Загоровского, Н.П. Ромашкиной. – М. : ИМЭМО РАН, 2016. – С. 19.

[2] Резолюция Генеральной Ассамблеи ООН A/RES/56/19 // Сайт Организации Объединенных Наций. – URL : https://undocs.org/ru/A/RES/56/19 (дата обращения 20.11.2020).

[3] Информационное право и информационная безопасность : учебник для магистров и аспирантов : в 2 ч. / А.В. Морозов, Л.В. Филатова, Т.А. Полякова; ВГУЮ (РПА Минюста России). – М. : ВГУЮ (РПА Минюста России); Саратов : Ай Пи Эр Медиа, 2016. – Ч. 2. – Учебное электронное издание: 1 электрон. опт. диск (CD-ROM). – С. 561.

[4] Конвенция об обеспечении международной информационной безопасности (концепция). Министерство иностранных дел Российской Федерации. – URL : https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptlCkB6DZ29/content/id/191666 (дата обращения 26.11.2020).

США, Великобритании и некоторых стран Европейского Союза. Впоследствии многие из положений рассматриваемого проекта вошли в документы, принятые на уровне ОДКБ, СНГ и ШОС, однако широкой поддержки в общем конвенция не получила[1].

2015 год ознаменовался тем, что государствами-членами ШОС внесены в качестве основного документа ООН «Правила поведения в области обеспечения международной информационной безопасности»[2]. Представленный текст носит миротворческий характер, нацелен на предотвращение конфликтов в информационном пространстве.

В мае 2017 года Россия обнародовала проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности. Проект содержит основные принципы, на которых должна строиться борьба с киберпреступностью.

В декабре 2018 года Генеральная Ассамблея ООН резолюцией A/RES/73/27 «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» учредила Рабочую группу открытого состава, которая своей деятельностью должна вырабатывать нормы, правила и принципы ответственного поведения государств в сфере информатизации и телекоммуникаций в контексте международной безопасности, изучать применимость международного права в киберпространстве, существующие и потенциальные угрозы и иное[3]. В свою очередь, ранее действовавшая Группа правительственных экспертов прекратила свою работу ввиду ряда противоречий между участниками (США и их союзниками с одной стороны, и Россией, БРИКС и развивающимися странами – с другой). Несмотря на имеющиеся противоречия и разногласия, формирование Рабочей группы открытого состава – большой успех российской стороны, которая остаётся главным идеологом продвижения вопросов международной информационной безопасности[4].

---

1 Магдилова Л.В. Международные стандарты в области развития глобального информационного общества / Л.В. Магдилова, Ш.П. Ярбилов // Закон и право. – № 9. – 2019. – С. 187.

2 Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности». Министерство иностранных дел Российской Федерации. – URL : https://www.mid.ru/mezdunarodnaa-informacionnaabezopasnost//asset_publisher/UsCUTiw2pO53/content/id/916241?p-p_id=101_INSTANCE_Us CUTiw2pO53&_101_INSTANCE_Us CUTiw2pO53_languageld=ru_RU (дата обращения 26.11.2020).

3 Резолюция Генеральной Ассамблеи ООН A/RES/73/27. – URL : https://undocs.org/pdf?symbol=ru/A/RES/73/27 (дата обращения: 26.11.2020); Угрозы информационной безопасности … 2015. – 151 с.; *Верхелст Э.* Глобальное управление в сфере кибербезопасности : взгляд с позиции международного права и права Европейского Союза / Э. Верхелст, Я. Ваутерс // Вестник международных организаций: образование, наука, новая экономика. – 2020. – Вып. 15. – № 2. – С. 148–149.

4 Ющенко В.А. Международная информационная безопасность: общая характеристика и Российский подход к изучению / В.А. Ющенко // Русская политология. – 2018. – № 4(9). – С. 59.

Однако через несколько дней после предыдущего решения, Генеральная Ассамблея ООН приняла резолюцию, и ранее существовавшая Группа правительственных экспертов ООН, стала именоваться «Группой правительственных экспертов ООН на 2019–2021 гг. по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности», инициирована США. Данное объединение государств занимается нормами, правилами, принципами, мерами укрепления доверия и наращиванием потенциала, а также тем, как международное право может применяться в киберпространстве[1].

