

**КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМ. АЛЬ-ФАРАБИ**  
**Юридический факультет**  
**Кафедра таможенного, финансового и экологического права**

**Согласовано**

На заседанииченого совета факультета  
Протокол № 10 от 07 июня 2023 года  
Председатель факультета  
И. Байдельдинов



**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ**

**98454**

**Нормативное регулирование финансово-цифровой среды.**  
**Образовательная программа «БВ04109 Цифровая экономика»**

Курс – 3

Семестр – 6

Кол-во кредитов – 5

Форма обучения: очная

Алматы, 2023

УМК дисциплины составлен к.ю.н., доцентом Аманжоловым Ж.М. на основании образовательной программы «БВ04109 - Цифровая экономика»

«01» 09 2023 протокол №1

Заведующий кафедрой  
д.ю.н., и.о.профессора



Г.А. Куналиева

**СИЛЛАБУС**  
**Весенний семестр 2023-2024 учебного года**  
**Образовательная программа «БВ04109 Цифровая экономика»**  
**3 курс, русское отделение**

ID и наименование дисциплины	Самостоятельная работа студента (СРС)	Кол-во кредитов			Общее кол-во кредитов	Самостоятельная работа студента под руководством преподавателя (СРСП)
		Лекции (Л)	Практ. занятия (ПЗ)	Лаб. занятия (ЛЗ)		
98454 Нормативное регулирование финансово-цифровой среды.	7	15	30	-	5	-
<b>АКАДЕМИЧЕСКАЯ ИНФОРМАЦИЯ О ДИСЦИПЛИНЕ</b>						
Формат обучения	Цикл, компонент	Типы лекций	Типы практических занятий	Форма и платформа итогового контроля		
Офлайн	ПД компонент по выбору	Классический обзор, аналитическая лекция	логические задания, дискуссий, составление научных проектов, тестовые задания	Устно офлайн		
<b>Лектор - (ы)</b>	Аманжолов Жайсанбек Меирбекулы					
<b>e-mail:</b>	zh.amanzholov@mail.ru					
<b>Телефон:</b>	87784691621					
<b>Ассистент- (ы)</b>						
<b>e-mail:</b>						
<b>Телефон:</b>						
<b>АКАДЕМИЧЕСКАЯ ПРЕЗЕНТАЦИЯ ДИСЦИПЛИНЫ</b>						
Цель дисциплины	Ожидаемые результаты обучения (РО)*			Индикаторы достижения РО (ИД)		
Целью дисциплины является формирование у студентов достаточного уровня знаний о правовом регулировании финансово-цифровой среды, приобретение умений использовать эти знания в профессиональной деятельности и формирование необходимых компетенций. В результате изучения дисциплины студенты будут: - владеть основными правовыми положениями о сущности финансово-цифровой среды и основных процессах, характеризующих данный тип категории; - обладать возможностями	1. Разъяснение теоретических и практических основ нормативно-правового регулирования финансово-цифровой среды.			1.1 Доказывает особенности правового регулирования финансово-цифровой среды государства. 1.2 Умеет анализировать предмет и систему, методы, принципы регулирования финансово-цифровой среды. 1.3 Определяет место и роль нормативного регулирования финансово-цифровой среды в системе права РК. 1.4 Умеет анализировать финансово-правовые нормы и отношения в рассматриваемой сфере.		
	2. Исследование особенностей правовых режимов использования цифровых технологий.			2.1 Знает основные законодательные и нормативные документы, регулирующие деятельность в финансово-цифровой среде. 2.2 . Анализирует особенности правовых режимов использования цифровых технологий.		

<p>современных справочных информационных правовых систем;  - правильно ориентироваться в правовых нормах действующего законодательства РК и адекватно его применять в конкретных практических ситуациях в финансово-цифровой среде;  - применять теоретические правовые знания в практической деятельности, составляющих основу правового регулирования финансово-цифровой среды.</p>		<p>2.3 . Умеет практически применять законодательные и нормативные документы.</p>
	<p>3. Формирование представления об организации контрольно-надзорной деятельности в финансово-цифровой среде.</p>	<p>3.1 Выявляет и анализирует возможности и последствия действий в финансово-цифровой среде.</p> <p>3.2 Владеет навыками оценки рисков в финансово-цифровой среде.</p> <p>3.3 Владеет навыками взаимодействия с контрольнонадзорными органами, регулирующими деятельность в финансово-цифровой среде.</p>
	<p>4. Изучение системы государственного регулирования финансово-цифровой среды и знакомство с государственными программами стратегического развития в сфере цифровых технологий.</p>	<p>4.1 Знает особенности государственного регулирования финансово-цифровой среды.</p> <p>4.2 Владеет навыками работы с нормативными документами.</p> <p>4.3 Может разрабатывать документацию организации с использованием законодательно-нормативных документов.</p>
	<p>5. Ознакомление с ответственностью за неправомерные действия в цифровой среде; –знакомство с методами противодействия и нейтрализации неправомерных действий в цифровой среде; изучение основных принципов и методов обеспечения цифровой безопасности; рассмотрение правовых основ обеспечения и защиты прав</p>	<p>5.1 Различает виды ответственности за неправомерные действия в финансово-цифровой среде.</p> <p>5.2 Умеет использовать методы противодействия и</p>

	в цифровой среде и основных направлений цифровой криминалистики.	<p>нейтрализации правонарушений в финансово-цифровой среде;</p> <p>5.3 Использует Законодательно-нормативные документы для обеспечения и защиты прав в финансово-цифровой среде.</p> <p>5.4 Классифицирует компьютерные преступления и основные направления цифровой криминалистики.</p>
<b>Пререквизиты</b>	93980 Актуальные проблемы участия Республики Казахстан в международных финансовых институтах; 67774 Современные тенденции и проблемы науки уголовного права; 93970 Проблемы становления и развития системы конституционализма в РК	
<b>Постреквизиты</b>	90043 Публикация в научном журнале/ материалах научно-практической конференции; 86183 Научный семинар.	
<b>Учебные ресурсы</b>	<p><b>Литература:</b></p> <p><b>Основная:</b></p> <ol style="list-style-type: none"> <li>1. Цифровая экономика. Учебное пособие/ М.М. Ковалев, Г.Г. Головенчик. – Минск: Изд. центр БГУ, 2018. – 328 с.</li> <li>2. Кулумбетова Д.Б., Маулина Н.Х., Асанова А.Б. Цифровая трансформация казахстанского банковского сектора на современном этапе развития //Научный вестник: Финансы, банки, инвестиции № 3. 2021.</li> <li>3. Касенова Г.Е Современные финансовые услуги банков: учебное пособие /Казак Университеті- Алматы, 2021, 264с.</li> <li>4. Глоссарий по цифровым финансовым услугам. Совместная публикация Всемирного почтового союза и Международного союза электросвязи. 2017 // <a href="https://creativecommons.org/licenses/by-nc-sa/4.0/">https://creativecommons.org/licenses/by-nc-sa/4.0/</a></li> <li>5. Цифровая трансформация финансовых услуг: модели развития и стратегии для участников отрасли. SKOLKOVO Business School – Ernst &amp; YoungInstitute for Emerging Market Studies (IEMS) // <a href="https://www.skolkovo.ru">https://www.skolkovo.ru</a>.</li> <li>6. Новикова Е.А Цифровизация финансового сектора: новые инструменты и перспективы их использования: Материалы конференции «Право, экономика и управление: от теории к практике». Чебоксары, 2020г.</li> <li>7. Касенова Г.Е Финансовые риски: учебное пособие /Казак Университеті- Алматы, 2020, 264с.</li> <li>8. Государственная программа "Цифровой Казахстан" от 12 декабря 2017 года // <a href="https://adilet.zan.kz/rus/docs/P1700000827">https://adilet.zan.kz/rus/docs/P1700000827</a></li> </ol> <p><b>Дополнительная:</b></p> <ol style="list-style-type: none"> <li>1. Закон Республики Казахстан «О введении национальной валюты Республики Казахстан» от 12 ноября 1993г. // <a href="https://online.zakon.kz">https://online.zakon.kz</a></li> <li>2. Закон Республики Казахстан «О Национальном Банке Республики Казахстан». от 30 марта 1995 № 2155 (с доп.и изм. 03.03.2023г.) // <a href="https://online.zakon.kz">https://online.zakon.kz</a></li> <li>3. Закон Республики Казахстан «О банках и банковской деятельности в Республики Казахстан» от 31августа 1995. № 2444 (с доп.и изм. 03.03.2023г.). // <a href="https://online.zakon.kz">https://online.zakon.kz</a></li> <li>4. Закон Республики Казахстан от 4 июля 2003 года № 474-ІІ «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» (с доп.и изм. по состоянию на 12.09.2022 г.)</li> <li>5. Закон РК от 24 мая 2021 года № 43-VІІ «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам регулирования банковской, микрофинансовой и коллекторской деятельности в РК», (с изм. и доп. по состоянию на 03.03.2023 г.) // <a href="https://online.zakon.kz">https://online.zakon.kz</a></li> <li>6. Концепция развития Open API и Open Banking в Республике Казахстан на 2023–2025 годы // <a href="https://www.nationalbank.kz/">https://www.nationalbank.kz/</a></li> <li>7. Бюро национальной статистики. Информационный бюллетень. Проект Kazstat // <a href="https://new.stat.gov.kz/ru/">https://new.stat.gov.kz/ru/</a>.</li> <li>8. Концепции развития Open API и Open Banking// <a href="https://www.nationalbank.kz/">https://www.nationalbank.kz/</a></li> <li>9. Исследования Международного финансового центра «Астана» // <a href="https://aifc.kz/ru/">https://aifc.kz/ru/</a></li> </ol>	

	<p>10. Краткий отчет Mobile banking rank Казахстан 2022 // <a href="https://markswebb.ru/report/mobile-banking-rank-kz-2022/">https://markswebb.ru/report/mobile-banking-rank-kz-2022/</a></p> <p>11. Концепция развития финансового сектора Республики Казахстан до 2030 года от 26 сентября 2022 года // <a href="https://adilet.zan.kz/rus/docs/U2200001021">https://adilet.zan.kz/rus/docs/U2200001021</a></p> <p><b>Интернет-ресурсы:</b></p> <ol style="list-style-type: none"> <li>1. Официальный сайт НБРК // <a href="http://www.nationalbank.kz">http://www.nationalbank.kz</a></li> <li>2. Официальный сайт Агентства РК по регулированию и развитию финансового рынка // <a href="https://www.gov.kz">https://www.gov.kz</a></li> <li>3. Официальный сайт Казахстанской фондовой биржи KASE // <a href="http://www.kase.kz">http://www.kase.kz</a></li> <li>4. Аналитические дэшборды // <a href="http://Ranking.kz">Ranking.kz</a></li> <li>5. Аналитический портал // <a href="https://kapital.kz/finance">https://kapital.kz/finance</a></li> </ol>
--	--

<p><b>Академическая политика дисциплины</b></p>	<p>Академическая политика дисциплины определяется Академической политикой и Политикой академической честности КазНУ имени аль-Фараби.</p> <p>Документы доступны на главной странице ИС Univer.</p> <p><b>Интеграция науки и образования.</b> Научно-исследовательская работа студентов, докторантов – это углубление учебного процесса. Она организуется непосредственно на кафедрах, в лабораториях, научных и проектных подразделениях университета, в студенческих научно-технических объединениях. Самостоятельная работа обучающихся на всех уровнях образования направлена на развитие исследовательских навыков и компетенций на основе получения нового знания с применением современных научно-исследовательских и информационных технологий. Преподаватель исследовательского университета интегрирует результаты научной деятельности в тематику лекций и семинарских (практических) занятий, лабораторных занятий и в задания СРСП, СРС, которые отражаются в силлабусе и отвечают за актуальность тематик учебных занятий и заданий.</p> <p><b>Посещаемость.</b> Дедлайн каждого задания указан в календаре (графике) реализации содержания дисциплины. Несоблюдение дедлайнов приводит к потере баллов.</p> <p><b>Академическая честность.</b> Практические/лабораторные занятия, СРС развивают у обучающегося самостоятельность, критическое мышление, креативность. Недопустимы плагиат, подлог, использование шпаргалок, списывание на всех этапах выполнения заданий. Соблюдение академической честности в период теоретического обучения и на экзаменах помимо основных политик регламентируют «Правила проведения итогового контроля», «Инструкции для проведения итогового контроля осеннего/весеннего семестра текущего учебного года», «Положение о проверке текстовых документов обучающихся на наличие заимствований».</p> <p>Документы доступны на главной странице ИС Univer.</p> <p><b>Основные принципы инклюзивного образования.</b></p> <p>Образовательная среда университета задумана как безопасное место, где всегда присутствуют поддержка и равное отношение со стороны преподавателя ко всем обучающимся и обучающимся друг к другу независимо от гендерной, расовой/этнической принадлежности, религиозных убеждений, социально-экономического статуса, физического здоровья студента и др. Все люди нуждаются в поддержке и дружбе ровесников и сокурсников. Для всех студентов достижение прогресса скорее в том, что они могут делать, чем в том, что не могут. Разнообразие усиливает все стороны жизни. Все обучающиеся, особенно с ограниченными возможностями, могут получать консультативную помощь по телефону 87010555110 / e-mail <a href="mailto:kuanalieva.guldanakz@mail.ru">kuanalieva.guldanakz@mail.ru</a></p> <p><b>Интеграция МООС (massive open online course).</b> В случае интеграции МООС в дисциплину, всем обучающимся необходимо зарегистрироваться на МООС. Сроки прохождения модулей МООС должны неукоснительно соблюдаться в соответствии с графиком изучения дисциплины.</p> <p><b>ВНИМАНИЕ!</b> Дедлайн каждого задания указан в календаре (графике) реализации содержания дисциплины, а также в МООС. Несоблюдение дедлайнов приводит к потере баллов.</p>
---	--

**ИНФОРМАЦИЯ О ПРЕПОДАВАНИИ, ОБУЧЕНИИ И ОЦЕНИВАНИИ**

<b>Балльно-рейтинговая буквенная система оценки учета учебных достижений</b>			<b>Методы оценивания</b>
<b>Оценка</b>	<b>Цифровой эквивалент баллов</b>	<b>Баллы, % содержание</b>	<b>Оценка по традиционной системе</b>
А	4,0	95-100	Отлично
<b>Критериальное оценивание</b> – процесс соотнесения реально достигнутых результатов обучения с ожидаемыми результатами обучения на основе четко			

A-	3,67	90-94	Хорошо	выработанных критериев. Основано на формативном и суммативном оценивании.	
B+	3,33	85-89		<b>Формативное оценивание</b> – вид оценивания, который проводится в ходе повседневной учебной деятельности. Является текущим показателем успеваемости. Обеспечивает оперативную взаимосвязь между обучающимся и преподавателем. Позволяет определить возможности обучающегося, выявить трудности, помочь в достижении наилучших результатов, своевременно корректировать преподавателю образовательный процесс. Оценивается выполнение заданий, активность работы в аудитории во время лекций, семинаров, практических занятий (дискуссии, викторины, дебаты, круглые столы, лабораторные работы и т. д.). Оцениваются приобретенные знания и компетенции.	
B	3,0	80-84		<b>Суммативное оценивание</b> – вид оценивания, который проводится по завершению изучения раздела в соответствии с программой дисциплины. Проводится 3-4 раза за семестр при выполнении СРМ. Это оценивание освоения ожидаемых результатов обучения в соотнесенности с дескрипторами. Позволяет определять и фиксировать уровень освоения дисциплины за определенный период. Оцениваются результаты обучения.	
B-	2,67	75-79		<b>Формативное и суммативное оценивание</b>	<b>Баллы % содержание</b>
C+	2,33	70-74		Активность на лекциях	5
C	2,0	65-69		Работа на практических занятиях	25
C-	1,67	60-64		Самостоятельная работа	30
D+	1,33	55-59	Проектная и творческая деятельность	0	
D	1,0	50-54	Итоговый контроль (экзамен)	40	
FX	0,5	25-49	ИТОГО	100	
F	0	0-24	Неудовлетворительно		

**Календарь (график) реализации содержания дисциплины. Методы преподавания и обучения.**

Неделя	Название темы	Кол-во часов	Макс. балл
<b>МОДУЛЬ 1 Предпосылки формирования и направления развития финансово-цифровой среды</b>			
1	<b>Л 1.</b> Введение в дисциплину. Понятие, цель, задачи финансово-цифровой среды	2	1
	<b>СЗ 1.</b> Юридические аспекты формирования и развития финансово-цифровой среды	4	7
2	<b>Л 2.</b> Тенденции развития права и правовое регулирование отношений в финансово-цифровой среде.	2	1
	<b>СЗ 2.</b> Объекты интеллектуальной собственности, используемые в цифровой экономике. Виды интеллектуальных прав, используемых в отношении по созданию и распространению информации в цифровой среде. Объекты интеллектуальных прав, охраняемые свидетельствами. Правовое регулирование отношений в цифровой среде.	4	7
	<b>СРСП 1.</b> Консультации по выполнению <b>СРС 1.</b>		
3	<b>Л 3.</b> Гражданско-правовое регулирование отношений при создании и распространении информации в Интернете. Исключительные права в цифровой сфере: объекты, границы, пределы осуществления.	2	1
	<b>СЗ 3.</b> Государственная программа «Цифровой Казахстан». Виды информации, распространяемые в Интернете. Информация, которая запрещена для распространения в Интернете. Документы, регулирующие распространение информации в цифровой среде. Понятие и виды исключительных прав.	4	7