27 декабря 2019 года по указу Президента России в Министерстве иностранных дел Российской Федерации создан 42-й департамент международной информационной безопасности, который занимается вопросами международного сотрудничества в сфере информационной безопасности, противодействия неправомерному использованию информационно-телекоммуникационных технологий, а также использования и управления сетью Интернет[2]. Что свидетельствует о большом интересе и озабоченности России вопросами международной информационной безопасности, тем самым вновь созданный департамент может консолидировать и более эффективно координировать деятельность федеральных органов государственной власти по продвижению позиции нашего государства по важным аспектам международной информационной безопасности на международной арене и многосторонних форматах.

Помимо участия в работе ООН, Россия в рассматриваемой области, участвует в деятельности ее специализированных подразделений: Регионального содружества в области связи; Всемирной организации по интеллектуальной собственности; ООН по вопросам образования, науки и культуры (ЮНЭСКО); Международного союза электросвязи и других. Также является участником (членом, представителем и т. п.) других международных организаций: ШОС, БРИКС, ОДКБ, СНГ; на постоянной основе проводит двусторонние встречи с Белоруссией, Бразилией, Кубой, КНР, Индией и рядом арабских стран.

Как показывает наш анализ, интерес международного сообщества к проблемам международной информационной безопасности стал более активным и внимательным примерно с конца XX века – начала XXI века, это связанно с беспрецедентным ростом и засильем разнообразных информационных технологий (подвижной радиотелефонной связи, компьютерных устройств, информационных сетей и др.), их доступности для населения даже не самых обеспеченных стран, активизации случаев использования

---

[1] Верхелст Э. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права Европейского Союза / Э. Верхелст, Я. Ваутерс // Вестник международных организаций: образование, наука, новая экономика. – Вып. 15. – № 2. – 2020. – С. 148–149.

[2] Министерство иностранных дел Российской Федерации. – URL : https://www.mid.ru/about/structure/central_office (дата обращения 28.11.2020).

информационно-телекоммуникационных технологий в преступной деятельности трансграничного и трансконтинентального характера, разведывательными и иными службами государств в собственных интересах и не всегда мирных, и иные причины.

Российская Федерация на международной арене на постоянной основе прилагает серьёзные усилия по решению проблем международной информационной безопасности: внесла большой вклад в формирование терминологии, созданию и совершенствованию международно-правовых норм в рассматриваемой деятельности, активно участвует в работе организаций международного, межгосударственного, регионального и национального характера.

Шаповалова Я.В.,
кандидат юридических наук, доцент,
ООО «Юридическая
экспертная компания «Вектор»
г. Краснодар

СРЕДСТВА И СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОМ ПРОСТРАНСТВЕ

В первую очередь необходимо определиться со значением термина образовательное пространство, используемом в контексте данной работы, так как содержание этого понятия зачастую зависит от ракурса, под которым его рассматривают. Мы будем использовать здесь термин образовательное пространство как совокупность всех образовательных и воспитательных учреждений, научно-педагогических центров, правительственных и общественных организаций, реализующих образовательный процесс.

В условиях пандемии мы наблюдаем стремительное развитие инфокоммуникационных технологий и формирование новых способов обучения и обмена информацией по телекоммуникационным каналам, замещение прямого диалога между субъектами образовательного процесса на взаимодействие с текстом – все это решительно изменяет образовательное пространство. Вместе с тем информационные технологи привносят определенные риски в образовательную деятельность, которые необходимо учитывать, изучать и противостоять им, в случае негативных последствий. Образовательные учреждения выполняют в том числе и задачу подготовки специалистов, адаптированных к электронному делопроизводству, а также относятся к базовым организациям, где апробировалась система обработки персональной информации.

В рамках заданной темы ставилась цель определить правовую регламентацию обработки персональных данных в образовательном пространстве и проанализировать способы и средства их охраны и защиты. Охрана

персональной информации объединяет три аспекта правовой регламентации: юридический (например, определение понятий), технический (электронное обеспечение сбора и хранения информации) и делопроизводственный (организация процесса сбора и хранения персональных данных).