	<b>СРС 1.</b> Тема: Исключительные права в цифровой среде: охрана и защита. (презентация).		20
4	<b>Л 4.</b> Основы нормативно-правового регулирования в сфере информационных технологий: технологии искусственного интеллекта, правовой режим нейросетей.	2	1
	<b>СЗ 4.</b> Документы, регулирующие использование технологии искусственного Интеллекта. Виды искусственного интеллекта и основные проблемы правового регулирования некоторых направлений. Риски при использовании технологии искусственного интеллекта. Нейросети: понятие, классификация и правовое регулирование.	4	7
5	<b>Л 5.</b> Правовое регулирование в сфере сбора, передачи, хранения, обработки, доступа к информации и обработки персональных данных.	2	1
	<b>СЗ 5.</b> Персональные данные: определение, виды, правовые основания обработки персональных данных. Конфиденциальность информации: понятие, особенности регулирования, правила работы. Основные направления развития законодательства в сфере сбора, передачи, хранения, обработки и доступа к информации. Законодательство с сфере регулирования общественных отношений, связанных с обработкой персональных данных. Организации, регулирующие деятельность в сфере сбора, передачи, хранения, обработки и доступа к информации. Обезличивание персональных данных. Законодательство, устанавливающее режимы различных видов тайн ответственность за неправомерные действия в сфере сбора, передачи, хранения, обработки, доступа к информации и обработки персональных данных.	4	7
<b>МОДУЛЬ 2 Государственное регулирование в условиях финансово-цифровой среды</b>			
6	<b>Л 6.</b> Понятие и основные направления государственного регулирования цифровой экономики. Правовые условия для формирования единой финансово-цифровой среды доверия	2	1
	<b>СЗ 6.</b> Методы противодействия коррупции в условиях цифровой среды. Инструменты государственного регулирования. Формы государственной поддержки научной и инновационной деятельности. Структура механизма государственного регулирования процессов цифровизации в РК	4	7
	<b>СРСП 2.</b> Консультации по выполнению <b>СРС 2.</b>		
7	<b>Л 7.</b> Информационная инфраструктура и безопасность	2	1
	<b>СЗ 7.</b> Создание глобальной конкурентоспособной инфраструктуры передачи, обработки и хранения данных. Внедрение цифровых технологий в строительстве и управлении городским хозяйством «Умный город». Риски в сфере информационной безопасности и пути их преодоления (повышение уровня защищенности личности, информационной безопасности и устойчивости сетей общего пользования; создание новых сервисов (услуг) для граждан, гарантирующих защиту их персональных данных; профилактика и выявление правонарушений с использованием информационных технологий, разработка новых механизмов поддержки отечественных разработчиков программного обеспечения и компьютерного оборудования в сфере информационной безопасности).	4	8
	<b>СРС 2</b> (форма дебаты). Тема: Ответственность за неправомерные действия при разработке и использовании технологии искусственного интеллекта.		23
<b>Рубежный контроль 1</b>			100
8	<b>Л 8.</b> Цифровые технологии и право	2	1
	<b>СЗ 8.</b> Понятие и свойства сквозных цифровых технологий. Правовые предпосылки для развития приоритетных сквозных цифровых технологии (большие данные, технологии распределенного реестра, квантовые технологии, новые производственные технологии, промышленный интернет, робототехника и сенсорики, технологии беспроводной связи, виртуальная и дополненная реальность). Создание сквозных цифровых технологий (преимущественно на основе отечественных разработок) как одна из стратегических задач развития РК на период до 2025 года. Отраслевое регулирование правоотношений в сфере робототехники.	4	6
9	<b>Л 9.</b> Электронный бюджет. Понятие, правовой статус и порядок функционирования.	2	1
	<b>СЗ 9.</b> Электронный и цифровой бюджет, особенности формирования. Проектное бюджетирование как метод повышения эффективности государственных и местных расходов. Анализ процессов планирования и исполнения бюджета, процессы управления закупками, процессы сбора и анализа показателей социально-экономического развития региона.	4	6
	<b>СРСП 3.</b> Обсуждение актуальных вопросов дальнейших тенденций развития финансово-цифровой среды по Посланию Президента РК народу Казахстана (презентация).		15

10	Л 10. Организация финансового контроля в условиях цифровизации финансовых правоотношений.	2	1
	СЗ 10. Особенности организации финансового контроля с использованием современных информационно-коммуникационных средств. Налоговый мониторинг как одна из форм финансового контроля. Понятие цифровых правоотношений, контроль за соблюдением прав и законных интересов их субъектов. Контроль в сфере закупок для государственных и местных нужд с использованием единой информационной системы в сфере закупок.	4	6
	СРСП 4. Консультации по выполнению СРС 3		
<b>МОДУЛЬ 3 Особенности правового регулирования финансово-цифровой среды</b>			
11	Л 11. Цифровая форма платежных средств и государственный финансовый контроль в цифровой среде. Особенности использования криптовалют.	2	1
	СЗ 11. Денежные элементы цифровой экономики. Цифровые валюты в альтернативных платежных системах. Основные направления регулирования в сфере обращения цифровых финансовых активов и цифровой валюты. Цифровая форма законных платежных средств. Понятие и особенности использования криптовалют. Ответственность за неправомерные действия в сфере обращения цифровых финансовых активов и цифровой валюты.	4	6
	СРС 3. Тема: Вопросы правового регулирования налоговой службы Республики Казахстан. Виды налогов. Анализ налогового законодательства (реферат).		12
12	Л 12. Особенности договорного регулирования в условиях цифровой экономики	2	1
	СЗ 12. Понятие и система договоров в сфере цифровой экономики. Трансформация договорного права в условиях цифровой экономики. Технология блокчейн. Особенности заключения и исполнения договоров в цифровой среде. Договоры по созданию объекта инновации. Договоры по передаче в пользования объектов инновационной деятельности. Организационные договоры.	4	6
	СРСП 5. Консультации по выполнению СРС 4		
13	Л 13. Трудовые отношения в финансово-цифровой среде. Особенности использования смарт-контрактов. Проблемы ведения электронного документооборота.	2	1
	СЗ 13. Особенности правового режима электронной цифровой подписи. Правовые основы введения электронных трудовых книжек. Применение смарт-контрактов и возможности правового регулирования их применения в финансово-цифровой среде. Право на забвение.	4	6
	СРС 4. Тема: Развитие Open API, Open Banking и экосистемы цифровых финансовых сервисов в Республике Казахстан (презентация).		15
14	Л 14. Правовые основы обеспечения и защиты прав в финансово-цифровой среде. "Цифровая" криминалистика.	2	1
	СЗ 14. Трансформация судебной защиты прав в условиях цифровизации. Правовые условия судопроизводства и нотариата в цифровой среде. Создание и функционирование единой информационной системы нотариата. Основные направления развития законодательства об альтернативных механизмах онлайн урегулирования споров в цифровой среде. Правовые условия процедуры медиации. Применение «цифровой» криминалистики.	4	6
15	Л 15. Уголовно-правовая охрана отношений, возникающих в связи с развитием финансово-цифровой среды.	2	1
	СЗ 15. Классификация преступлений с использованием цифровых технологий. Способы защиты от уголовно-правовых рисков для граждан и организаций. Основные угрозы в цифровой сфере. Ответственность за правонарушения, связанные с использованием цифровых технологий. Превентивные меры в борьбе с уголовными преступлениями.	4	8
	СРСП 6. Консультации по экзаменам.		
<b>Рубежный контроль 2</b>			<b>100</b>
<b>Итоговый контроль (экзамен)</b>			<b>100</b>
<b>ИТОГО за дисциплину</b>			<b>100</b>

## РУБРИКАТОР СУММАТИВНОГО ОЦЕНИВАНИЯ КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Письменное задание. Тема: « Особенности организации финансового контроля с использованием современных информационно-коммуникационных средств. Налоговый мониторинг как одна из форм финансового контроля. Понятие цифровых правоотношений, контроль за соблюдением прав и законных интересов их субъектов. Контроль в сфере закупок для государственных и местных нужд с использованием единой информационной системы в сфере закупок.» (РК 25% из 100% )

Критерий	«Отлично» 20-25 %	«Хорошо» 15-20%	«Удовлетворительно» 10-15%	«Неудовлетворительно» 0-10%
<b>Понимание общей характеристики и видов финансово-правовой ответственности и финансовых правонарушений</b>	Глубокое понимание понятия и видов Особенности организации финансового контроля с использованием современных информационно-коммуникационных средств. Релевантные и уместные ссылки (цитаты) на первоисточники.	Понимает понятие и виды, а также особенности организации финансового контроля с использованием современных информационно-коммуникационных средств. Релевантные и уместные ссылки (цитаты) на первоисточники.	Ограниченное понимание понятия и видов, а также особенностей организации финансового контроля с использованием современных информационно-коммуникационных средств. Релевантные и уместные ссылки (цитаты) на первоисточники.	Поверхностное понимание/ непонимание понятия и видов, а также особенности организации финансового контроля с использованием современных информационно-коммуникационных средств. Соответствующие и уместные ссылки (цитаты) на первоисточники не приводятся.
<b>Понимание основных проблем финансовых правонарушений</b>	Очень хорошо связывает налоговый мониторинг как одну из форм финансового контроля. Идеальное обоснование аргументов фактами эмпирического исследования (например, на основе сравнительного правового или статистического анализа).	Связывает сравнение налоговый мониторинг как одну из форм финансового контроля. Подкрепляет аргументы фактами эмпирического исследования.	Связь в сравнении налогового мониторинга как одну из форм финансового контроля, ограничена. Ограниченное использование доказательств эмпирических исследований.	В сравнении налогового мониторинга как одну из форм финансового контроля связь незначительна или отсутствует. Мало или совсем не используют эмпирические исследования.
<b>Политическое предложение или практические рекомендации / предложения</b>	Составление грамотных научных и/или практических рекомендаций и рекомендаций, связанных с цифровыми правоотношениями в Казахстане.	Предлагает некоторые соображения и/или практические рекомендации и предложения по улучшению цифровых правоотношений в Казахстане	Ограниченные мнения и практические рекомендации по улучшению цифровых правоотношений в Казахстане. Рекомендации не являются существенными, не основаны на тщательном анализе и поверхностны.	Соображений и практических рекомендаций, связанных с улучшению цифровых правоотношений в Казахстане, мало или совсем нет, или рекомендации очень низкого качества.
<b>Письмо, APA style</b>	Письмо демонстрирует ясность, точность и правильность. Строго придерживается APA style.	Письмо демонстрирует ясность, точность и правильность. В основном придерживается APA style.	В письме есть некоторые основные ошибки, и необходимо улучшить ясность. Есть ошибки в следовании APA style.	Непонятно, что написано, трудно не отставать от содержания. Есть много ошибок в следовании APA style.

Декан \_\_\_\_\_ Д.Л. Байдельдинов

Заведующий кафедрой \_\_\_\_\_ Г.А. Куаналиева

Лектор \_\_\_\_\_ Ж.М. Аманжолов



## **№ 1. Введение в дисциплину. Понятие, цель, задачи финансово-цифровой среды**

История формирования понятия «цифровая экономика», по мнению многих исследователей, восходит к американскому ученому из Массачусетского технологического института Николасу Негропonte, который в 1995 г. использовал метафору о переходе от обработки атомов, составляющих материю физических веществ, к обработке битов, составляющих материю программных кодов. Другие эксперты отмечают, что впервые термин «цифровая экономика». озвучил канадский ученый Дон Тапскотт в 1994 г. в книге, переведенной на русский язык под названием «Электронно-цифровое общество: Плюсы и минусы эпохи сетевого интеллекта». В ней Тапскотт, описывая признаки развитых стран, отмечает цифровую форму представления объектов, влияние информационных технологий на бизнес, систему государственного управления и дает цифровой экономике следующее определение – это экономика, базирующаяся на использовании информационных компьютерных технологий.

В 1999 г. Нил Лейн, помощник президента США по науке и технологиям, в статье «Развитие цифровой экономики в XXI веке» фактически первым дал определение рассматриваемого явления: «Цифровая экономика – это конвергенция компьютерных и коммуникационных технологий в сети Интернет и возникающий поток информации и технологий, которые стимулируют развитие электронной торговли и масштабные изменения в организационной структуре». В 2001 г. Томас Мезенбург выделил три основных компонента цифровой экономики, которые можно статистически оценить и измерить:

- поддерживающая инфраструктура (аппаратное и программное обеспечение, телекоммуникации, сети и др.);
- электронный бизнес (ведение хозяйственной деятельности и любых других бизнес-процессов через компьютерные сети);
- электронная торговля (дистрибуция товаров через интернет).

Несмотря на значительное число работ, до сих пор нет однозначного понимания того, что представляет собой цифровая экономика.

### **Сравнительный**

анализ многочисленных определений цифровой экономики позволяет классифицировать взгляды на это понятие, основанные на использовании следующих признаков:

- тип экономики, характеризующийся активным внедрением и практическим использованием цифровых технологий сбора, хранения, обработки,

преобразования и передачи информации во всех сферах человеческой деятельности;

- совокупность видов экономической деятельности как отрасли национальной экономики по производству и торговле цифровыми товарами и услугами в виртуальной среде;
- система социально-экономических и организационно-технических отношений, основанных на использовании цифровых информационно-телекоммуникационных технологий и сетей в режиме реального времени;
- сложное сочетание различных элементов (технических, инфраструктурных, организационных, программных, нормативных, законодательных и др.), представляющее собой дополнение к реальной экономике, ориентированное на устойчивое экономическое развитие

Суммируя различные подходы, можно дать следующее определение:

Цифровая экономика – это система социальных, культурных, экономических и технологических отношений между государством, бизнес-сообществом и гражданами, функционирующая в глобальном информационном пространстве, посредством широкого использования сетевых цифровых технологий генерирующая цифровые виды и формы производства и продвижения к потребителю продукции и услуг, которые приводят к непрерывным

инновационным изменениям методов управления и технологий в целях повышения эффективности социально-экономических процессов.

Выделяют три базовые составляющие цифровой экономики:

- инфраструктура, включающая аппаратные средства, программное обеспечение, телекоммуникации и т. д.;
- электронные деловые операции, охватывающие бизнес-процесс, реализуемые через компьютерные сети в рамках виртуальных взаимодействий

между субъектами виртуального рынка;

- электронная коммерция, включающая в себя все финансовые и торговые транзакции, осуществляемые при помощи компьютерных сетей, а также бизнес-процессы, связанные с проведением таких транзакций.

Выделяют следующие отрасли цифровой экономики:

- электронная торговля – новый вид безмагазинной торговли товарами и услугами, который осуществляется через интернет в виртуальных магазинах;
- электронный маркетинг – комплекс мероприятий маркетинга компании, связанный с применением электронных средств, объектом которого выступает информационно-аналитическая и экспертно-исследовательская деятельность предприятия (организации, компании);

□ электронный банкинг – технологии предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (т. е. без его

визита в банк), чаще всего с использованием компьютерных и телефонных сетей;

□ электронные страховые услуги – страховые услуги, которые можно заказать посредством сети Интернет.

Институциональная структура цифровой экономики состоит из трех основных элементов: институциональных субъектов, институциональных объектов и институционального механизма. Субъектами цифровой экономики являются:

□ цифровые транснациональные корпорации 6-го поколения (киберкорпорации), изменившие в последние годы с помощью сделок в интернете как

форму и эффективность мировых рынков, так и собственную структуру (Apple, Google, Hon Hai, IBM, Microsoft, Oracle, Samsung, Sony, LG, America Movil, Deutsche Telekom, NTT, Vodafone и др.);

□ «компании-единороги» – непубличные технологические компании, стоимость которых превышает 1 млрд долл. (ByteDance, Didi Chuxing, JUUL Labs, WeWork, Airbnb и др.);

□ иные субъекты хозяйствования, занятые производством ИКТ-товаров и услуг;

□ инновационные центры (Парк высоких технологий, Сколково);

□ лица, занятые на предприятиях цифровой сферы.

В институциональную структуру цифровой экономики Беларуси входят основные субъекты: Министерство связи и информатизации, Комиссия Совета

Министров по информатизации, ОАЦ при Президенте, Парк высоких технологий, стартапы последних лет, привлекшие многомиллионные инвестиции.

Объекты цифровой экономики функционируют комплексно в виде парадигмы «люди – бизнес – вещи», охватывают более 3000 видов деятельности и включают более 1800 видов криптовалют, огромный мир интернет-вещей, сетевую организацию финансирования (краудфандинг), биржи цифровых валют,

частный и публичный акционерный капитал и т. д.

В странах ЕАЭС объекты указаны в Стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до

---

2025 г., Цифровой повестке ЕАЭС до 2025 г. и др.

Одна из ключевых ролей государства в выстраивании институциональной системы состоит в создании институтов развития. Приоритетные задачи, которые предполагается решить с помощью данных институтов, следующие: развитие инфраструктуры (производственной, социальной и т. д.) и высокотехнологичных производств; стимулирование инноваций; наращивание темпов экономического роста в стране на долгосрочной основе и т. п. Институты развития цифровой экономики делятся на политические (институты власти), экономические, научные и общественные (социальные).

## **№ 2. Тенденции развития права и правовое регулирование отношений в финансово-цифровой среде.**

**В**лияние цифровизации на сферу правового регулирования — одна из наиболее актуальных и широко обсуждаемых в науке тем. Сказанное справедливо и для финансового права: современная финансово-правовая повестка связана с обсуждением правовой природы цифровых валют, целесообразности введения цифрового рубля, анализом особенностей правового регулирования цифровых финансовых активов, правового статуса операторов информационных систем, в которых происходит выпуск и обращение утилитарных цифровых прав, цифровых финансовых активов, цифровых валют и т.д. Не будет преувеличением сказать, что цифровизация затронула все без исключения институты финансового права, обусловив необходимость научного исследования и оценки происходящих процессов<sup>1</sup>.

В науке финансового права справедливо отмечается, что цифровизация ведет к транс-

совых активов) имеет своим следствием включение в предмет финансового права и новых видов общественных отношений. В то же время, как нам представляется, это справедливо и в отношении метода рассматриваемой отрасли права.

Следует отметить, что именно сочетание предмета и метода правового регулирования — основополагающий критерий, позволяющий выделить ту или иную совокупность правовых норм в качестве самостоятельной отрасли права. И если вопросам предмета

финансового права в свое время было уделено достаточно много внимания<sup>2</sup>, то метод данной отрасли зачастую воспринимается как само собой разумеющаяся категория, которая не требует дополнительных научных изысканий. Не в последнюю очередь это предопределяется тем фактом, что основным, материальным критерием выделения отрасли является предмет правового регулирования. На это, например, обращает внимание Т. Н. Радько, отмечающий, что метод — это «юридический, как бы дополнительный критерий»<sup>3</sup>.

<sup>1</sup> См.: Актуальные проблемы финансового права в условиях цифровизации экономики : монография / под ред. Е. Ю. Грачевой. М., 2020 ; Финансовое право в условиях развития цифровой экономики : монография / под ред. И. А. Цинделиани. М., 2019.

<sup>2</sup> См., например: *Грачева Е. Ю.* Финансовое право России: вчера и сегодня // Вестник Московского университета. Серия 11 : Право. 2012. № 3. С. 20–38 ; *Халфина Р. О.* К вопросу о предмете и системе советского финансового права // Вопросы советского административного и финансового права. М. : Издательство Академии наук СССР, 1952. С. 182–214 ; *Цинделиани И. А.* Предмет и система финансового права как отрасли права в советской финансово-правовой литературе // Финансовое право. 2011. № 12. С. 16–22 ; *Шохин С. О.* К вопросу о предмете и системе финансового права // Там же. 2019. № 2. С. 12–14 ; *Худяков А. И.* Дискуссионные вопросы предмета финансового права // Там же. 2009. № 3. С. 2–8 ; *Винницкий Д. В.* Предмет и система финансового права на современном этапе // Известия высших учебных заведений. Правоведение. 2002. № 5 (244). С. 30–42.

<sup>3</sup> *Радько Т. Н.* Теория государства и права : учебник. М., 2011. С. 397.

Среди работ, посвященных вопросам метода финансового права, в первую очередь следует назвать докторскую диссертацию И. В. Рукавишниковой<sup>4</sup> — фундаментальный и всеохватывающий характер данной работы привел к тому, что научная дискуссия по соответствующей теме была исчерпана на многие годы. В то же время представляется, что в свете изменений в механизме правового регулирования финансовых отношений, происходящих вследствие цифровизации экономики, теория метода финансового права может быть дополнена новыми выводами.

Традиционно в теории права под методом правового регулирования понимается совокупность приемов и способов, посредством которых нормы права воздействуют на участников общественных отношений. С. С. Алексеев выделяет четыре элемента метода правового регулирования. Данные элементы отражают характер:

- юридического положения субъектов<sup>5</sup>;
- юридических фактов;
- способов формирования содержания прав и обязанностей субъектов;
- юридических мер воздействия<sup>6</sup>.

В зависимости от соотношения всех перечисленных факторов, в теории права выделяют два метода правового воздействия — метод диспозитивного (децентрализованного) воздействия и метод императивного (централизованного) регулирования. Указанные методы отражаются в

сочетании конкретных способов правового регулирования, определяющих характер закрепленных в норме права предписаний. В теории права принято выделять три основных способа правового регулирования: дозволение (управомочивание), обвязывание, запрет<sup>7</sup>. Существует также мнение о возможности выделения иных, дополнительных способов правового регулиро-

вания, таких как рекомендации, согласования, договоры и т.д.<sup>8</sup>

Следует отметить, что с течением времени менялись и представления о методе финансового права. Так, в советский период развития финансово-правового учения признавалось, что «для финансового права характерен императивный метод». Вместе с тем изменение экономического базиса, связанного с переходом к рыночным отношениям, имело своим следствием пересмотр многих постулатов финансового права, в том числе воззрений на метод данной отрасли. Построение рыночных отношений привело к широкому распространению частных хозяйствующих субъектов в целом и специализированных участников финансового рынка в частности, а основным способом аккумуляции денежных средств в централизованные денежные фонды государства стал метод обязательных (в первую очередь

налоговых) платежей. Очевидно, что новая экономическая реальность потребовала и изменения подходов к правовому регулированию финансовых отношений.

Кроме того, отказ от административно-командной модели экономики привел к повышению роли финансового права в регулировании общественных отношений и, как следствие, к отказу от господствующего в правовой теории мнения о подчиненном характере финансового права по отношению к административному. Между тем общее сходство метода правового регулирования названных отраслей права обусловило необходимость выделения специфических черт финансово-правового подхода к правовому регулированию общественных отношений.

Так, разграничивая методы финансового и административного права, О. Н. Горбунова подчеркнула, что в финансовых отношениях пред-

<sup>4</sup> Рукавишников И. В. Метод финансового права : диссертация на соискание ученой степени кандидата юридических наук. Саратов, 2004. 521 с.

<sup>5</sup> Может характеризоваться равенством участников правоотношений или же состоянием власти и подчинения.

<sup>6</sup> Алексеев С. С. Собрание сочинений : в 10 т. [+ справоч. том]. М., 2010. Т. 3 : Проблемы теории права : курс лекций. С. 132.

<sup>7</sup> См.: Теория государства и права : учебник для вузов / под ред. В. М. Корельского, В. Д. Первалова. М., 2003. С. 268–269.

<sup>8</sup> Финансовое право : учебник / под ред. Н. И. Химичевой. М., 2009. С. 44.

писания, как правило, исходят от финансово-кредитных органов государства, которые не находятся в прямом подчинении других государственных органов, а взаимодействуют с ними по функциональной линии. Кроме того, автор отмечает, что регулированию финансовых отношений свойственно меньше усмотрения и произвола, нежели административному регулированию<sup>9</sup>. Данное замечание, однако, вызывает сомнения и во многом носит субъективный характер.

Представляется, что более точно специфику метода финансового права выразила Е. Ю. Грачева, указавшая на то, что субъекты, выдающие властные предписания (финансовые, налоговые и кредитные органы), и другие участники финансовых отношений в целом не находятся в административной зависимости<sup>10</sup>.

Н. И. Химичева также подчеркивала целый ряд специфических особенностей метода финансового права, которые проявляются:

- в содержании предписаний — они связаны с определением порядка и размера обязательных и добровольных платежей;
- в круге органов, уполномоченных на властные действия, — участники финансовых отношений находятся во взаимосвязи функций финансовой деятельности, что однако, не означает того, что

метод властных предписаний в рамках финансово-правового регулирования не затрагивает отношения вертикального соподчинения<sup>11</sup>.

И. В. Рукавишникова считает, что существенными признаками метода финансового права являются:

- имущественный аспект;
- преимущественная императивность правового регулирования;
- наличие менее жестких властно-подчиненных связей между субъектами финансовых отношений;

- допустимость определенной самостоятельности властвующих субъектов в выборе форм осуществления возложенных на них обязанностей;
- уникальное сочетание способов правового регулирования<sup>12</sup>.

Представляется что все вышеперечисленные особенности в полной мере характеризуют уникальность метода финансового права, позволяющего отграничить его от методов иных отраслей российского права.

Как было отмечено выше, методы финансово-правового регулирования в том числе предопределяются господствующей на том или ином этапе исторического развития экономическими отношениями. В настоящее время мы становимся свидетелями перехода к экономике нового типа — вследствие четвертой промышленной революции происходят коренные изменения в производственной сфере и сфере

услуг, на рынке труда, финансовых рынках, в системе государственного управления и т.д. Связано это с интенсивным внедрением во все сферы общественной жизни новых цифровых технологий. Указанный процесс принято именовать «цифровизацией».

Как справедливо отмечается в науке финансового права, «технологии являются инструментом, способствующим финансово-правовому регулированию, администрированию, финансовому контролю»<sup>13</sup>. Таким образом, очевидно влияние цифровизации на конкретные способы правового регулирования финансовых отношений.

По справедливому замечанию К. С. Бельского, «метод финансового права — единый метод правового регулирования, но со своими особенностями»<sup>14</sup>. Очевидно, что цифровизация не ведет к изменению основного метода финансового права: финансовые отношения

<sup>9</sup> Финансовое право : учебник / отв. ред. О. Н. Горбунова. М., 2006. С. 28–29.

<sup>10</sup> Финансовое право : учебник / отв. ред. Е. М. Ашмарина, С. О. Шохин. М., 2009. С. 47.

<sup>11</sup> Финансовое право : учебник / под ред. Н. И. Химичевой. С. 43–44.

<sup>12</sup> См.: Рукавишников И. В. Метод финансового права / отв. ред. Н. И. Химичева. М., 2011. С. 114–115.

<sup>13</sup> Ситник А. А. Правовое регулирование финансового контроля и надзора в сфере денежного обращения в Российской Федерации : диссертация юрид. наук. М., 2020. С. 18.

<sup>14</sup> Финансовое право : учебник для бакалавров / под ред. И. А. Цинделиани. М., 2016. С. 38.

регулируются в первую очередь методом власти и подчинения, при этом в установленных законом случаях допустимо ограниченное применение диспозитивного метода. Диспозитивность и императивность метода правового регулирования — достаточно общие категории, отражающие лишь концептуальный подход к модели правового регулирования, применяемой той или иной отраслью российского права. В то же время нельзя не признать, что сам по себе механизм правового регулирования претерпевает существенную трансформацию в условиях цифровизации экономики, поскольку меняются и конкретные способы правового и неправового воздействия на участников финансовых отношений. При этом следует обратить внимание на то, что метод, наряду с нормой права, правоотношением и правоприменительными актами, является одним из элементов механизма правового регулирования. По справедливому замечанию И. В. Рукавишниковой, метод «не обособлен от других элементов, а имманентно присущ каждому из них»<sup>15</sup>. Таким образом, метод раскрывает то, как механизм правового регулирования воздействует на общественные отношения.

Говоря непосредственно о влиянии цифровизации на метод финансового права, можно выделить следующие тенденции:

— *дополнение способов правового*

*регулируе- ния техническими средствами.* По мнению Т. Я. Хабриевой и Н. Н. Черногора, «...важный вопрос состоит в том, возникнут ли в связи с решением технологической задачи гибридные формы средств или способов правового регулирования, включающих как сугубо юридические, так и цифровые (например,

цифровой код) инструменты?»<sup>16</sup>. Широкое внедрение цифровых технологий влечет за собой ускорение не только передачи информации, но также и ее обработки, в том числе в автоматическом режиме. Цифровые технологии обеспечивают обработку огромных массивов информации, ее сопоставление, выявление фактов несоответствия установленным требованиям. Одним из наиболее ярких примеров является технология «АСК НДС-2»<sup>17</sup>, которая аккумулирует в себе информацию о плательщиках налога на добавленную стоимость, позволяя проследить процесс уплаты налога на всех стадиях реализации товаров, работ и услуг. В последнее время общепотребимым стал термин «финансовые технологии», который используется для обозначения, с одной стороны, различных методов и инструментов, способствующих

оказанию финансовых услуг, а с другой — отдельной, самостоятельной индустрии, занимающейся разработкой, внедрением и применением соответствующих инструментов. Регулирующие и надзорные технологии направлены на обеспечение соблюдения законодательных требований субъектами финансового рынка и их клиентами, упрощение обмена информацией, автоматизацию процесса анализа данных учета и отчетности по операциям с денежными средствами и иным имуществом. Внедрение «финансовых технологий» в целом ведет к повышению эффективности существующих способов правового регулирования;

– изменение «имущественного аспекта». По замечанию И. В. Рукавишниковой, «имущественный аспект метода правового регулиро-

<sup>15</sup> Рукавишникова И. В. Метод финансового права / отв. ред. Н. И. Химичева. С. 98.

<sup>16</sup> Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 97.

<sup>17</sup> Приказ ФНС России от 16.11.2016 № ММВ-7-12/622@ «О вводе в промышленную эксплуатацию модернизированного программного обеспечения подсистемы “Визуальный сетевой анализ объектов и связей” АИС “Налог-3” в части интеграции с программными средствами, обеспечивающими автоматизацию перекрестных проверок, реализующих функции камеральной налоговой проверки налоговых деклараций по НДС

на основе сведений из книг покупок, книг продаж и журналов учета выставленных и полученных счетов-фактур («АСК НДС-2»)» // Документ официально не опубликован. СПС «КонсультантПлюс».

вания финансовых отношений проявляется в его содержании»<sup>18</sup>, т.е. в направленности на поддержание стабильности финансовой деятельности. Вследствие изменения экономического базиса происходит и трансформация содержания метода финансового права — за счет расширения сферы правового регулирования, властные предписания государственных органов стали распространяться на принципиально новые сферы общественной жизни. Имущество сегодня — это не только традиционные объекты материального мира, но и не имеющие овеществленной формы электронно-цифровые данные. В частности, в 2019 г. Гражданский кодекс РФ был дополнен статьей 141.1, закрепляющей определение и порядок распоряжения цифровыми правами<sup>19</sup>. Так, в соответствии с п. 1 названной статьи цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. К указанным цифровым правам, в частности, относятся цифровые финансовые активы и

утилитарные цифровые права, которые по своей правовой природе являются финансовыми инструментами. В целях обеспечения стабильности соответствующих секторов финансового рынка были приняты федеральные законы, регулирующие обращение указанных объектов, а функции по надзору за деятельностью субъектов финансовых отношений, опосредующих операции с цифровыми финансовыми активами и утилитарными цифровыми правами, были возложены на Банк России. Таким образом, очевидно, что метод финансового права в настоящее время

стал применяться для регулирования новых секторов финансового рынка;

– *усиление диспозитивности.* Данное последствие цифровизации не является вполне очевидным. В то же время внедрение новейших цифровых технологий обеспечивает большую вариативность механизма правового регулирования финансовых отношений. Данный факт может быть проиллюстрирован целым рядом примеров. Так, в рамках налоговых правоотношений налогоплательщики и налоговые агенты должны предоставлять налоговые декларации, расчеты и иные документы. При этом по общему правилу<sup>20</sup> они могут выбирать форму предоставления таких сведений — на материальном носителе или в электронной форме. Кроме того, с 1 января 2019 г. физические лица, в том числе индивидуальные предприниматели, проживающие в ряде субъектов РФ, получили

право применять специальный налоговый режим «налог на профессиональный доход». Внедрение данного специального налогового режима во многом стало возможным именно благодаря развитию цифровых технологий. Например, статья 3 Федерального закона от 27.11.2018

№ 422-ФЗ<sup>21</sup> посвящена правовому регулированию порядка использования мобильного приложения «Мой налог», применяемого в целях администрирования в рамках рассматриваемого специального налогового режима;

– *трансформация основных способов правового регулирования:*

а) *обязывание.* Государство возлагает на субъектов финансовых отношений целый ряд обязанностей, связанных с использованием цифровых технологий. Так, в рамках контрольных правоотношений традиционно могут выбирать форму предоставления

<sup>18</sup> Рукавишников И. В. Метод финансового права / отв. ред. Н. И. Химичева. С. 105.

<sup>19</sup> Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124

части третьей Гражданского кодекса Российской Федерации» // СЗ РФ. 2019. № 12. Ст. 1224.

<sup>20</sup> В ряде случаев налогоплательщики обязаны предоставлять сведения исключительно в электронной форме (см.: п. 3 ст. 80 НК РФ).

- <sup>21</sup> Федеральный закон от 27.11.2018 № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима “Налог на профессиональный доход”» // СЗ РФ. 2018. № 49 (ч. I). Ст. 7494.

документов контролирующему лицу. В то же время на основании п. 1.5 Инструкции Банка России от 15.01.2020 № 202-И<sup>22</sup> Банк России и поднадзорные лица осуществляют обмен документами и информацией в связи с проведением проверок в первую очередь через личный кабинет участника информационного обмена и только при отсутствии такой возможности — на материальном носителе (на бумажном носителе и (или) на отчуждаемом (съёмном) машинном носителе информации);

б) запрет. Право — универсальный регулятор общественных отношений. Между тем в настоящее время признается факт того, что право ограничено в своих возможностях влияния на цифровую среду. Наиболее заметным образом это проявляется на примере цифровых (крипто-) валют. Понимая невозможность эффективного регулирования обращения указанных инструментов, государство, в частности, ввело запрет на принятие цифровых валют в качестве встречного предоставления за передаваемые ~~товары, выполняемые работы и оказываемые услуги~~<sup>23</sup>;

в) управомочивание. Цифровые технологии расширяют возможности по реализации и защите прав и законных интересов субъектов финансовых

правоотношений. Например, налогоплательщики на основании пп. 1 п. 1 ст. 21 НК РФ вправе получать по месту своего учета от налоговых органов бесплатную информацию (в том числе в письменной форме) о действующих налогах и сборах, налоговом законодательстве и т.д. При этом они могут реализовать данное право через свой личный кабинет; — *расширение возможностей регулирования трансграничных общественных отношений*. Как уже было отмечено, право хотя и

является универсальным, но тем не менее остается ограниченным инструментом воздействия на субъектов финансовых отношений. Юрисдикция государства (т.е. пределы его компетенции) очерчена границами даного публичного правового образования. Очевидно, что попытки одного государства регулировать общественные отношения на территории другого государства есть прямое вмешательство в суверенитет последнего. Подобные действия могут нести самые неблагоприятные последствия.

Между тем усиливающаяся глобализация обуславливает интенсификацию трансграничного движения денежных средств, что неизбежно влечет за собой ряд проблем, связанных в том числе с определением объема фискальных прав различных юрисдикций. Так, очевидно, что налогоплательщики стремятся перевести свой капитал в низконалоговые юрисдикции в целях сохранения причитающихся им

доходов. Между тем у государства, на территории которого даный доход извлекается, существует прямо противоположный интерес — обложить поступления налогоплательщика налогом на своей территории и пресечь факты незаконного вывода капитала за рубеж. Для определения полноты исполнения налогоплательщиком налоговой обязанности государству зачастую требуется информация, носящая закрытый характер (о зарубежных счетах, об офшорных операциях, объектах недвижимого имущества и т.д.). Помимо решения юридического вопроса о допустимости и основаниях предоставления такого рода информации, требуется также техническое обеспечение возможности передачи соответствующих сведений. В этих целях в конце 2017 г. в законодательство о налогах и сборах был введен разд. VII.1 «Выполнение международных договоров Российской Федерации по вопросам налогообложения и взаимной административ-

<sup>22</sup> Инструкция Банка России от 15.01.2020 № 202-И «О порядке проведения Банком России проверок поднадзорных лиц» // Вестник Банка России. 2020. № 32.

<sup>23</sup> Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Ч. 5 ст. 14 // СЗ РФ. 2020. № 31 (ч. I). Ст. 5018.

ной помощи по налоговым делам»<sup>24</sup>, закрепляющий порядок автоматического обмена финансовой информацией с иностранными государствами (территориями). Заметим, что подобный информационный обмен стал возможен в первую очередь благодаря внедрению современных цифровых технологий.

Подводя итог проведенного исследования, хотелось бы отметить, что цифровизация оказывает существенное влияние на метод финансового права. Безусловно, она не затрагивает таких его существенных характеристик, как императивность и диспозитивность, — это обобщенные категории, характерные для метода любой отрасли права. В то же время внедрение цифровых технологий меняет внутреннюю

суть процессов воздействия на общественные отношения, расширяя и трансформируя способы влияния на поведение участников таких отношений. Дополняя традиционные способы правового регулирования техническими средствами обеспечения их реализации, государство повышает эффективность механизма правового регулирования. Цифровые технологии предоставляют праву возможность регулирования общественных отношений принципиально новыми способами, расширяя вариативность инструментария метода финансового права. Представляется, что рассмотренные в статье тенденции будут только усиливаться, приводя к изменению содержания метода финансового права.