Обработка и защита персональных данных субъектов образовательного пространства регулируется целым перечнем законодательных актов. Так, правовые основы защиты персональных данных были закреплены в Конституции Российской Федерации (ст. 2, 23, 24, 45). Перечень персональных данных впервые был закреплен в Указе Президента РФ от 06 марта 1997 г.[1], в 2015 году Россия ратифицировала Конвенцию о защите физических лиц[2], в 2006 г. были приняты Закон о персональных данных[3] и Закон об информации, информационных технологиях и о защите информации[4], многочисленные подзаконные и ведомственные акты[5]. Таким образом, в России оформилась система нормативных актов, регулирующих отношения, возникающие при охране и защите персональных данных в образовательном процессе, однако некоторые проблемы, относящиеся к определению правовой сущности персональных данных и мерам их защиты имеют полемический характер, недостаточно эффективны.

Специфика учебных заведений требует обрабатывать личные данные не только обучаемых, но и их родителей, если учащиеся несовершеннолетние, а также персонала учебных заведений.

В образовательных учреждениях при разработке мероприятий по защите персональной информации юридическая работа заключается в разработке локальных актов, которые должны регламентировать организацию, юридическую, техническую часть деятельности с персональными данными (их обработка и хранение и т.д.), а также вопросы взаимодействия с надзорными органами. Разработка и принятие Положения о защите, хранении, обработке и передаче персональных данных – обязанность, которую необходимо выполнить оператору персональных данных (образовательной организации), отсутствие этого документа квалифицируется как прямое нарушение федеральных законов. При разработке локальных нормативных актов,

---

1 Собрание Законодательства Российской Федерации. 1997. № 10. Ст. 1127.

2 Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» //Собрание законодательства Российской Федерации. 2005. № 52 (Ч. 1). Ст. 5573.

3 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» //Собрание законодательства Российской Федерации. 2006. № 31 (Ч. 1). Ст. 3451.

4 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31 (Ч. 1). Ст. 3448.

5 Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» //Собрание законодательства Российской Федерации. 2012. № 45. Ст. 6257 и др.

регулирующих вопросы обработки, хранения и защиты персональных данных в учреждениях образования могут быть использованы примерные формы[1], однако при использовании подобных нормативно-методических документов по защите персональных данных необходимо иметь в виду, что регулирующими органами могут вноситься уточнения и разъяснения, которые должны своевременно приниматься к исполнению всеми операторами информационных систем, обрабатывающих персональные данные.

Методическую помощь образовательным организациям, не имеющим в штате необходимых специалистов, могут оказывать на договорных условиях организации, имеющие соответствующие лицензии. Такие организации вправе осуществлять консультирование при проведении сегментирования интегрированных информационных систем, определении состава и классификации информационных систем, обрабатывающих персональные данные; давать пояснения при формировании перечня организационно-технических мероприятий, необходимых для создания системы защиты информационных систем, обрабатывающих персональные данные; осуществлять аудит информационных систем персональных данных, подбор и установку необходимых технических средств защиты информации[2]. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия[3].

Обобщая средства и способы защиты персональных данных в образовательном учреждении перечислим основные моменты: при получении персональной информации необходимо получить письменное согласие от их собственника на обработку таких сведений, включая разрешение на передачу этих данных третьим лицам в рамках действующего законодательства и в объемах, необходимых для реализации рабочего процесса в образовательном учреждении; для хранения персональных данных должен быть приказ руководителя образовательной организации об ответственных лицах, которые будут иметь доступ к этим документам. Руководитель образовательного учреждения несет персональную ответственность за конфиденциальность данных, полученных для обработки в рамках трудовых

---

[1] Форма: Положение о защите, хранении, обработке и передаче персональных данных работников и обучающихся образовательной организации (Авторский материал - подготовлен для системы «КонсультантПлюс», 2020) //СПС «КонсультантПлюс».

[2] Письмо Рособразования от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных» // СПС «КонсультантПлюс».

[3] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» //Собрание законодательства Российской Федерации. 2012. № 45. Ст. 6257.

взаимоотношений. В его ведении должны находиться соответствующие журналы контрольного внутреннего и исходящего учета персональных данных, содержащие, помимо описи конфиденциальных документов, порядок их изъятия из хранилища и передачи в третьи руки. В число третьих лиц входят как представители государственных контрольно-надзорных органов, судебной системы, так и представители иных негосударственных структур. Контроль за выполнением требований по защите персональных данных при их обработке организуется и проводится образовательной организацией самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации не реже одного раза в три года.

Раздел 4

Актуальные проблемы методики преподавания в условиях информационного общества

Скидан М.Н.,
старший преподаватель
кафедры социально-гуманитарных
и естественнонаучных дисциплин,
СКФ ФГБОУВО «РГУП»
г. Краснодар

ПРЕПОДАВАНИЕ ФИЗИЧЕСКОЙ КУЛЬТУРЫ В ВУЗАХ В ФОРМАТЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Простыми словами дистанционное обучение – это обучение на расстоянии, при котором отсутствует прямой контакт учащихся с преподавателем, но учебный процесс не приостанавливается за счёт всемирной системы объединённых компьютерных сетей для хранения, переработки и передачи информационных данных. После того, как начался карантин, дистанционное обучение стало необходимой мерой по медицинским показателям. Такая система преподавания имеет свои как плюсы, так и минусы, хотя с самого начала, по мнению учащихся и преподавателей, она приносила лишь одни неудобства, ухудшала уровень дисциплины и успеваемости. Её преимущества балансируются с недостатками, что видно на лицо.

В первую очередь, дистанционное обучение (ДО) проявляется в гибкости, заключающейся в возможности выбирать время для обучения, то есть конструктивно планировать свой день, тем самым становясь самостоятельнее. Оно предоставляет возможность обучаться и работать в комфортной обстановке, удаленно находясь где угодно: дома, в городе или на даче.

Дистанционное обучение определяет актуальность зданий, получаемых на расстоянии. Это достигается благодаря возможности интернета в подборе яркого, красочного демонстрационного материала, использование видео- и аудиоконтента, что способствует не только удержанию внимания, но и развитию клипового мышления, мышления формирующегося через короткие яркие, красочные образы и послания, например, через ленту теленовостей, видеороликов, музыкальных сопровождений. Уровень актуальности также может быть увеличен доступностью учебных материалов, находящихся в онлайн-библиотеках.

Перечень недостатков также велик, как перечень преимуществ дистанционного обучения. К ним относятся, например, то, что обучение на

расстоянии конечно позволяет сэкономить время и денежные средства, но оно также ограничивает выбор, заключающегося в необходимости практического опыта, а не только теоретического, который способствует возникновению нехватки личного общения, ведь прямой физический и зрительный контакт с оппонентом является основным элементом взаимодействия индивида, личности с социумом, то есть с обществом и государством в целом.

Комфортная рабочая обстановка не всегда является преимуществом в дистанционном обучении, ведь находясь дома, студенты и преподаватели постоянно отвлекаются на домашние дела, позволяют себе часто расслабиться, отдохнуть, отложив работу на потом и, тем самым уменьшая эффективность работоспособности.

Указанные недостатки способствуют появлению необходимости у преподавателей работать с развитием мотивации у студентов, так как они теряют контроль, забывая о том, что им нужно выполнять домашнее задание, ходить на лекции, семинары, готовить устные ответы, изучать дополнительную литературу, улучшающие моторику и ораторские способности. У преподавателей в учебном процессе намного больше обязанностей: им приходится подготавливать учебные планы, контролировать их выполнение, пытаться подобрать способы предоставления информации студентам, ведь каждый индивидуален и у каждого по-своему может быть развито мышление, активность головного мозга, что усложняет задачу преподавателей.

Первоначальными задачами преподавателей являются мотивирование и вдохновение учащихся к изучению их предмета или, иными словами, учебной дисциплины, а затем поощрение за хорошо выполненную работу, труд или же за приложенные ими попытки к подготовке. Поощрение может выражаться по-разному, и даже тут преподавателю нужно определиться с видом и формой поощрения, чтобы не обделить других студентов и не посеять между ними коллективные конфликты. Например, поощрение может быть в виде благодарности, почётной грамоты, увеличения стипендии, проведения игровых, развлекательных мероприятий.