## БИБЛИОГРАФИЯ

1. Актуальные проблемы финансового права в условиях цифровизации экономики : монография / под ред. Е. Ю. Грачевой. — М. : Проспект, 2020. — 256 с.
2. Алексеев С. С. Собрание сочинений : в 10 т. [+ Справоч. том]. Т. 3 : Проблемы теории права : курс лекций. — М. : Статут, 2010. — 781 с.
3. Винницкий Д. В. Предмет и система финансового права на современном этапе // Известия высших учебных заведений. Правоведение. — 2002. — № 5 (244). — С. 30–42.
4. Грачева Е. Ю. Финансовое право России: вчера и сегодня // Вестник Московского университета. Серия 11 : Право. — 2012. — № 3. — С. 20–38.
5. Радько Т. Н. Теория государства и права : учебник. — 2-е изд. — М. :

- Перспект, 2011. — 752 с.
6. Рукавишникова И. В. Метод финансового права : дис д-ра юрид. наук — Саратов, 2004. — 521 с.
  7. Ситник А. А. Правовое регулирование финансового контроля и надзора в сфере денежного обращения в Российской Федерации : дис д-ра юрид. наук. — М., 2020. — 506 с.
  8. Теория государства и права : учебник для вузов / под ред. В. М. Корельского, В. Д. Первалова. — 2-е изд., изм. и доп. — М. : Норма, 2003. — 616 с.
  9. Финансовое право в условиях развития цифровой экономики : монография / под ред. И. А. Цинделиани. — М. : Проспект, 2019. — 320 с.
  10. Финансовое право : учебник / отв. ред. Е. М. Ашмарина, С. О. Шохин. — М. : Элит, 2009. — 750 с.
  11. Финансовое право : учебник / отв. ред. О. Н. Горбунова. — 3-е изд., перераб и доп. — М. : Юристъ, 2006. — 587 с.
  12. Финансовое право : учебник / под ред. Н. И. Химичевой. — 4-е изд., перераб и доп. — М. : Норма, 2009. — 768 с.
  13. Финансовое право : учебник для бакалавров / под ред. И. А. Цинделиани. — 3-е изд. — М. : Проспект, 2016. — 656 с.

---

<sup>24</sup> Федеральный закон от 27.11.2017 № 340-ФЗ «О внесении изменений в часть первую Налогового кодекса Российской Федерации в связи с реализацией международного автоматического обмена информацией и документацией по международным группам компаний» // СЗ РФ. 2017. № 49. Ст. 7312.

14. ~~Хабриева Т. Я., Черногор Н. Н.~~  
Право в условиях цифровой реальности // Журнал российского права. — 2018. — № 1. — С. 85–102.
15. *Халфина Р. О.* К вопросу о предмете и системе советского финансового права // Вопросы советского административного и финансового права. — М. : Изд-во Академии наук СССР, 1952. — С. 182–214.
16. *Худяков А. И.* Дискуссионные вопросы предмета финансового права // Финансовое право. — 2009. — № 3. — С. 2–8.
17. *Цинделиани И. А.* Предмет и система финансового права как отрасли права в советской финансово-правовой литературе // Финансовое право. — 2011. — № 12. — С. 16–22.
18. *Шохин С. О.* К вопросу о предмете и системе финансового права // Финансовое право. — 2019. — № 2. — С. 12–14.

R  
E  
F  
E  
R  
E  
N  
C  
E  
S  
(  
T  
R  
A  
N  
S  
L  
I  
T  
E  
R  
A  
T  
I  
O

М  
а  
т  
е  
р  
и  
а  
л  
н  
о  
с  
т  
у  
п  
и

1. Aktual'nye problemy finansovogo prava v usloviyah cifrovizacii ekonomiki : monografiya / pod red. E. Yu. Grachevoj. — M. : Prospekt, 2020. — 256 s.
2. Alekseev S. S. Sobranie sochinenij : v 10 t. [+ Spravochn. tom]. T. 3 : Problemy teorii prava : kurs lekciij. — M. : Statut, 2010. — 781 s.
3. Vinnickij D. V. Predmet i sistema finansovogo prava na sovremennom etape // Izvestiya vysshih uchebnyh zavedenij. Pravovedenie. — 2002. — № 1 (244). — S. 30–42.
4. Gracheva E. Yu. Finansovoe pravo Rossii: vchera i segodnya // Vestnik Moskovskogo universiteta. Seriya 11 : Pravo. — 2012. — № 3. — S. 20–38.
5. Rad'ko T. N. Teoriya gosudarstva i prava : uchebnik. — 2-e izd. — M. : Prospekt, 2011. — 752 s.
6. Rukavishnikova I. V. Metod finansovogo prava : dis. d-ra jurid. nauk — Saratov, 2004. — 521 s.
7. Sitnik A. A. Pravovoe regulirovanie finansovogo kontrolya i nadzora v sfere denezhnogo obrashcheniya v Rossijskoj Federacii : dis. d-ra jurid. nauk. — M., 2020. — 506 s.
8. Teoriya gosudarstva i prava : uchebnik dlya vuzov / pod red. V. M. Korel'skogo, V. D. Perevalova. — 2-e izd., izm. i dop. — M. : Norma, 2003. — 616 s.
9. Finansovoe pravo v usloviyah razvitiya cifrovoj ekonomiki : monografiya / pod red. I. A. Cindeliani. — M. : Prospekt, 2019. — 320 s.
10. Finansovoe pravo : uchebnik / otv. red. E. M. Ashmarina, S. O. Shohin. — M. : Elit, 2009. — 750 s.
11. Finansovoe pravo : uchebnik / otv. red. O. N. Gorbunova. — 3-e izd., pererab i dop. — M. : Yurist", 2006. — 587 s.
12. Finansovoe pravo : uchebnik / pod red. N. I. Himichevoj. — 4-e izd., pererab i dop. — M. : Norma, 2009. — 768 s.
13. Finansovoe pravo : uchebnik dlya bakalavrov / pod red. I. A. Cindeliani. — 3-e izd. — M. : Prospekt, 2016. — 656 s.
14. Habrieva T. Ya., Chernogor N. N. Pravo v usloviyah cifrovoj real'nosti // Zhurnal rossijskogo prava. — 2018. — № 1. — S. 85–102.
15. Halfina R. O. K voprosu o predmete i sisteme sovetskogo finansovogo prava // Voprosy sovetskogo administrativnogo i finansovogo prava. — M. : Izd-vo Akademii nauk SSSR, 1952. — S. 182–214.
16. Hudyakov A. I. Diskussionnye voprosy predmeta finansovogo prava // Finansovoe pravo. — 2009. — № 3. — S. 2–8.
17. Cindeliani I. A. Predmet i sistema finansovogo prava kak otrasli prava v sovetskoj finansovo-pravovoj literature // Finansovoe pravo. — 2011. — № 12. — S. 16–22.
18. Shohin S. O. K voprosu o predmete i sisteme finansovogo prava // Finansovoe pravo. — 2019. — № 2. — S. 12–14.

**№ 3. Гражданско-правовое регулирование отношений при создании и распространении информации в Интернете. Исключительные права в цифровой сфере: объекты, границы, пределы осуществления.**

По расчетам консалтингового подразделения Cisco IBSG в промежутке между 2008 и 2009 гг. количество

подключенных к интернету предметов превысило количество людей, таким образом, произошёл эволюционный переход от интернета людей к интернету вещей. Под интернетом вещей понимают межсетевое информационное взаимодействие, включающее взаимодействие физических устройств, транспортных средств, зданий и других предметов, встроенных в электронику, программное обеспечение, датчики, исполнительные механизмы и сеть, которые позволяют этим объектам собирать и обмениваться данными. В отличие от классического интернета, обеспечивающего коммуникативные связи между людьми, интернет вещей обеспечивает межмашинные коммуникации между неодушевленными вещами, а также между неодушевленным и одушевленным мирами, между вещами и человеком, информируя последнего о происходящем в помещении, квартире, доме, на заводе, складе, открытой территории и принимая от человека соответствующие решения в форме сигналов для корректировки ситуации. Интернет вещей предполагает подключение к глобальной компьютерной сети бытовых предметов при помощи встроенных модулей связи, благодаря чему они получают возможность взаимодействовать друг с другом, внешней средой, обмениваться данными и совершать операции без участия человека. Список предметов, которые могут использовать эту возможность, неограничен: это может быть автотранспорт, бытовая техника, коммуникационные приборы. Датчики, встроенные в предметы, в режиме реального времени отслеживают происходящие процессы, встроенные модули связи осуществляют

коммуникацию с другими предметами по Сети. По подсчетам, к концу 2018 г. количество подключенных к интернету вещей устройств во всем мире достигло 22 млрд штук. Прогнозируется, что к 2025 г. к интернету будет подключено 38,6 млрд устройств, а к 2030 г. – 50 млрд. Интернет вещей применяется в широком диапазоне областей жизни: для удовлетворения общественных и личных нужд, в здравоохранении, при самостоятельном планировании человеком оздоровительных мероприятий, для автоматизации быта, а также как средство поддержки личностного развития и мониторинга окружающей среды. Дальнейшее применение технологий интернета вещей изменит облик многих индустрий и областей жизнедеятельности. В ряде областей человеческие трудозатраты и ошибки будут сведены к минимуму. Так, интернет вещей в электроэнергетике кардинально изменит технологии, обеспечит экономию средств и создаст новые продукты во всех звеньях энергосистемы. В сельском хозяйстве интернет вещей позволит внедрить точное земледелие и значительно усовершенствовать управление сельхозтранспортом. Решения интернета вещей в логистике помогут сократить затраты, повысить прозрачность цепочки доставки товаров и сократить использование человеческого труда. Технологии умного города позволят создать более привлекательную городскую среду с эффективно работающей транспортной системой, ЖКХ, удобной инфраструктурой и обеспечить безопасность населения. Среди компонентов умного дома наибольшей популярностью у потребителей пользуются устройства повышения безопасности, контроля потребления воды и энергии, умные бытовые приборы и термостаты. По оценке Глобального

института McKinsey, интернет вещей до 2025 г. будет ежегодно приносить мировой экономике от 4 до 11 трлн долл. США. Проект интернета вещей принят в качестве приоритетного на государственном уровне в ЕС и Китае, является ключевым для таких корпораций, как Cisco, IBM, Intel, Ericsson, Huawei, ZTE, NEC, HP и др. Интернет вещей, постепенно проникая во все сферы деятельности людей, вывел в число активно обсуждаемых технологических трендов такое понятие, как «промышленный интернет вещей» (IIoT). Технологии интернета вещей, применяемые в промышленности, позволяют существенно сократить затраты и повысить производительность. По результатам опроса PricewaterhouseCoopers крупнейших немецких компаний выявлено, что по ожиданиям компаний в течение 2019–2022 гг. инвестиции в промышленные интернет-технологии могут позволить повысить эффективность в среднем на 18 % и сократить затраты на 14 %. При этом интернет вещей позволяет промышленным компаниям трансформировать бизнес-модели и наращивать доходы от услуг (например, от послепродажного обслуживания): компании прогнозируют, что в среднем эти технологии обеспечат рост выручки на 2,9 % ежегодно. По прогнозам аналитиков из Market Research Engine, рынок IIoT будет расти со среднегодовым темпом более 8 % и к 2022 г. превысит 176 млрд долл. Zion Market Research утверждает, что сектор IIoT к 2023 г. достигнет 232 млрд долл. По данным Global Market Insights мировой рынок IIoT (включая оборудование, сенсоры, датчики, роботизированные системы, платформы, ПО и услуги) к 2023 г.

составит 700 млрд долл. По прогнозам агентства Machina Research к 2025 г. мировой рынок IIoT достигнет 484 млрд евро. Выводы по теме 3. Цифровизация – уже повсеместная реальность, а проникновение интернета и цифровых технологий в традиционные отрасли стало одним из основных трендов последних лет и происходит в общемировом масштабе, что позволяет говорить о цифровой трансформации всех отраслей экономики, жизни социума и о формировании нового хозяйственного уклада – цифровой экономики. Практическое использование технологий цифровой экономики является современным трендом в общественной и хозяйственной жизнедеятельности современного государства, активно влияет на потребительское поведение, проявляется в мобильности и стремлении компаний к постоянному совершенствованию.

#### **№ 4. Основы нормативно-правового регулирования в сфере информационных технологий: технологии искусственного интеллекта, правовой режим нейросетей.**

Искусственный интеллект – собирательный термин, охватывающий множество так называемых умных технологий, которые объединяет способность к творческой деятельности и самообучению. Заметим, что английский термин означает «умение рассуждать разумно». ИИ воспринимает информацию и реагирует на нее, не дожидаясь вмешательства или команды человека. ИИ не просто хранит огромные массивы данных на компьютере – он их анализирует. На самом высоком уровне сложности данная технология задействована в самоуправляемых автомобилях, беспилотниках (дронах), роботах, а в повседневной жизни ее функции сводятся к способности

компьютера накапливать и затем применять <sup>Папаскья Г. Т.</sup> информацию, обучаясь, развиваясь и принимая решения на основании изученных данных.

Одно из первых определений ИИ еще в 1956 г. дал Дж. Маккарти: свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека. В начале 1980-х гг. ученые в области теории вычислений Барр и Файгенбаум предложили следующее определение искусственного интеллекта:

Искусственный интеллект – это область информатики, которая занимается разработкой интеллектуальных компьютерных систем, т. е. систем, обладающих возможностями, которые мы традиционно связываем с человеческим разумом, – понимание языка, обучение, способность рассуждать, решать проблемы и т. д. Позже к ИИ стали относить алгоритмы и программные системы, отличительным свойством которых является то, что они могут решать некоторые задачи так, как это делал бы размышляющий над их решением человек.

Сферы применения ИИ достаточно широки, их можно разделить по критерию ключевых точек развития. ИИ может помогать человеку выполнять свою работу быстрее и качественнее, принимать более взвешенные и эффективные решения и в конечном итоге автоматизировать процессы принятия решений, осуществляя их без участия людей. По сути, технологии ИИ имитируют способность человека воспринимать <sup>Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март</sup> информацию, размышлять и действовать. Большинство руководителей прекрасно понимают,

что искусственному интеллекту под силу изменить почти все аспекты ведения бизнеса. Благодаря этой технологии к 2030 г. мировая экономика может вырасти на 15,7 трлн долл. США. Наибольшие экономические выгоды от ИИ будут в Китае (рост ВВП на 20 % к 2030 г.) и Северной Америке (рост на 14,5 %).

## **№ 5. Правовое регулирование в сфере сбора, передачи, хранения, обработки, доступа к информации и обработки персональных данных.**

Вопросы правового регулирования персональных данных, включая биометрические данные, их сбор, хранение, передачу, распространение и другие действия, методы защиты персональных данных регулируются в Казахстане законом Республики Казахстан «О персональных данных и их защите». Закон регулирует общественные отношения в сфере персональных данных, а также определяет цель, принципы и правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных.

### [Оглавление \(показать/скрыть\)](#)

Закон определяет **персональные данные** – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе; а **биометрические данные** как персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность. Закон разграничивает персональные данные по категории доступа к ним. Персональные данные по доступности подразделяются на **общедоступные и ограниченного доступа**. **Общедоступные персональные данные** – персональные данные, доступ к которым является свободным с согласия субъекта

или на которые в соответствии с законодательством Республики Казахстан не распространяются требования соблюдения конфиденциальности, в том числе биографические справочники, телефонные, адресные книги, общедоступные электронные информационные ресурсы, средства массовой информации и т.д.

**Персональные данные ограниченного доступа** – персональные данные, доступ к которым ограничен законодательством Республики Казахстан.

По общему правилу, сбор персональных данных осуществляется с согласия субъекта, которому принадлежат эти персональные данные, или его законного представителя.

Однако закон устанавливает перечень случаев, когда сбор персональных данных осуществляется **без согласия субъекта или его законного представителя**:

- 1) осуществления деятельности правоохранительных органов и судов, исполнительного производства;
- 2) осуществления государственной статистической деятельности;
- 3) использования государственными органами персональных данных для статистических целей с обязательным условием их обезличивания;
- 4) реализации международных договоров, ратифицированных Республикой Казахстан;
- 5) защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно;
- 6) осуществления законной профессиональной деятельности журналиста и (или) деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии соблюдения требований законодательства Республики Казахстан по обеспечению прав и

свобод человека и гражданина;

- 7) опубликования персональных данных в соответствии с законами Республики Казахстан, в том числе персональных данных кандидатов на выборные государственные должности;
- 8) неисполнения субъектом своих обязанностей по представлению персональных данных в соответствии с законами Республики Казахстан;
- 9) получения государственным органом, осуществляющим регулирование, контроль и надзор финансового рынка и финансовых организаций, информации от физических и юридических лиц в соответствии с законодательством Республики Казахстан;
- 10) в иных случаях, установленных законами Республики Казахстан.

Субъект, которому принадлежат персональные данные или его законный представитель дает (или отзывает) согласие на сбор, обработку персональных данных **письменно или в форме электронного документа либо иным способом с применением элементов защитных действий**.

Лицо, которое осуществляет сбор, хранение, передачу, распространение или другие действия с персональными данными, в соответствии с Законом называется **оператор персональных данных**. В качестве оператора баз персональных данных может выступать государственный орган, физическое и (или) любое другое юридическое лицо, которые осуществляют сбор, обработку и защиту персональных данных.

Законом предусматриваются следующие действия (операции) по обработке персональных данных:

*Действия (операции) по обработке персональных данных*

*Описание действий (операций) по обработке персональных данных*

<b>Обработка персональных данных</b>	Действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных		определение принадлежности персональных данных субъекту персональных данных невозможно
			Действия с персональными данными, направленные на реализацию целей деятельности собственника, оператора и третьего лица
<b>Сбор персональных данных</b>	Действия, направленные на получение персональных данных	<b>Использование персональных данных</b>	
			Действия по обеспечению целостности, конфиденциальности и доступности персональных данных
<b>Блокирование персональных данных</b>	Действия по временному прекращению сбора, накопления, изменения, дополнения, использования, распространения, обезличивания и уничтожения персональных данных	<b>Хранение персональных данных</b>	
			Действия, в результате совершения которых происходит передача персональных данных, в том числе через средства массовой информации или предоставление доступа к персональным данным каким-либо иным способом
<b>Накопление персональных данных</b>	Действия по систематизации персональных данных путем их внесения в базу, содержащую персональные данные	<b>Распространение персональных данных</b>	
			Передача персональных данных на территорию иностранных государств.
<b>Уничтожение персональных данных</b>	Действия, в результате совершения которых невозможно восстановить персональные данные	<b>Трансграничная передача персональных данных</b>	
<b>Обезличивание персональных данных</b>	Действия, в результате совершения которых	<p><b>Субъект, которому принадлежат персональные данные, наделен следующими правами:</b></p> <p>1) вправе знать о наличии у собственника и (или) оператора, а также третьего лица своих персональных данных, а также</p>	

получать информацию, содержащую: подтверждение факта, цели, источников, способов сбора и обработки персональных данных; перечень персональных данных; сроки обработки персональных данных, в том числе сроки их хранения;

- 2) требовать от собственника и (или) оператора изменения и дополнения своих персональных данных при наличии оснований, подтвержденных соответствующими документами;
- 3) требовать от собственника и (или) оператора, а также третьего лица блокирования своих персональных данных в случае наличия информации о нарушении условий сбора, обработки персональных данных;
- 4) требовать от собственника и (или) оператора, а также третьего лица уничтожения своих персональных данных, сбор и обработка которых произведены с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;
- 5) отозвать согласие на сбор, обработку персональных данных, кроме случаев законом;
- 6) дать согласие (отказать) собственнику и (или) оператору на распространение своих персональных данных в общедоступных источниках персональных данных;
- 7) на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда;
- 8) на осуществление иных прав, предусмотренных настоящим Законом и иными законами Республики Казахстан.

**Собственник и (или) оператор баз персональных данных является обязанными лицами, и в соответствии с законом на них возлагаются следующие**

**обязательства:**

- 1) утверждать перечень персональных данных, необходимый и достаточный для выполнения осуществляемых ими задач, если иное не предусмотрено законами Республики Казахстан;
- 2) принимать и соблюдать необходимые меры, в том числе правовые, организационные и технические, для защиты персональных данных в соответствии с законодательством Республики Казахстан;
- 3) соблюдать законодательство Республики Казахстан о персональных данных и их защите;
- 4) принимать меры по уничтожению персональных данных в случае достижения цели их сбора и обработки, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;
- 5) представлять доказательство о получении согласия субъекта на сбор и обработку его персональных данных в случаях, предусмотренных законодательством Республики Казахстан;
- 6) сообщать информацию, относящуюся к субъекту, в течение трех рабочих дней со дня получения обращения субъекта или его законного представителя, если иные сроки не предусмотрены законами Республики Казахстан;
- 7) в случае отказа предоставить информацию субъекту или его законному представителю в срок, не превышающий трех рабочих дней со дня получения обращения, представлять мотивированный ответ, если иные сроки не предусмотрены законами Республики Казахстан;
- 8) в течение одного рабочего дня: изменить и (или) дополнить персональные данные на основании соответствующих документов, подтверждающих их достоверность, или уничтожить персональные данные при невозможности их изменения и (или) дополнения; блокировать персональные данные, относящиеся к субъекту, в случае наличия информации о нарушении условий их

сбора, обработки;  
уничтожить персональные данные в случае подтверждения факта их сбора, обработки с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;  
снять блокирование персональных данных в случае неподтверждения факта нарушения условий сбора, обработки персональных данных.

**Гарантии защиты персональных данных**— защита персональных данных осуществляется путем применения комплекса мер, в том числе правовых, организационных и технических, в целях:

- 1) реализации прав на неприкосновенность частной жизни, личную и семейную тайну;
- 2) обеспечения их целостности и сохранности;
- 3) соблюдения их конфиденциальности;
- 4) реализации права на доступ к ним;
- 5) предотвращения незаконного их сбора и обработки.

По закону уполномоченный орган в сфере персональных данных является **Правительство Республики Казахстан**, которое наделено следующей компетенцией:

- 1) разрабатывает основные направления государственной политики в сфере персональных данных и их защиты;
- 2) осуществляет руководство деятельностью центральных исполнительных органов, входящих в структуру Правительства Республики Казахстан, местных исполнительных органов, в сфере персональных данных и их защиты;
- 3) [утверждает](#) порядок определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач;
- 4) [утверждает](#) порядок осуществления

собственником и (или) оператором, а также третьим лицом мер по защите персональных данных;

5) выполняет иные функции, возложенные на него [Конституцией](#), законами Республики Казахстан и актами Президента Республики Казахстан.

**Государственные органы** в пределах своей компетенции:

- 1) разрабатывают и (или) [утверждают](#) нормативные правовые акты в сфере персональных данных и их защиты;
- 2) рассматривают обращения физических и (или) юридических лиц по вопросам персональных данных и их защиты;
- 3) принимают меры по привлечению лиц, допустивших нарушения законодательства Республики Казахстан о персональных данных и их защите, к ответственности, [установленной законами](#) Республики Казахстан;
- 4) осуществляют иные полномочия, предусмотренные законами Республики Казахстан, актами Президента Республики Казахстан и Правительства Республики Казахстан.

Общий надзор за соблюдение законодательства о персональных данных и их защите осуществляют органы прокуратуры. За нарушение требований законодательства предусмотрена ответственность:

<i>Виды правовой ответственности</i>	<i>Описание норм ответственности за нарушение требований законодательства о персональных данных и их защите</i>
<b>Уголовная ответственность</b>	<b>Статья 147 Уголовного Кодекса Республики Казахстан. Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан</b>

**о персональных данных и их защите**

1. Несоблюдение мер по защите персональных данных лицом, на которое возложена обязанность принятия таких мер, если это деяние причинило существенный вред правам и законным интересам лиц, — **наказывается штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.**

2. Незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконных сбора и (или) обработки иных персональных данных — **наказывается штрафом в размере до**

**пяти тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до трех лет, либо лишением свободы на тот же срок.**

3. Деяния, предусмотренные частью второй настоящей статьи, совершенные лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сети телекоммуникаций, либо в целях извлечения выгод и преимуществ для себя или для других лиц, или организаций — **наказываются лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет или без такового.**

	<p>4. Распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконного сбора и (или) обработки иных персональных данных – <b>наказывается лишением свободы на срок до пяти лет.</b></p> <p>5. Распространение сведений, указанных в части четвертой настоящей статьи, в публичном выступлении, публично демонстрирующемся произведении, в средствах массовой информации или с использованием сетей телекоммуникаций – <b>наказывается лишением свободы на срок до семи лет.</b></p>		<p><b>должностных лиц, субъектов малого предпринимательства или некоммерческие организации – в размере тридцати, на субъектов среднего предпринимательства – в размере пятидесяти, на субъектов крупного предпринимательства – в размере ста месячных расчетных показателей, с конфискацией предметов и (или) орудия административного правонарушения или без таковой.</b></p> <p>2. Те же деяния, совершенные собственником, оператором или третьим лицом с использованием своего служебного положения, если эти действия не влекут установленную законом уголовную ответственность – <b>влекут штраф на физических лиц в размере пятидесяти, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации – в размере семидесяти пяти, на субъектов среднего предпринимательства – в размере ста, на субъектов крупного предпринимательства – в размере двухсот месячных расчетных</b></p>
<p><b>Административная ответственность</b></p>	<p><b>Статья 79 Кодекса Республики Казахстан «Об административных правонарушениях». Нарушение законодательства Республики Казахстан о персональных данных и их защите</b></p> <p>1. Незаконный сбор и (или) обработка <a href="#">персональных данных</a> – <b>влекут штраф на физических лиц в размере двадцати, на</b></p>		

	<p>показателей, с конфискацией предметов и (или) орудия административного правонарушения или без таковой.</p> <p>3. Несоблюдение собственником, оператором или третьим лицом мер по защите персональных данных – влечет штраф на физических лиц в размере ста, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации – в размере ста пятидесяти, на субъектов среднего предпринимательства – в размере двухсот, на субъектов крупного предпринимательства – в размере трехсот месячных расчетных показателей.</p> <p>4. Деяние, предусмотренное частью третьей настоящей статьи, повлекшее утерю, незаконный сбор и (или) обработку персональных данных, если эти деяния не влекут установленную законом уголовную ответственность, – влечет штраф на физических лиц в размере двухсот, на должностных лиц, субъектов малого предпринимательства или некоммерческие</p>	<p><b>Гражданско-правовая ответственность</b></p>	<p>организации – в размере пятисот, на субъектов среднего предпринимательства – в размере семисот, на субъектов крупного предпринимательства – в размере тысячи месячных расчетных показателей.</p> <p>1. Оспаривание действия (бездействия) субъекта, собственника и (или) оператора, а также третьего лица при сборе, обработке и защите персональных данных могут быть обжалованы в порядке, установленной главой 29 Гражданского процессуального Кодекса Республики Казахстан.</p> <p>2. Споры, возникающие при сборе, обработке и защите персональных данных, подлежат рассмотрению в порядке, установленном Гражданским процессуальным Кодексом Республики Казахстан.</p>
	<p>№ 6. Понятие и основные направления государственного регулирования цифровой экономики. Правовые условия для формирования единой финансово-цифровой среды доверия</p>		<p>Власти Казахстана утвердили в 2017 году госпрограмму «Цифровой Казахстан». По планам правительства, страну ожидает полная цифровая трансформация, которая произойдет с помощью 23 проектов-</p>

«ледоколов», призванных «взламывать целие сектора экономики для появления в них цифрового бизнеса».

Чем запомнился 2023 год

Главные итоги и тенденции. Мнения ключевых игроков ИТ-рынка

Унифицированные коммуникации в России

Аналитический обзор TAdviser

2023/11/24 14:37:56

Цифровой Казахстан  
Власти Казахстана утвердили в 2017 году госпрограмму «Цифровой Казахстан». По планам правительства, страну ожидает полная цифровая трансформация, которая произойдет с помощью 23 проектов-«ледоколов», призванных «взламывать целие сектора экономики для появления в них цифрового бизнеса».

Содержание[Свернуть]

ИТ-рынок Казахстана

2023

В Казахстане разработали цифровой кодекс для решения проблем регулирования ИТ-отрасли

Президент Казахстана поставил задачи по ИКТ-развитию страны

Превратить Казахстан в ИТ-страну.

Президент Токаев - о планах по цифровизации

Президент Казахстана назвал 5 приоритетов цифровой трансформации Казахстана

Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март  
Как проходит цифровая трансформация Казахстана

В Казахстане создают Национальную инфраструктуру пространственных данных за 15 млрд тенге

2022: Бесплатную инфосистему для фермеров разрабатывают в Казахстане

2021: ИТ-министр Казахстана отчитался об итогах цифровизации страны

2020

Создание центра цифровой трансформации госучреждений в Казахстане

Для реализации проекта «Цифровой Казахстан» остро не хватает ИТ-специалистов

В Казахстане начали полностью

переходить на электронные зачётки в вузах  
2019: Экономический эффект - 714,3 млрд тенге

2018: Инициировано создание национального Института в сфере информационной безопасности  
2017

Программа «Цифровой Казахстан» включает 23 проекта

Е-система госзакупок "Самрук-Казына"

До 1 мая в столице Казахстана заработает ситуационный центр

"Цифровой Казахстан": Назарбаев призвал развивать в стране 3D-принтинг и мобильный банкинг

Казахстан

Смотрите также

ИТ-рынок Казахстана

Основная статья: ИТ-рынок Казахстана

2023

В Казахстане разработали цифровой кодекс для решения проблем регулирования ИТ-отрасли

Министерство цифрового развития, инноваций и аэрокосмической промышленности Казахстана (МЦРИАП) разработало цифровой кодекс для решения проблем регулирования ИТ-отрасли. На реализацию этого проекта было потрачено 120 млн тенге (около 263 тыс. по курсу на

момент выхода новости - 24 ноября 2023 года).

Папаскья Г. Т.

~~Трансформация рынка финансовых услуг с помощью цифровых технологий~~

«Сегодня цифровое пространство стало основным каналом взаимодействия граждан, бизнеса и государства. Кодификация сделает также доступным и понятным для граждан и бизнеса применение законов в цифровой среде, устраним обременительные требования и регуляторные барьеры. Темпы развития и масштабы распространения цифровых технологий предъявляют новые требования не только к скорости принятия регуляторных актов, но и структуре законодательства. Принятие Цифрового кодекса позволит сформировать единое правовое пространство для развития цифровой экономики и цифровой трансформации государственного управления, — заявил вице-министр МЦРИАП Аскар Жамбакин. Согласно документу, одним из главных барьеров на пути развития цифровизации в Казахстане к ноябрю 2023 года являются:

громоздкое, противоречивое и нестабильное законодательство; избыточное регулирование функций государственных органов и административных процедур на законодательном уровне, что лишает уполномоченных органов самостоятельности, а также возможности принимать оперативные решения по оптимизации внешних и внутренних бизнес-процессов, внедрению передовых практик и цифровых решений; законодательные пробелы в регулировании цифровых прав человека и гражданина;

Актualityные проблемы российского права. 2021. Т. 16. № 3 (124) март

бесконтрольное использование больших данных, алгоритмов обработки данных с применением ИИ,

интернета вещей для ведения «цифровой слежки»;

ответственность единой законодательной базы, регулирующей деятельность провайдеров цифровых услуг.[1]

Президент Казахстана поставил задачи по ИКТ-развитию страны

Президент Казахстана Касым-Жомарт Токаев, выступая на одном из ИТ-форумов в октябре 2023 года, рассказал о задачах по развитию информационно-коммуникационных технологий в стране.

По словам казахстанского лидера, стране предстоит принять стратегический документ, определяющий сферу применения, задачи и инструменты развития искусственного интеллекта. Это передовая международная практика, такой шаг позволит нам задать устойчивый вектор технологического прогресса страны. Считаю, что прежде всего мы должны сосредоточиться на внедрении технологий искусственного интеллекта в таких значимых для нашей экономики отраслях, как нефтегазовый сектор, энергетика, сельское хозяйство, транспорт и логистика. Искусственный интеллект может в значительной мере оптимизировать процесс трансформации наших городов в полноценные smart city, благоприятные для проживания и работы, — пояснил Токаев.

»

По его словам, также стране необходимо укреплять цифровую инфраструктуру и увеличить вычислительные мощности.

«

Поручаю правительству в течение двух лет обеспечить строительство дата-центров, специализирующихся на искусственном интеллекте. Для этого могут быть привлечены такие мировые игроки, как Amazon, Google, Mastercard и City Group.

Во время недавней поездки в Нью-Йорк я встретился с руководством этих компаний, и были достигнуты соответствующие договоренности. Важно также развивать экосистему данных для искусственного интеллекта. Большие данные - это, по сути, «топливо» для искусственного интеллекта, - продолжил Токаев.

Еще одно поручение президент Казахстана — развернуть до конца 2025 года 5G-сети во всех областных центрах. При этом изначально назывались более поздние сроки — до 2027 года.

«Правительству следует всесторонне проработать данный вопрос. При необходимости внести изменения в законодательство, - заключил казахстанский президент, подчеркнув, что жителей самых отдаленных районов необходимо обеспечить доступом к интернету с помощью низкоорбитальных спутниковых систем.[2]

Превратить Казахстан в ИТ-страну. Президент Токаев - о планах по цифровизации Президент Казахстана Касым-Жомарт Токаев в своем ежегодном послании народу подчеркнул, что республика должна стать ИТ-страной. Его слова приводит официальный Telegram-канал пресс-службы президента Казахстана.

«Вы знаете, я уделяю повышенное внимание вопросам цифровизации и внедрения инноваций. Перед нами стоит стратегически важная задача —

превратить Казахстан в ИТ-страну. Достижения в сфере цифровизации у нас уже имеются — мы в числе мировых лидеров по индексу развития электронного правительства и финтехе, - заявил казахстанский лидер.

Президент Казахстана Касым-Жомарт Токаев

По его словам, объем экспорта казахстанской ИТ-отрасли только за 2022 год вырос в пять раз и до конца 2023-го может превысить \$0,5 млрд.

«Но и это не предел. Новая задача правительства — довести экспорт ИТ-услуг до одного миллиарда долларов к 2026 году. Этому будет содействовать открытие совместных предприятий с крупными зарубежными ИТ-компаниями. Правительству надлежит внести детальные предложения по этому вопросу, - заявил президент.

Бывший заместитель председателя правления национального инфокоммуникационного холдинга «Зерде» Павел Коктышев считает, что Казахстан имеет все шансы стать активно действующей цифровой ИТ-экономикой. Связывает он это с тем, что в стране постоянно растущие тренды не только по экспорту, но и по росту выручки и новым компаниям.

«Рынок сейчас на этапе роста и он еще довольно долго будет на этом этапе. Единственное — скорость, про которую говорит президент, потребует, если честно, большой мобилизации при привлечении крупных международных компаний в

Казахстан. Также и структурирование, <sup>Папаскья Г. Т.</sup> допустим, он целый блок посвятил развитию среднего бизнеса. Я считаю, что по ряду направлений то, что сегодня президент говорил и про развитие инноваций, и про развитие экспорта, одним из важных ключевых решений является развитие венчурной индустрии, и он тоже об этом сказал, - прокомментировал Павел Коктышев.[3]

»

Президент Казахстана назвал 5 приоритетов цифровой трансформации Казахстана  
В июле 2023 года президент Казахстана Касым-Жомарт Токаев назвал пять ключевых приоритетов в цифровой трансформации страны.

Отмечается, что Казахстан выступает в качестве привлекательного пространства для развития инноваций, цифрового производства и творчества. Это особенно важно в свете сложившейся геополитической обстановке и в условиях макроэкономических вызовов. При этом цифровая трансформация является одним из определяющих факторов конкурентоспособности как отдельных компаний, так и крупных регионов.

Касым-Жомарт Токаев  
Приоритет №1 —  
человекоцентричность

Речь идет о предоставлении гражданам современных услуг. В частности, планируется осуществить переход к качественно новому формату цифровизации госуправления — Invisible Government. Суть заключается в том, что главный фокус

государственной политики сосредоточен на человеке, его нуждах и интересах. Все государственные услуги будут максимально переведены в электронный формат.

Унифицированные коммуникации: как российские поставщики укрепляют свои позиции. Обзор TAdviser 15.1 т

Приоритет №2 — создание благоприятных условий для ИТ-отрасли

Казахстан намерен стать ведущим игроком в сфере новых цифровых технологий, криптоиндустрии, а также регулируемого и прозрачного цифрового майнинга. Развитие ИТ-сектора является важным направлением государственной деятельности. Будут созданы условия для привлечения международного капитала в казахстанскую цифровую экосистему.

Приоритет №3 — масштабная модернизация ИТ-инфраструктуры

Казахстан формирует цифровую инфраструктуру, сопряженную с международными коридорами и трансграничными потоками данных. В частности, совместно с азербайджанскими партнерами начата работа на транскаспийском участке для подключения к мировым центрам концентрации трафика. На местный рынок привлекаются крупнейшие игроки сферы облачных вычислений.