Сложнее всего бывает развить мотивацию у студентов к занятиям физичкой культурой на дистанционном обучении. В соответствии с государственным образовательным стандартом учебная дисциплина «Физическая культура» включена в программу обязательных гуманитарных дисциплин вуза, из чего следует, что данная дисциплина присутствует во всех учебных заведений, учреждениях. Значение данной дисциплины обусловлено поддержанием здоровья студентов, развитием основных (выносливость, сила, быстрота) и специфических (устойчивость к перегрузкам) физических качеств, укреплением воли и избавлением от лени. Для того, чтобы начать заниматься физической культурой, необходимо наличие такого компонента как мотивация. Возникновению мотивации способствуют цели человека,

определяющиеся желаниями, которыми могут быть: желание поддерживать стабильное состояние здоровья, желание привести свою фигуру в хорошую форму, бросить вредные привычки. Большая часть студентов не испытывает интереса к занятиям или не хочет заниматься вообще. Среди них доминирует низкий уровень грамотности о вопросах, касающихся здоровья, профилактики заболеваний. В связи с этим, главной задачей преподавателей является формирование у студентов желания заниматься физической культурой при нахождении на дистанционном обучении, путём подходящего разъяснения им значения физических упражнений, занятий и подготовки курса физических тренировок.

В современном вузе необходим поиск новых организационных форм, средств и методов, позволяющих более эффективно реализовывать должное направление. Решить эту проблему возможно с помощью компетентной организации учебного процесса по физической культуре, используя различные виды спорта и современные системы физических упражнений, учитывающих индивидуальность студента, его интересы и состояние здоровья. Также эту проблему можно решить путём применения к физическим тренировкам игровой и соревновательный методов, метода круговой тренировки, шире использовать музыкальное сопровождение, усилить творческую составляющую при организации занятий физической культурой. Но перед этим преподавателю надо найти общий язык со студентами, продумать моменты поощрения.

Таким образом, познание основ физического развития человека и физической подготовленности дают возможность студентам вуза более эффективно и качественно использовать методы и средства для самообразования и саморазвития. Успешное использование средств физической культуры и спорта в учебном процессе и дифференцированного контроля студентов за физической подготовленностью поможет им сохранить физическую работоспособность, сформирует способность к быстрой адаптации, ускорит процессы восстановления и реабилитации после физических и умственных нагрузок. У студентов формируется успешное выполнение учебных требований и улучшается успеваемость по другим дисциплинам. Воспитывается высокая организованность и дисциплина в учебе, быту, отдыхе. Физическая подготовленность способствует рациональному использованию свободного времени для личностного и профессионального развития будущего специалиста.

Черепова А.О.,
преподаватель кафедры гуманитарных
и социально-экономических дисциплин,
ЗСФ ФГБОУВО «РГУП»
г. Томск

К ВОПРОСУ МЕТОДИКИ ФОРМИРОВАНИЯ ЕСТЕСТВЕННОНАУЧНОГО МЫШЛЕНИЯ СТУДЕНТОВ ЮРИДИЧЕСКИХ СПЕЦИАЛЬНОСТЕЙ

Система профессионального образования в настоящее время предъявляет серьезные требования к подготовке высококвалифицированных выпускников, готовых решать сложные профессиональные задачи. В этом контексте перед современной системой образования встают новые цели, требующие новых методов обучения, обеспечивающих не только прямую передачу знаний и умений, а формирующих у молодого специалиста новые компетенции, обладающие свойством широкого переноса. Такие умения, будучи сформированными в процессе изучения общеобразовательных дисциплин, затем свободно используются студентами при изучении других предметов и в практической деятельности. Так, дисциплины естественнонаучного цикла, изучаемые на первом этапе среднего и высшего образования, позволяет преподавателю привлечь знания студентов из профилирующей предметной области. Такой метод прекрасно иллюстрирует изучаемый теоретический материал, формирует эрудицию, развивает рефлексивные умения студентов. Но основной ценностью интегрированного подхода к изучению естественных наук является приведение студента к пониманию универсальных научных принципов и к осознанию взаимосвязи изучаемых наук. Таким образом, одной из профессиональных компетенций современного юриста является способность и готовность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, использовать для их решения интегративное естественнонаучное мышление.