Приоритет №4 — развитие цифровой экономики и индустрии 4.0

Данное направление предполагает инновационные гранты и налоговые преференции для технологического обновления и принятия цифровых решений. Для дальнейшего развития цифровой экономики правительству

предстоит своевременно внедрять новые меры поддержки.

Папаскья Г. Т.

Трансформация рынка финансовых услуг в условиях цифровизации

Приоритет №5 — укрепление человеческим капиталом

По мере цифровой трансформации растет потребность в квалифицированных ИТ-специалистах. Поставлена задача к 2025 году подготовить как минимум 100 тыс. таких сотрудников. Для достижения этой цели внедрено шефство профильных университетов над региональными вузами, расширено грантовое обучение, открыты 12 частных инновационных ИТ-школ.[4]

Как проходит цифровая трансформация Казахстана

В июле 2023 года портал Global CIO опубликовал исследование, посвященное казахстанскому ИТ-рынку и подготовленное в разрезе особенностей цифровой трансформации различных отраслей.

По словам авторов отчета, в 2022 году Казахстан вошел в топ-30 самых развитых в цифровом отношении стран мира. В мировом рейтинге Казахстан занимает 51-е место в Индексе развития ИКТ и 58 место — в Индексе сетевой готовности. К 2025 году правительство Казахстана планирует войти в число 20 лучших в Индексе развития электронного правительства ООН, в число 50 лучших в Индексе электронной коммерции B2C (Business to Consumers) и в число 40 лучших стран по Индексу развития информационно-коммуникационных технологий.

Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март

Объем услуг, оказанных в Казахстане в сфере программирования,

консультационных и других сопутствующих услуг, по итогам 2022 года составил 772 млрд тенге (примерно \$1,67 млрд по среднему курсу доллара к тенге за 2022 год), что на 19,5% больше, чем годом ранее.

Крупнейшими экономическими и ИТ-центрами являются города Астана и Алматы: компании из этих городов производят 41,5% и 49% ИТ-услуг соответственно. Количество компаний, занимающихся разработкой программного обеспечения и консультационными услугами в сфере ИТ, за последние 4 года увеличилось в 2,7 раз, говорится в исследовании за 2022 год.

Финтех и банковский сектор

Рынок финтеха в Казахстане является одним из самых быстроразвивающихся в стране и крупнейшим в Центральной Азии. Банки активно сотрудничают с цифровыми компаниями и формируют экосистемы, а сервисы становятся персонализированными и способными решать широкий спектр задач, включая как финансовые, так и нефинансовые, указывают исследователи. По данным за 2022 год, 86% жителей Казахстана являются активными пользователями мобильных банков.

Цифровизация в горно-металлургическом комплексе

В 2022 году горнодобывающая отрасль в Казахстане была в начале пути цифровизации, однако применение цифровых технологий на некоторых предприятиях уже позволило получать значительные эффекты на всех этапах создания стоимости. Для цифровой

трансформации горно-металлургического комплекса (ГМК) <sup>Папаскья Г. Т.</sup> главным стоп-фактором остается нехватка цифровых компетенций внутри компании, а именно проведение организационной, технологической и культурной трансформации, чтобы вся организация, включая работников производства и технологов, владела подходом data-driven и инструментами аналитики self-service, считают аналитики. Они перечислили несколько трендов в цифровизации ГМК в Казахстане:

использование искусственного интеллекта и промышленного интернета вещей в качестве инструментов экономической устойчивости предприятий; импортозамещение в плане технологий и ИТ-поставщиков; дефицит квалифицированных кадров: для цифровой трансформации нужно большое количество специалистов с глубоким пониманием горного дела и информационных технологий одновременно. Таких специалистов сейчас нет, их нужно обучать. господдержка цифровой трансформации: запущен нацпроект «Горная индустрия 4.0» по объединению ИТ, добычи и подготовки специалистов в ВУЗах. Строительная сфера

К концу 2022 года в Казахстане реализованы несколько государственных проектов, нацеленных на строительную сферу:

единый геопортал инфраструктурных данных (ЕГИД). В 2022 году оцифрованы 63,7% сведений об инженерных сетях застроенной

территории, внесены 142 618 записей в слой «акт ввода в эксплуатацию», в системе работают 1908 пользователей; E-PSD - единая цифровая платформа для взаимодействия заказчиков и экспертных организаций по принципу «одного окна»; ИС «Казреестр» — система для автоматизированного сбора, обработки, хранения и анализа сведений в сфере государственной регистрации учета долей в жилищном строительстве. Она содержит уникальные номера проектов, уведомление ГАСК (получение разрешения на строительство), сведения о помещениях, электронные договоры долевого участия (функция автопроверки и авторегистрации договоров); e-QURYLYS — система для обеспечения мониторинга и прозрачности работ на всех этапах строительного процесса. В e-QURYLYS уже зарегистрировано более 25 000 объектов строительства, только за март 2022 года сдано 6230 отчетов; e-SHANYRAQ — система для повышения прозрачности и эффективности деятельности субъектов жилищного фонда и жилищно-коммунального хозяйства. В ней проводится анализ эффективности работы коммунальных служб, приборизация учета воды и тепла, учет и контроль эксплуатации лифтов, отслеживается состояние коммунальной инфраструктуры, составляется технический паспорт состояния многоквартирных жилых домов. Цифровизация госуслуг

К 2022 году на деятельность по управлению информационно-коммуникационной инфраструктурой в рамках формирования и развития государственных электронных информационных ресурсов и систем было заложено 58,2 млрд тенге. Развитию госуслуг способствует не только синергия с банковским сектором, но и высокое

покрытие интернетом и сотовой связью территорий страны. Сейчас в Казахстане насчитывается 6 406 населенных пунктов, из которых 4974 (77%) подключены к широкополосному мобильному интернету. 2 928 населенных пунктов подключены к сети 4G, 2 046 — обеспечены технологией 3G. К 2027 году запланирован 75% охват сетью 5G каждого города республиканского значения и столицы и 60% 5G охват в областных центрах.[5]

В Казахстане создают Национальную инфраструктуру пространственных данных за 15 млрд тенге. В конце марта 2023 года стало известно о том, что в Казахстане появится Национальная инфраструктура пространственных данных (НИПД). На реализацию проекта планируется выделить 15,5 млрд тенге (приблизительно 2,79 млрд рублей по курсу на 13 апреля 2023 года).

## № 7. Информационная инфраструктура и безопасность

Власти Казахстана рассматривают вопрос о создании в стране специализированного Института, который бы занимался актуальными проблемами обеспечения информационной безопасности страны. Инициатором создания подобного заведения является Ержан Сейткулов, директор научно-исследовательского института информационной безопасности и криптологии ЕНУ им. Л.Н. Гумилева, член Общественного совета Министерства оборонной и аэрокосмической промышленности Республики Казахстан[9].

Ключевой идеей создания новой структуры, является то, что это должно

позволить более эффективно реализовывать научно-исследовательские и опытно-конструкторские работы, направленные на обеспечение информационной безопасности государства.

В качестве основных задач деятельности нового Института отмечаются такие как, реализация стратегической задачи по поэтапному импортозамещению, участие в реализации государственной политики в сфере обеспечения информационной безопасности, развитие государственно-частного партнерства, поддержка отечественных исследователей и стартапов, актуализация и разработка национальных стандартов в сфере информационной безопасности, подготовка кадров, экспертиза научно-технических проектов и т.д.

Предполагается, что новый Институт будет непосредственным участником государственной системы «Киберщит Казахстана», которой будет оказывать на постоянной основе научно-аналитическое сопровождение ее деятельности. В современных условиях цифровой экономики существует большое количество вызовов и угроз экономической безопасности, преодоление и противодействие которым является важнейшим направлением национальной безопасности государства. Однако нарушители, посягающие на экономическую безопасность государства, организаций и граждан, все чаще находят новые и более совершенные способы осуществления своих злонамеренных действий с использованием цифровых технологий. Задача государственных органов, обеспечивающих экономическую и информационную безопасность — выявить такие способы, минимизировать их влияние в случае возможной

реализации и создать условия, направленные на повышение информационной безопасности в условиях цифровой экономики [1]. «Без цифровой экономики мы не сможем перейти к следующему технологическому укладу. А без этого перехода к новому технологическому укладу у российской экономики, а значит и страны, нет будущего» — отметил президент Российской Федерации Владимир Владимирович Путин, отвечая на вопросы во время «Прямой линии» в 2017 г. Безусловно, функционирование цифровой экономики в условиях постоянной цифровой трансформации неизбежно связано с возникновением и влиянием определенного рода угроз. Вызовы и угрозы, с которыми сталкивается цифровая экономика на сегодняшний день, имеют целью подрыв информационной и экономической безопасности российского государства. Следует отметить, что экономическая и информационная безопасности являются подсистемой национальной безопасности (рис. 1). Исходя из стратегических целей, определяющих национальные интересы страны, вытекают задачи, позволяющие обеспечить устойчивое развитие страны в долгосрочном промежутке времени. Экономическая безопасность в системе национальной безопасности играет фундаментальную роль, поскольку без экономического потенциала невозможно противостоять внешним угрозам со стороны мирового сообщества [3].

**ROLE OF INFORMATION SECURITY IN TERMS OF DIGITAL ECONOMY ABSTRACT.**

The current level of economic development implies an active use of the Internet, satellite communications, and new technologies of processing, storing,

Папаскья Г. Т.

Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март

and transmitting information, which, in its turn, makes the problem of protecting personal data and ensuring information security of the state and enterprises urgent. Unauthorized access to information resources of organizations, destruction, blocking, copying and use of companies' information for the deceptive purposes of third parties cause significant damage to both individuals and businesses and the state. The article examines the correlation of the concepts of information security and economic security, specifies today's existing challenges and threats to economic security in the context of digital transformation, analyzes the statistical data of economic crimes using digital technologies; it identifies possible causes and factors of weakening the security of the digital economy. The authors present an analysis of statistical data that characterize the number and structure of crimes related to violation of information security of the country and territories. In particular, they examine the following types of crimes: cyber attacks on the websites of public authorities; creation, use and distribution of malicious computer programs; fraud using electronic means of payment.

**KEYWORDS.** Information security, digital economy, economic security, threats to economic security, national security.

**ARTICLE INFO.** Received December 20, 2019; accepted March 2, 2020; available online March 31, 2020. Baikal Research Journal электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6

Нынешнее состояние преступности характеризуется тем, что происходит переход большого количества антисоциальных злоумышленных деяний в киберсреду. По данным Генеральной прокуратуры Российской Федерации, за последние 6 лет киберпреступность выросла в 11 раз [4]. Это очень

показательные значения. А если <sup>Папаскья Г. Т.</sup> обратить внимание на масштабы и прибыльность в данной преступной сфере, то по некоторым оценкам ущерб мировой экономики от преступности в сфере цифровых и компьютерных технологий составляет от 0,7 до 3 трлн долл. И все это имеет положительную динамику<sup>1</sup>. Для повышения качества жизни граждан, обеспечения конкурентоспособности России, развития экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствования системы государственного управления на основе использования информационных и телекоммуникационных технологий была разработана государственная программа Российской Федерации «Информационное общество»<sup>2</sup>. Для того чтобы определить, насколько широко распространен доступ в интернет для населения и организаций, мы решили проанализировать статистику Федеральной службы государственной статистики в отношении развития информационного общества в Российской Федерации. Таким образом, мы определили, что по состоянию на конец 2017 г. около 80 чел. населения из 100 имеют мобильный широкополосный доступ в интернет, при этом сохраняется тенденция к увеличению количества абонентов (рис. 2). Фиксированный широкополосный доступ имеет 21 чел. из 100. Эта разница обуславливается размером необходимых инвестиций провайдерами в построение телекоммуникационных сетей. В целом, растет количество абонентов, имеющих как фиксированный, так и мобильный доступ в интернет. <sup>Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март</sup> 1 Портал правовой статистики : сайт / Генеральная прокуратура РФ. М., 2019. URL: [\[crimestat.ru/\]\(http://crimestat.ru/\) \(дата обращения: 15.11.2019\). 2 Об утверждении государственной программы Российской Федерации «Информационное общество» : Постановление Правительства РФ от 15 апр. 2014 г. № 313 // СПС «КонсультантПлюс». Рис. 1. Структура национальной безопасности \[2\] Baikal Research Journal электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11\(1\).6 Среди организаций также наблюдается рост тех, кто используют интернет в своей деятельности. По состоянию на 2017 г. доля таких организаций составила 89 % \(рис. 3\). Можно отметить, что, как среди организаций, так и среди населения доступ в интернет распространен достаточно широко. Значит, высока доля потенциальных жертв киберпреступлений \[5\]. Мы решили посмотреть, какое количество организаций используют средства защиты информации, и на 2017 г. доля подобных организаций составила 87,2 % \(рис. 4\). С 2010 г. доля таких организаций выросла на 17,2 %. По данным Совета Безопасности Российской Федерации, в 2015 г. было зафиксировано около 14,4 млн кибератак на веб-сайты госорганов. В 2016 г. эта цифра увеличилась более чем в 3,6 раза и составила 52,5 млн попыток взломать инфорРис. 2. Число абонентов мобильного широкополосного доступа в Интернет на 100 человек населения, чел. Источник: Федеральная служба государственной статистики : офиц. сайт. М., 2019. URL: <https://www.gks.ru/folder/14477> \(дата обращения: 14.11.2019\). Рис. 3. Доля организаций, использовавших Интернет, в общем числе обследованных организаций, % Источник: Федеральная служба государственной статистики : офиц. сайт. М., 2019. URL:](http://</a></p></div><div data-bbox=)

<https://www.gks.ru/folder/14477> (дата обращения: 14.11.2019). *Baikal Research Journal* электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6 мационные системы органов государственной власти<sup>3</sup>. Цель большинства атак — получение информации ограниченного доступа и нарушение функционирования технических средств [6]. Структура киберпреступлений по данным прокуратуры представлена на рис. 5. Наиболее значимый удельный вес в количестве преступлений в сфере информационных технологий занимает интернет-мошенничество [7]. В эпоху развития информационных технологий интернет является неким проводником в мир безграничной информации и зачастую простому пользователю затруднительно оценить степень достоверности информации, которую ему преподносят различные сайты и ресурсы. С другой стороны, мошенники, использующие возможности информационных технологий, имеют все возможности для обмана своих потенциальных жертв. Если в реальной жизни им зачастую приходится коммуницировать со своими жертвами, то в сети Интернет их личность остается в тени, тем самым создавая иллюзию невозможности идентификации преступника [8]. Также немаловажным следует признать и тот факт, что для совершения обмана в виртуальной реальности не обязательно обладать особыми навыками, и без них можно создавать сайты-однодневки с целью своего обогащения. Нелегальный контент, наоборот, имеет наименьшую долю в структуре киберпреступлений

по причине того, что в России у людей сформировано особое отношение к такого рода контенту. Нелегальным он считается только по закону, но в подсознании людей информация воспринимается как вполне легальная и пользоваться ею можно на безвозмездных началах по отношению к правообладателю. С нелегальным контентом борется служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, у данного органа есть 3 Статистика и аналитика // Министерство внутренних дел РФ. М., 2019. URL: <https://www.Deljatel-nost/statistics> (дата обращения: 17.11.2019). Рис. 4. Доля организаций, использовавших средства защиты информации, передаваемой по глобальным сетям, %  
Источник: Федеральная служба государственной статистики : офиц. сайт. М., 2019. URL: <https://www.gks.ru/folder/14477> (дата обращения: 14.11.2019). *Baikal Research Journal* электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6 полномочия блокировать и ограничивать доступ пользователей к нежелательному контенту. Примечательно, что доли преступлений примерно одинаковы независимо от масштаба предприятия [9]. Это связано с тем, что киберпреступники выбирают себе объект преступления в зависимости от степени защищенности информационных систем<sup>4</sup>. Самое главное правило защиты информационной системы предприятия заключается в следующем: деньги, выделяемые на защиту информационной безопасности не должны превышать стоимость и потенциальную ценность защищаемой информации. Другими словами, микропредприятие не<sup>43</sup> будет защищать свою информацию настолько же эффективно

(пропорционально затратам), насколько это делают крупные корпорации [там же]. Структура киберпреступлений против хозяйствующих субъектов представлена на рис. 6. Отсюда можно сделать вывод: более доступная информация является менее ценной и наоборот. Можно провести параллель с реальной жизнью: одни преступники крадут кошельки в метро, другие — используют различные схемы для максимизации своего дохода. И те, и другие находят себе жертву по своему «уму». Так, согласно отчету центра мониторинга и реагирования, на компьютерные атаки в кредитно-финансовой сфере (Департамент информационной безопасности Банка России), в 2018 г. более 97 % хищений со счетов физических лиц и 39 % хищений со счетов юридических лиц было совершено с использованием приемов социальной инженерии. Это приемы, с помощью которых преступник злонамеренно вводит в заблуждение свою жертву с помощью обмана или злоупотребления доверия

Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2018 / АО Лаборатория Касперского. URL: <https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/> (дата обращения: 17.11.2019). Рис. 5. Структура киберпреступлений, % Источник: Портал правовой статистики / Генеральная прокуратуры РФ. М., 2019. URL: <http://crimestat.ru/> (дата обращения: 15.11.2019). Baikal Research Journal электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguerp.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6 ем5. Отличительная

черта этого вида мошенничества — направленность на конкретные группы граждан: конечной целью злоумышленников является перевод средств жертв на собственные счета, при этом средства достижения этой цели варьируются. По данным МВД РФ, самыми популярными нарушениями в сфере информационных технологий являются нарушения по следующим статьям [10]: 272 УК РФ «Неправомерный доступ к компьютерной информации» (рис. 7), 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» (рис. 8), 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» (рис. 9)б. Неправомерный доступ к компьютерной информации наказывается уголовной ответственностью в случаях, когда это действие повлекло: 1) нарушение целостности (уничтожение или модификация информации); – нарушение конфиденциальности (копирование информации); – нарушение доступности (блокирование информации) [11]. Согласно данным статистики МВД за период с 2012 по 2018 гг. заметен нисходящий тренд расследований преступлений. Число зарегистрированных преступлений год от года варьируется, но остается на достаточно высоком уровне. На рис. 8 представлена статистика преступлений по ст. 273 УК РФ, с 2015 по 2018 гг. количество расследованных дел по отношению к зарегистрированным составляет около 50 %. Вредоносное программное обеспечение (далее — ПО) по-прежнему остается одним из основных инструментов компьютерных преступников. Пользователь чаще всего добровольно скачивает «пиратские» видеоигры, компьютерные программы, 5

Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента

информационной безопасности Банка России 1.09.2017 — 31.08.2018 // Банк России : офиц. сайт. М., 2019. URL: [https://www.cbr.ru/Content/Document/File/50959/survey\\_0917\\_0818.pdf](https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf) (дата обращения: 14.11.2019). 6 Статистика и аналитика // Министерство внутренних дел Российской Федерации. М., 2019. URL: <https://www.Deljatel-nost/statistics> (дата обращения: 17.11.2019). Рис. 6. Статистика по предприятиям, пострадавшим от кибератак, %  
Источник: Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2018 / АО Лаборатория Касперского. URL: <https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/> (дата обращения: 17.11.2019). Baikal Research Journal электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6 Рис. 7.  
Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) Источник: Статистика и аналитика // Министерство внутренних дел Российской Федерации. М., 2019. URL: <https://www.Deljatel-nost/statistics> (дата обращения: 17.11.2019). которые распространяются в сети Интернет бесплатно. Киберпреступник «взламывает» лицензионные платные программы, игры с целью встроить в них свое вредоносное ПО, при этом, пользователь ничего не подозревает. По такой схеме работает ПО, которое незаконно использует чужие вычислительные системы без ведома владельцев компьютеров. Расширение сферы безналичных расчетов повлекло за собой возникновение своеобразной криминальной индустрии, необходимой

для совершения несанкционированных операций по переводу денежных средств, в том числе с использованием платежных карт (рис. 9). Криминальные технологии постоянно совершенствуются, становясь доступными широкому кругу лиц, которые могут не обладать широкими познаниями в области информационных технологий [12]. Повышение доступности мошеннических схем и инструментов для их реализации ожидаемо влечет за собой рост числа незаконных транзакций. Так, в 2016 г. количество несанкционированных операций с использованием платежных карт выросло на 13,8 % (с 260 тыс. до 296 тыс.), а объем ущерба составил 1,08 млрд (1,15 млрд) р.  
7 В подавляющем большинстве, несанкционированные операции производятся «посредством сети Интернет и мобильных устройств, в том числе интернет-банкинга». Чаще всего (в 93 % случаев) такие операции означают использование электронных средств платежа (ЭСП) без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности аутентификационной информации. 7 Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2017 — 31.08.2018 // Банк России : офиц. сайт. М., 2019. URL: [https://www.cbr.ru/Content/Document/File/50959/survey\\_0917\\_0818.pdf](https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf) (дата обращения: 14.11.2019). Baikal Research Journal электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6  
Обеспечение экономической и информационной безопасности в условиях цифровой трансформации связано с рядом проблем. Быстро и активно развивающиеся информационные технологии, которые

активно используются мошенниками и злоумышленниками, заставляют государство и хозяйствующих субъектов совершенствовать системы защиты и противодействия возможным угрозам и повышать уровень информационной безопасности в целом. Однако, на сегодняшний день, это происходит медленно, и нарушители все чаще находят все более новые и изощренные способы совершения своих преступлений, которые труднее обнаружить и выявить. Исходя из этого, разработка возможных мер противодействия таким угрозам и повышения информационной безопасности становится все сложнее [13]. Экономическую безопасность государства нельзя обособлять от экономической безопасности хозяйствующего субъекта и отдельной личности, их обязательно нужно рассматривать в совокупности. Это связано с тем, что состояние защищенности экономической системы в целом определяется по самому слабо защищенному звену. Таким звеном в экономической безопасности государства является отдельный человек, и пока его безопасность будет на низком уровне, всегда будут иметь место вызовы и угрозы безопасности страны в целом. Растущая информатизация экономических процессов требует повышения уровня ее безопасности. В настоящее время практически у каждого человека есть компьютер, смартфон, имеющий выход в интернет. У каждого есть счет в банке, банковская карта и, чаще всего, есть мобильное приложение этого банка — это удобно, быстро и главное — без больших потерь времени, нервов и Рис. 8. Создание, использование и распространение вредоносных компьютерных программ Источник:

Статистика и аналитика // Министерство внутренних дел Российской Федерации. М., 2019. URL: <https://www.Deljatel-nost/statistics> (дата обращения: 17.11.2019). Baikal Research Journal электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6 Рис. 9. Мошенничество с использованием электронных средств платежа Источник: Статистика и аналитика // Министерство внутренних дел Российской Федерации. М., 2019. URL: <https://www.Deljatel-nost/statistics> (дата обращения : 17.11.2019). сил на походы непосредственно в банк. Это понимают и мошенники, желающие обогатиться за чужой счет преступным путем. Они различными путями «взламывают» личные кабинеты пользователей мобильных приложений банков, получают несанкционированный доступ к денежным средствам, персональным данным клиентов банков и реализуют свои злоумышленные цели. Но многие банки, крупные компании все чаще вводят новые способы защиты и повышения безопасности личных данных и электронных счетов своих клиентов. Это касается не только банков, но и других экономических субъектов рынка, которые, так или иначе, работают с информационными и компьютерными технологиями в процессе своей экономической деятельности. Распространение социальной инженерии способствует возможностям преступника получить несанкционированный доступ к персональным данным граждан и использовать их в своих корыстных целях. На сегодняшний день не составляет труда приобрести базы данных с номерами телефонов, ФИО, паспортными данными граждан на различных интернет-сайтах, телеграм-каналах. Несмотря на то, что в

Российской Федерации есть закон «О персональных данных», нарушение которого предусматривает уголовную и административную ответственность, количество совершаемых противозаконных деяний не снижается. Нарушители эффективно маскируются — этому способствует отсутствие прямого физического контакта нарушителя и потенциальной жертвы. В целях повышения информационной безопасности в условиях цифровой экономики, а, следовательно, и экономической безопасности страны, организации и человека в частности, можно предложить следующие меры: *Baikal Research Journal* электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6 1. Эффективное выполнение задач и мероприятий, предусмотренных стратегией развития информационного общества в РФ на 2017–2030 гг. и доктриной информационной безопасности РФ. 2. Повышение информированности населения о возможных угрозах в сфере цифровых технологий, о способах и видах мошенничества, в результате которых люди могут потерять свои деньги, о том, как избежать этого мошенничества, как повысить безопасность своих сбережений и персональных данных, которые являются целью злоумышленников. 3. Совершенствование нормативно-правовой базы в сфере обеспечения информационной безопасности, возможное ужесточение наказаний за совершение преступлений против экономической и информационной безопасности людей и страны. Также очень важно разработать новые

правовые нормы в отношении определенных случаев мошенничества, не охваченных существующими законами. 4. В современных условиях цифровой экономики каждая организация должна регулярно оценивать уровень своей информационной безопасности, осуществлять постоянный и всесторонний анализ возможных угроз и последствий от их реализации. Важными для организации должны быть вопросы о том, созданы ли условия для внедрения современных цифровых технологий по защите информации, эффективно ли осуществляется менеджмент в сфере обеспечения информационной безопасности, насколько рационально распределены финансовые ресурсы между кадровым обеспечением организации и цифровыми технологиями, направленными на защиту данных и т.п. 5. Усиление работы по блокировке сайтов, рассылок и call-центров мошеннических структур. 6. Построение взаимодействия с операторами не только мобильной связи и телеком-провайдерами, но и ip-телефонии и мессенджеров, а также повышение взаимодействия с профильными государственными органами [6]. 7. Составление банками и финансовыми организациями «белого списка» разрешенных к запуску программ на банкоматах. Программы не из этого списка не смогут быть запущены на банкоматах, следовательно, преступники не смогут внедрять вредоносное ПО в операционные системы банкоматов. Список использованной литературы 1. Ярочкин В.И. Информационная безопасность / В.И. Ярочкин. — Москва : Гаудеамус, 2014. — 802 с. 2. Коротков Э.М. Управление экономической безопасностью общества / Э.М. Коротков, А.А. Беляев // Менеджмент в России и за рубежом. — 2001. — № 6. 43 С. 9–25. 3. Гафнер В.В. Информационная безопасность : учеб. пособие / В.В. Гафнер.

- Ростов-на-Дону : Феникс, 2010. — 324 с. <sup>Параскуа Е. Т.</sup> 4. Жмуров Д.В. Эра милосердия. Пути развития преступности / Д.В. Жмуров, А.А. Протасевич, А.С. Костромина. — DOI 10.17150/2411-6262.2019.10(2) // Baikal Research Journal. — 2019. — Т. 10, № 2. — URL: <http://brj-bguer.ru/reader/article.aspx?id=23010>. 5. Блокчейн в цифровой криминологии: постановка проблемы / А.П. Суходолов, Е.А. Антонян, М.В. Рукинов [и др.]. — DOI 10.17150/2500-4255.2019.13(4).555-563 // Всероссийский криминологический журнал. — 2019. — Т. 13, № 4. — С. 555–563. 6. Булай Ю.Г. Профилактика и противодействие киберпреступности, а также международным киберугрозам / Ю.Г. Булай, Р.И. Булай // Академическая мысль. — 2017. — № 1. — С. 31–35. 7. Лагутин П.Д. Киберпреступность как актуальная угроза обществу / П.Д. Лагутин, Т.А. Миханова // Молодой ученый. — 2018. — № 42 (228). — С. 108–109. 8. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение / Д.Н. Карпова // Власть. — 2014. — № 8. — С. 46–50. Baikal Research Journal электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6 9. Котова Н.Н. Информационное обеспечение экономической безопасности бизнеса / Н.Н. Котова, В.В. Борчанинов // Вестник Южно-Уральского государственного университета. Серия: Экономика и менеджмент. — 2017. — Т. 11, № 1. — С. 20–27. 10. Овтин В.В. Особенности <sup>Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март</sup> неправомерного доступа к компьютерной информации по статье 272 УК РФ: ответственность и наказание / В.В. Овтин, В.В. Гудырев // Студенческий. — 2018. — № 8-4 (28). — С. 69–72. 11. Ларина Л.Ю. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру России / Л.Ю. Ларина // Актуальные вопросы борьбы с преступлениями. — 2017. — № 3. — С. 22–25. 12. Гольдяпина И.Ю. Система информационного законодательства: вопросы теории / И.Ю. Гольдяпина // Проблемы права. — 2014. — № 3 (46). — С. 95–99. 13. Никонов А.И. Системы защиты информации и их место в политике безопасности / А.И. Никонов, Н.О. Павлов // Вестник НГИЭИ. — 2016. — № 8 (63). — С. 48–54. References 1. Yarochkin V.I. Informatsionnaya bezopasnost' [Information Security]. Moscow, Gaudeamus Publ., 2014. 802 p. 2. Korotkov E.M., Belyaev A.A. Managing the Company's Economic Security. Menedzhment v Rossii i za rubezhom = Management in Russia and Abroad, 2001, no. 6, pp. 9–25. (In Russian). 3. Gafner V.V. Informatsionnaya bezopasnost' [Information Security]. Rostov-on-Don, Feniks Publ., 2010. 324 p. 4. Zhmurov D.V., Protasevich A.A., Kostromina A.S. The Era of Mercy. Ways of Criminality Development. Baikal Research Journal, 2019, vol. 10, no. 2. DOI: 10.17150/2411-6262.2019.10(2).18. Available at: <http://brj-bguer.ru/reader/article.aspx?id=23010>. (In Russian). 5. Sukhodolov A.P., Antonyan E.A., Rukinov M.V., Shamrin M.Yu., Spasennikova M.G. Blockchain in Digital Criminology: Problem Statement. Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology, 2019, vol. 13, no. 4, pp. 555–563. DOI: 10.17150/2500-4255.2019.13(4).555-563. (In Russian). 6. Bulai Yu.G., Bulai R.I. Cybercrime as Well as International Cyber Threats and Their Solution. Akademicheskaya mysl' = Academic Thought, 2017, no. 1, pp. 31–35. (In Russian). 7. Lagutin P.D., Mikhanova T.A. Cybercrime

as an Actual Threat to Society. Molodoi uchenyi = Young Scientist, 2018, no. 42 (228), pp. 108–109. (In Russian). 8. Karpova D.N. Cybercrime: a Global Challenge and its Solution. Vlast' = Power, 2014, no. 8, pp. 46–50. (In Russian). 9. Kotova N.N., Borchaninov V.V. The Information Support for the Economic Security of Business. Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Ekonomika i menedzhment = Bulletin of South Ural State University. Series: Economics and Management, 2017, vol. 11, no. 1, pp. 20–27. (In Russian). 10. Ovtin V.V., Gudyrev V.V. Features of Illegal Access to Computer Information Under Article 272 of the Criminal Code of the Russian Federation: Responsibility and Punishment. Studencheskii = Student, 2018, no. 8-4 (28), pp. 69–72. (In Russian). 11. Larina L.Yu. Criminal Liability for Unlawful Interference Critical Information Infrastructure the Russian Federation. Aktual'nye voprosy bor'by s prestupleniyami = Actual Issues of Fight Against Crimes, 2017, no. 3, pp. 22–25. (In Russian). 12. Golyapina I.Yu. System of Information Legislation: Issues of Theory. Problemy prava = Issues of Law, 2014, no. 3 (46), pp. 95–99. (In Russian). 13. Nikonov A.I., Pavlov N.O. Systems of Information Security and their Place in the Security Policy. Vestnik NGIEI = Bulletin NGIEI, 2016, no. 8 (63), pp. 48–54. (In Russian). Информация об авторах  
Бушуев Алексей Леонидович — студент, Байкальский государственный университет, Российская Федерация, г. Иркутск, e-mail: a.l.98bushuev@mail.ru.  
Деревцова Ирина Валерьевна — кандидат экономических наук, доцент, кафедра мировой экономики и экономической безопасности, Байкальский государственный университет, Российская Федерация, г.

Иркутск, e-mail: derevczovai@mail.ru.  
Baikal Research Journal электронный научный журнал Байкальского государственного университета 2020. Т. 11, № 1 2020, vol. 11, no. 1 <http://brj-bguer.ru> ISSN 2411-6262 DOI 10.17150/2411-6262.2020.11(1).6 Мальцева Юлия Алексеевна — студент, Байкальский государственный университет, Российская Федерация, г. Иркутск, e-mail: maltseva.iuliya@gmail.com. Терентьева Виктория Дмитриевна — студент, Байкальский государственный университет, Российская Федерация, г. Иркутск, e-mail: tervik@bk.ru. Авторы  
Aleksey L. Bushuyev — Undergraduate Student, Baikal State University, Irkutsk, Russian Federation, e-mail: a.l.98bushuev@mail.ru. Irina V. Derevtsova — PhD in Economics, Associate Professor, Chair of World Economy and Economic Security, Baikal State University, Irkutsk, Russian Federation, e-mail: derevczovai@mail.ru. Yulia A. Maltseva — Undergraduate Student, Baikal State University, Irkutsk, Russian Federation, e-mail: maltseva.iuliya@gmail.com. Viktoriya D. Terentyeva — Undergraduate Student, Baikal State University, Irkutsk, Russian Federation, e-mail: tervik@bk.ru. Для цитирования Роль информационной безопасности в условиях цифровой экономики / А.Л. Бушуев, И.В. Деревцова, Ю.А. Мальцева, В.Д. Терентьева. — DOI: 10.17150/2411-6262.20.11(1).6 // Baikal Research Journal. — 2020. — Т. 11, № 1. For Citation  
Bushuyev A.L., Derevtsova I.V., Maltseva Yu.A., Terentyeva V.D. Role of Information Security in Terms of Digital Economy. Baikal Research Journal, 2020, vol. 11, no. 1. DOI: 10.17150/2411-6262.20.11(1).6. (In Russian).  
**№ 8. Цифровые технологии и право**  
Внедрение цифровых технологий в современных условиях развития технологических процессов привело к кардинальному изменению качества

экономики. На современном этапе развития <sup>Лапаскья Г. Г.</sup> общественных отношений многие экономические процессы трансформируются на основе новых принципов управления, в основу которых заложены цифровые инновации, которые находят свое проявление в разных сферах. В связи с постоянно меняющимися экономическими процессами и динамичным развитием российского законодательства возникла необходимость законодательного регулирования основных механизмов и установления правовых режимов в сфере цифровых правоотношений. Цифровые технологии создают новую реальность, отличную от того физического мира, в котором мы живем. Они создают новую технологическую среду, в которой действует такой социальный феномен, как право, система права. Более того, цифровые технологии начинают диктовать свои условия, к которым необходимо адаптироваться правовым институтам, в том числе институтам гражданского права[1].

#### Реклама

Фундаментальные права человека, установленные Конституцией и международно-правовыми актами, конкретизируются в законодательстве на каждом историческом этапе развития страны. Очевидно, наступило время конкретизации прав и свобод человека и гражданина применительно к цифровой реальности[2].

Цифровые права человека — это конкретизация (посредством закона и правоприменительных, в том числе судебных, актов) универсальных прав человека, гарантированных <sup>Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март</sup> международным правом и конституциями государств, применительно к потребностям

человека и гражданина в обществе, основанном на информации. Задача государства — признавать и защищать цифровые права граждан от всевозможных нарушений, обеспечивая при этом конституционно-правовую безопасность личности, общества и государства[3]. Глобализация экономики проявляется в международном разделении труда национальных экономик. Российское промышленное производство (вся экономика в целом) находится в самом начале технологической цепочки. Особенно это наблюдается в настоящее время, когда промышленно развитые страны перешли от концепции "индустриальной экономики" к теории информационного общества. В условиях информационной экономики повышается значение глобальных, национальных и региональных информационных сетей. Принято говорить об электронной коммерции, интернет-бизнесе, об изменениях в информационных технологиях. Новые технологии существенно трансформируют не столько частный, сколько публичный сектор, сферу государственной деятельности. Благодаря новым цифровым технологиям формируется и новая среда правового регулирования, в которой можно выделить следующие ключевые технологические факторы:

- Интернет вещей, промышленный Интернет (Internet of things);
- искусственный интеллект (artificial intelligence) и машинное обучение и робототехника;
- технологии виртуальной и дополненной реальности (augmented reality), квантовые технологии и нейротехнологии;
- технологии на принципах распределенного реестра (blockchain), криптовалюты, токены, майнеры, смарт-контракты, ICO...;
- глобальные базы данных (big data);

— облачные компьютерные сервисы и вычисления (cloud computing);

— "умные" комплексы и устройства (smart everything);

— социальные сети (Facebook, VK, Twitter, Telegram...);

— киберпространство, интернет-торговля, киберспорт, киберфейк, "электронное правительство" и кибербезопасность[4].