В современных условиях основная цель профессионального образования состоит в том, чтобы приучить выпускника думать самостоятельно, свободно распоряжаться научными знаниями, обосновывать свои взгляды, а не бездумно впитывать преподавательские поучения. Будущие студенты, пришедшие непосредственно со школьной скамьи, проходят длительный этап адаптации к принципиально новой для них форме обучения. Овладевая методами научного познания, учащиеся зачастую выбирают рационально-шаблонные подходы к решению тех или них задач. На начальном этапе эти «избитые» схемы еще работают, но на старших курсах мы можем столкнуться с проблемой неспособности студента видеть решаемую задачу широкомасштабно, учитывая взаимосвязи всех частей проблемы, не упуская возможных вариантов проработки того или иного вопроса.

Студенты факультета непрерывного образования, в подавляющем числе случаев, при подготовке к семинарам и контрольным заданиям используют материалы лекций и рекомендованные параграфы учебников. Алгоритм контрольных заданий (устных, либо письменных) заранее установлен, и студенты зачастую механически заучивают материал, не устанавливая логической цепочки изучаемого материала, теряя взаимосвязи и взаимодействия, существующие в единой картине мира. К тому же обучение студентов зачастую строится изолированно от других дисциплин профессиональной направленности. Общеобразовательные дисциплины, как правило, не рассматриваются в качестве базы для формирования умений и навыков в решении профессиональных задач. И этот факт является незаслуженно обойденным и в системе юридического образования. Установление такой, безусловно полезной, взаимосвязи: общеобразовательные – общепрофессиональные дисциплины дает прекрасную возможность формирования не частных, а общенаучных профессиональных навыков. Формирование таких компетенций мы видим, через организацию и проведение интегрированных занятий.

Конструкция интегрированного урока состоит в том, что выбираемая задача или проблема дискуссии, или ситуационная задача и т.п. должна быть пограничной относительно нескольких дисциплин.

Пример 1. Аральское море в СССР представляло собой до 60-х годов двадцатого столетия красивейший водоем, вмещающим тысячи кубометров чистейшей воды. Две питающие море-озеро артерии – река Амударья и река Сырдарья были перерезаны каналами отведения вод на орошаемые поля. В результате, спустя десяток лет, Аральское море начало стремительно высыхать, появилось масса экологических проблем, явившихся результатом бездумной деятельности человека.

Рекомендуемые вопросы:

1. Какие звенья цепи экосистемы были нарушены?
2. Какие возникли последствия?
3. Какие мероприятия по восстановлению разрушенной экосистемы возможно применить в данной ситуации?
4. Какие существуют источники охраны природных вод?

В качестве домашнего задания можно рекомендовать изучить данную проблему с биологической, экологической и юридической точки зрения, используя доступные литературные ресурсы. Полученные результаты обсудить на семинаре, используя методику «круглый стол». Таким образом студент учится анализировать конкретную ситуацию, включая интегративное мышление, охватывает несколько аспектов естественных наук, устанавливает взаимосвязи между изучаемыми дисциплинами приобретает полезные инструментарии для будущей профессиональной юридической деятельности.

Использование метода сравнения может быть представлено следующим примером:

Пример 2. Сравниваем традиционные и альтернативные источники энергии. Жизнь в потребительском обществе влечет к постоянному потреблению энергетических ресурсов одного или более регионов или же всей планеты. Как известно, потребление природных ресурсов и полезных ископаемых является крайне губительным для окружающей среды и непостоянным источником энергии. Большинством своим, это связано с исчерпыванием и не возобновлением таких ресурсов как нефть, каменный уголь и природный газ. Комплексная проблема будущей нехватки нефти как уникального природного сырья не относится к вопросам первостепенной важности в общественном сознании. В процессе эволюции, человечество также преуспело в процессе получения больших объемов энергии в результате расщепления атомов Урана до мельчайших частиц, но этот процесс является крайне опасным и ведет к необратимым последствиям.

Студентам предлагается продумать ответы на вопросы:

Что такое альтернативная энергия?

Какая доля альтернативных источников энергии в общем объеме вырабатываемой электроэнергии в мире?

Почему альтернативную энергетику не использовали раньше?

Почему растет интерес к альтернативным источника энергии?

Какие существуют законы и нормативные документы об охране природных источников энергии (общемировые, в России, в Томской области)?

Пример 3. Государственный природный заказник Ларинский находится в 100 км от города N, N-ской области. В результате несанкционированной деятельности туристической группы, которая оставила после своего пребывания непотушенный костер, произошло локальное возгорание. Пламя костра перекинулось на лесные массивы. Пожарным службам заказника удалось пресечь распространение пламени, но, в результате возгорания заказник потерял 1 га леса.

Студентам рекомендуется проанализировать ситуацию с нескольких позиции и разрешить поставленный вопрос: Какие последствия возникли в результате приведенного частного случая? Определить какие процессы иллюстрируют данный пример с точки зрения химии, физики, биологии, экологии, правоведения (с использованием соответствующих источников права).

Решение подобного вопроса возможно «обыграть» в форме деловой игры, которая являет собой метод активного обучения, столь востребованный в современном обучении в рамках ФГОС. Деловая игра может проходить как дискуссия, мозговой штурм, ролевой анализ ситуации.

На семинарах-диспутах по естественнонаучным дисциплинам возникает возможность всестороннего анализа и глобальных проблем человечества. Так, например, возможность обсудить глобальные экологические проблемы Арктики: изменение климата (причины) и таяние льдов (следствие), загрязнение вод Мирового океана стоками нефти и соединений органической химии, а также морским транспортом, изменения сред обитания

животных (вследствие косвенных антропогенных факторов) и цепь последствий и др.

В результате продумывания вопросов, учащийся видит проблему масштабно, может проследить цепочку событий и обосновать последствия вмешательства человека в природную среду. Может обосновать значимость применяемых мер, проанализировать схему мероприятий, направленных на восстановление разрушенной экосистемы, доказать необходимость применения юридических санкций, знакомится с юридической документацией. Помимо указанных действий, студент определяет значимость своей будущей профессии, которая играет огромную роль в решении серьезных экологических проблем человечества.

На занятиях по изучению дисциплин общеобразовательного цикла (естествознание, экология, география) могут быть предложены такие методы, как: деловая игра, аналитические задачи, нравственные дилеммы, научный диспут, критические оценки ситуаций и т.д., которые дают возможность рассматривать событие с точки зрения различных естественных наук, связывая их с будущей профессиональной деятельностью, пробовать стратегии решения поставленных проблем, приобрести опыт научного анализа ситуаций.

Современная жизнь предъявляет высокие требования к уровню профессиональной компетентности юриста. Планирование результата, поиск путей достижения этого результата, поиск идей, средств, приёмов исследования проблемы и её претворения в жизнь – те самые наиглавнейшие компетенции, которыми должен обладать современный юрист. Следовательно, будущий профессиональный юрист должен свободно распоряжаться научными знаниями, делать логические умозаключения, обосновывать свои взгляды и выводы.

Научное издание

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОГО И ПРАВОВОГО ПРОСТРАНСТВА В СОВРЕМЕННОМ МИРЕ

IV Международной Российско-Казахской научно-практической конференции
(10 декабря 2020 г.)

Сборник статей

Статьи публикуются в авторской редакции

Технический редактор – А.С. Семенов
Компьютерная верстка – М.Н. Гусева
Дизайн обложки – О.Я. Фоменко

Подписано в печать 22.02.2022
Бумага «Снегурочка»
Печ. л. 10,9
Усл. печ. л. 10,2
Уч.-изд. л. 9,2

Формат 60×84 $^{1}/_{16}$
Печать трафаретная
Изд. № 1228
Тираж 105 экз.
Заказ № 2340

ООО «Издательский Дом – Юг»
350010, г. Краснодар, ул. Зиповская 9, литер «Г», оф. 41/3
тел. +7(918) 41-50-571

e-mail: id.yug2016@gmail.com Сайт: http://id-yug.com