Цифровые технологии способны менять образ права, влиять на его регулятивный потенциал и эффективность, открывать дорогу или блокировать его действие в новых измерениях социальной реальности.

Векторы и пределы таких изменений до конца не ясны. Вероятно, это подтверждение зарождения нового права — "права второго модерна".

Зарождается новое право, регулирующее отношения в контексте мира цифр и искусственного интеллекта[5].

Вопрос о понятии "цифровое право" является дискуссионным. Связано это прежде всего с тем, что в одном понятии или определении достаточно сложно отразить всю сущность глобальных изменений. Кроме того, едва ли возможно учесть динамику изменений в данной сфере.

Популярной ошибкой законодателя в цифровую эпоху стало стремление угнаться за происходящими изменениями путем регламентации всего нового, что попадает в его поле зрения. Как правило, такая регламентация начинается с выработки терминологического аппарата и жесткой классификации, которая помогает описать новую реальность.

Острые дискуссии о том, что такое большие данные, цифровые платформы, социальные сети или искусственный интеллект, не утихают уже несколько

лет. И в настоящее время можно констатировать, что дискуссии о том, что такое криптовалюты и цифровые права, стали значительной составляющей разговора о нормативном регулировании цифровой экономики[6].

Известный российско-советский ученый-правовед М.М. Агарков предупреждал: "Право не является самодовлеющей и замкнутой системой явлений, которая живет и изменяется по своим собственным внутренним законам"[7]. Анализируя состояние правовой науки на рубеже XIX и XX столетий, который М.М. Агаркову пришлось пережить, исследователь отмечал, что к началу XX в. "цельного миросозерцания уже не было, и наука должна была обратиться к основным вопросам гражданского права, проверить старые истины, откинуть отжившее, быть может, заново формулировать свои исходные положения".

Движущая сила, которая в наших социально-исторических условиях призвана быть драйвером развития правовой сферы, — это энергия государственного и общественного запроса. Однако действие этой силы как осязаемый феномен общественной жизни в современном социуме предельно ослаблено. Механизация права, превращение его в замкнутую систему, которая живет и изменяется по своим собственным внутренним законам, стали историческим фактом индустриальной эпохи. Снижение адаптивности в силу его механизации и превращения в замкнутую систему делает право малоприспособленным к современным условиям[8].

Изменению под воздействием цифровых технологий подвергаются все компоненты права.

Традиционно субъектами права являются физические лица, юридические лица

(организации), государство. Однако в условиях цифровизации технологически обусловлено появление новых субъектов, например роботов. Европейским парламентом уже одобрены нормы гражданского права о робототехнике (16 февраля 2017 г.). Появляется новая "цифровая личность", новый субъект права наряду с человеком[9].

Существенные изменения наблюдаются и в таком компоненте права, как объект. Информация становится универсальным объектом права, существующим в любой правовой отрасли[10]. Более того, появляются новые объекты гражданских прав. Так, в настоящее время мы можем констатировать, что по поводу цифровых финансовых активов (или цифровых прав) — своего рода неюридических субстанций выражаются интересы и выстраивается взаимное поведение субъектов гражданских отношений, что является необходимой предпосылкой возникновения, существования, развития и осуществления гражданского права как такового. Как известно, невещественные материальные объекты, будучи дискретными образованиями, проявляют свою юридическую привязку особым образом: чаще всего инструментально, через принадлежность определенным субъектам источников или средств передачи и получения соответствующих энергий и воздействий. Дальнейшее развитие системы объектов гражданских прав приведет к включению таких объектов в имущественную группу в качестве промежуточной (между вещами и имущественными правами) объектной категории[11].

Динамичнее всего развиваются и подвергаются изменениям в связи с технологическим фактором общественные отношения.

Цифровизация экономики оказывает существенное влияние на сферу правового регулирования. Между субъектами правоотношений начинают складываться новые общественные отношения. Так, в сфере правового регулирования наблюдается появление отношений:

- 1) субъектами которых являются виртуальные или цифровые "личности";
- 2) связанных с юридически значимой идентификацией личности в виртуальном пространстве;
- 3) возникающих в связи с реализацией прав человека в виртуальном пространстве (право на доступ в Интернет, право на забвение, право на "цифровую смерть" и др.);
- 4) ориентированных на применение робототехники;
- 5) складывающихся по поводу нетипичных объектов — информации, цифровых технологий (финтех, регтех и др.), создаваемых посредством применения новых цифровых сущностей (криптовалюты) и объектов материального мира, а также связанных с использованием и оборотом того и другого;

б) сопряженных:

- с использованием оцифрованных информационных массивов — информационных баз данных;
- переводом в цифровую форму действий и операций, посредством которых реализуются государственные функции, оказываются государственные и муниципальные услуги, обеспечивается электронное участие граждан в управлении обществом и государством;
- совершением действий в виртуальном пространстве, направленных на возникновение, изменение и прекращение правоотношений, реализацию прав и

исполнение обязанностей, образующих их юридическое содержание;

— применением автоматизированных действий (Интернетом вещей), обеспечением информационной безопасности и др.[12]

Сфера правового регулирования становится мультисодержательной — в ее пределах не просто возникают новые отношения, но существенно изменяется ее структура, модифицируются сложившиеся связи[13].

Указанную сферу образуют как типичные, так и нетипичные для нее с точки зрения субъектного состава, объектов и среды существования общественные отношения, включая те, которые практически исключают непосредственное участие человека. Все чаще возникают общественные связи и отношения, составы фактических обстоятельств, а также события, происходящие помимо воли людей. В структуре сферы правового регулирования появился новый элемент — отношения, которые должны, но на данном этапе объективно не могут быть урегулированы правом в необходимом объеме.

Таким образом, вышеперечисленные направления деятельности в области применения цифровых технологий свидетельствуют о том, что в настоящее время формируется цифровое пространство.

Изменения происходят не только в общественных отношениях, регулируемых правом, но и, как следствие, в методах правового регулирования. Современный этап развития гражданского общества свидетельствует о происходящей

трансформации принципов и методов регулирования общественных и экономических отношений.

С общетеоретических позиций метод правового регулирования общественных отношений — это способы (приемы, средства) воздействия права на поведение людей. Эта точка зрения является господствующей в отечественной правовой науке. Профессор С.С. Алексеев пишет: "Он (метод. — В.Б.) представляет собой особые способы, средства, приемы, используемые при правовом регулировании определенного, качественно своеобразного вида общественных отношений"[14]. Причем метод правового регулирования — это совокупность способов (средств, приемов).

Аналогичной точки зрения придерживаются и представители отраслевых наук. Профессор В.Ф. Яковлев определяет гражданско-правовой метод регулирования общественных отношений как совокупность приемов (способов) воздействия отрасли на поведение людей[15]. По его мнению, правонаделение — главная сущностная черта гражданско-правового метода.

Существует и иное мнение по рассматриваемому вопросу. Например, профессор О.С. Иоффе и профессор М.Д. Шаргородский при определении метода регулирования видят в нем выражение какого-либо одного способа опосредования общественных отношений[16].

В современном обществе усиливаются тенденции к укреплению самоуправленческих начал и саморегулированию в управлении различными общностями и процессами. Появление разного рода виртуальных сообществ — не что иное, как свидетельство стремления определенных групп людей выйти из-под жесткой государственной регуляции. В этих условиях оказались весьма востребованы общинная и кооперативная модели организации человеческого взаимодействия. Именно по их образу и

подобно нередко формируются сетевые сообщества, потенциально способные образовывать саморегулируемую криптосреду[17].

Таким образом, важнейшим средством наметившихся преобразований является организация различных форм саморегулирования.

Саморегулирование — это институт, в рамках которого группой экономических агентов создаются, адаптируются и изменяются легитимные (не противоречащие установленным государством) правила, регулирующие хозяйственную деятельность этих агентов, и объекты регулирования имеют возможность легитимно управлять поведением регулятора (контролера)[18]. Частное право дает формы экономического саморегулирования практически во всех своих институтах, при этом саморегулирование становится проявлением метода правового регулирования в гражданском праве. В связи с этим следует применять такие средства и методы, которые бы дополняли и укрепляли иные формы социального регулирования. Во многом решение этой задачи будет зависеть от реального соотношения частного и публичного интересов в рассматриваемом сегменте правового регулирования.

Вслед за изменением сферы правового регулирования меняется и содержание права.

Появление новых общественных отношений вызывает к жизни новые юридические нормы, ведет к изменению или отмене уже действующих.

Сейчас можно констатировать наличие следующих тенденций и процессов:

1) в праве появляются новые понятия и легальные дефиниции, фиксирующие

цифровые личности и сущности, образующие ядро будущих правовых институтов;

2) более интенсивно задействована регулятивная статическая функция права, обеспечивающая закрепление и

оформление новых правовых институтов;

3) конкретизируются права человека, что создает иллюзию возникновения нового вида прав — цифровых[19];

4) для целей создания цифровой экономики широко применяются инструменты публичного права;

5) динамично изменяется композиция модели нормативного правового регулирования (соотношения в ней законов и подзаконных актов);

б) по сути, происходит перенастройка законодательства на решение задач, возникших в связи с цифровизацией, посредством "цифровой прививки" гражданскому, трудовому, административному, уголовному и многим другим отраслям законодательства. Изменения наблюдаются и в сфере реализации права. Многие юридически значимые действия совершаются в виртуальном пространстве — заключение сделок, удостоверение юридически значимых фактов и др. В процессе реализации права все чаще используются цифровые технологии (блокчейн, "умные" самоисполняющиеся контракты и др.), изучается возможность применения вновь возникающих технологий, например, в РАН, Сколково. При осуществлении отдельных видов деятельности людей постепенно заменяют роботы, происходит роботизация и технологизация юридической деятельности. Коренные изменения зафиксированы в познавательной-доказательственной составляющей судебного процесса, вводятся новые виды доказательств (электронные доказательства, в частности

цифровые следы), а также судебных экспертиз [20].

Очевидно, что в системе права назрели изменения. И перемены более кардинальные, нежели это представляется в теории права. Речь не просто о дискуссиях о системе права, о том, какие отрасли ее составляют и сколько их, по каким критериям они выделяются. Проблема одновременно и глубже, и видна невооруженному глазу. Наступление новых технологий способно вовсе переформатировать право, само это понятие, феномен, его содержание, механизм действия и проч. и систему права соответственно [21].

В этой связи особый интерес представляет рассмотрение проблемы единства российского частного права и такого явления, как дуализм права. Соотношение публичного и частного права имеет и практическое значение, так как в правоприменительной практике субъектам права необходимо руководствоваться конкретными нормами, обладающими отраслевой принадлежностью. На этом фоне существуют режимы публичного и частного права.

Надо согласиться с мнением С.С. Алексеева о том, что публичное и частное право — это не отрасли, а целые сферы, зоны права (суперотрасли). При чем такое деление права не только и, пожалуй, даже не столько классификационное, сколько концептуального порядка. Оно касается самих основ права, его места и роли в жизни людей, его определяющих ценностей [22]. С этой точки зрения выделение публичного и частного права в их чистом виде позволяет провести разграничение между ними и соответствующими отраслями объективного права.

На протяжении двадцатого столетия в советской юридической литературе сложилась устойчивая позиция, в соответствии с которой критериями определения отраслей права являются предмет и метод правового регулирования общественных отношений. В настоящее время в юридической науке определилась тенденция расширить перечень отраслей права, обосновать отраслевой статус институтов права и подотраслей права [23]. Представляется, что цифровизация права усугубляет общую проблему о критериях, позволяющих отнести ту или иную отрасль (институт) к публичному либо частному праву. Отметим, что в юридической литературе было предложено несколько теоретических конструкций по данной проблеме, среди которых можно выделить три основные концепции: теорию интереса, теорию метода, теорию предмета правового регулирования [24]. Вместе с тем ни одна из рассматриваемых концепций не позволяет провести четкое разграничение между публичным и частным правом. Цифровизация катализирует стирание граней между отраслями права. Информация и технологии — уже в каждой отрасли, они становятся общим знаменателем и способны определять единую логику права. Ценность отраслевых границ снижается в правовой практике, что неминуемо влияет и на теорию права [25]. Таким образом, право на пороге перемен под влиянием технологического фактора. Выделяемые в теории основные признаки права (система общеобязательных норм, санкционированных государством, выражающих государственную волю и обеспечиваемых государством) в цифровую эпоху теряют прежний смысл [26]. Мы являемся свидетелями формирования новой отрасли права — цифрового права.

В этой связи стоит отметить, что в дискуссии по вопросам системы права ряд ученых встали на путь отрицания отраслей права (Ц.А. Ямпольская, Р.З. Лившиц, И.А. Танчук). Представители данного направления в науке предлагали отойти от отрасли права и признать систему законодательства и отрасль законодательства. Однако данное направление не нашло своего закрепления в науке и не обрело большого числа последователей [27]. Возможно, именно сейчас данные концепции находят свою актуальность. Г.Ф. Шершеневич справедливо указывал, что теоретическая, педагогическая и практическая причины приводят к необходимости разделить действующее право по отделам [28]. Если следовать вышеуказанной логике, то система российского права состоит из отдельных отраслей права, между которыми постоянно проходят тектонические процессы, одни отрасли права умирают, но появляются другие отрасли [29].

Рассуждая о понятии цифрового права как самостоятельной отрасли, этапе, следует помнить, что главным является единство системы права, которое обеспечивается, во-первых, непротиворечивостью содержания правовых норм; во-вторых, системой конкретного государства, которое заинтересовано в единстве и устойчивости; в-третьих, единством целей и задач; в-четвертых, самим внутренним единством системы [30].

На данный момент уже существуют все его признаки: нормативность (устанавливает правила поведения общего характера); общеобязательность (действие распространяется на всех либо на большой круг субъектов); гарантированность государством

(подкреплено мерами государственного принуждения); интеллектуально-волевой характер (право выражает волю и сознание людей); формальная определенность (нормы права выражены в официальной форме); системность (право — это внутренне согласованный, упорядоченный организм).

Вместе с тем представляется преждевременным вывод о самостоятельности цифрового права. Однако теоретические, педагогические и практические причины приводят к необходимости предложения понятия цифрового права.

Процесс формирования новой отрасли цифрового права фактически и представляет собой "цифровизацию" права, которая будет иметь постоянную тенденцию к увеличению.

Итак, цифровое право — система общеобязательных, формально-определенных, гарантированных государством правил поведения, которая складывается в области применения или с помощью применения цифровых технологий и регулирует отношения, возникающие в связи с применением цифровых технологий.

С точки зрения отраслевого подхода цифровое право — это отрасль права, объединяющая правовые нормы, регулирующие отношения, возникающие в связи с приобретением, осуществлением и отчуждением цифровых прав, а также с применением цифровых технологий физическими и юридическими лицами. В перспективе в силу логики процесса цифровизации объективно складываются предпосылки для формирования нового направления правового регулирования — цифрового права, которое будет включать систему нормативных актов, технических регламентов и норм, соглашений участников внутри технологических платформ для обеспечения стабильности и

развития цифрового гражданского оборота. При формировании цифрового права как самостоятельного направления правового регулирования, с точки зрения автора, оправдан подход с использованием цифровых технологий, технологических платформ (комплекса цифровых технологий), объединяющих информационные, коммуникационные, производственные и иные современные технологии, для регулирующего воздействия на цифровой гражданский оборот. Цифровое право в объективном смысле представляет собой структуру нормативных правовых актов (включая международные договоры в области цифрового гражданского оборота) и акты локального действия (правила, соглашения) в технологических платформах. Цифровое право регулирует сферу цифрового гражданского оборота с участием нематериальных цифровых объектов, обладающих объявленной или действительной коммерческой ценностью (экономическим содержанием), признаваемых законом и основанных на принципах создания и действия комплексных технологий (технологических платформ) распределенного реестра или иных цифровых технологий (искусственный интеллект, виртуальная и дополненная реальность, криптовалюты и токены, облачные вычисления и др.) [31]. Цифровая экономика в настоящее время находится в стадии своего становления и развития, многие экономические и технологические модели отношений не являются устоявшимися, что следует принимать во внимание при разработке понятия "цифровое право". Однако сущность правового регулирования никогда не исчерпывается естественными законами

экономического развития. Право нельзя лишить ценностного измерения, это не точная наука. Общество в цифровой экономике может быть очень разным, и, как показывает практика, его спонтанное развитие, как правило, приводит к росту неравенства. Поэтому перенастройка правового регулирования, его адаптация к динамическим процессам цифровизации не исключает, а напротив, делает неизбежным определенный телеологический и ценностный выбор [32]. Это означает, что правовая политика должна опираться на определенные идеалы и развиваться в единстве с экономической и социальной политикой.

#### Литература

1. Агарков М.М. Ценность частного права / М.М. Агарков // Сборник трудов профессором и преподавателей Государственного иркутского университета. Отд. 1: Науки гуманитарные. Вып. 1. Иркутск, 1921. 173 с.
2. Алексеев С.С. Общие теоретические проблемы системы советского права / С.С. Алексеев. Москва: Госюриздат, 1961. 187 с.
3. Алексеев С.С. Предмет советского социалистического гражданского права / С.С. Алексеев // Ученые труды Свердловского юридического института. Т. 1. Серия "Гражданское право" / Свердловск, 1959. 336 с.
4. Алексеев С.С. Частное право: Научно-публицистический очерк / С.С. Алексеев. Москва: Статут, 1999. 157 с.
5. Зорькин В.Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума / В.Д. Зорькин // Российская газета. 2018. 29 мая.
6. Иванов А.Ю. Законотворчество и правовая основа цифрового будущего: вызовы и решения / А.Ю. Иванов // Аналитические материалы к рабочим мероприятиям форума "Развитие

- парламентаризма" (г. Москва, 1 — 3 июля 2019 г.). Москва, 2019. С. 18 — 25.
7. Карцхия А.А. Гражданско-правовая модель регулирования цифровых технологий: Диссертация доктора юридических наук / А.А. Карцхия. Москва, 2018. 394 с.
8. Карцхия А.А. Цифровое право как будущее классической цивилистики / А.А. Карцхия // Право будущего: Интеллектуальная собственность, Инновации, Интернет: ежегодник. Т. 1 / Ответственный редактор Е.Г. Афанасьева. Москва: ИНИОН РАН, 2018. С. 26 — 40.
9. Крючкова П.В. Саморегулирование как дискретная институциональная альтернатива регулирования рынков: Диссертация доктора экономических наук / П.В. Крючкова. Москва, 2005. 283 с.
10. Кулагин М.И. Предпринимательство и право: опыт Запада / М.И. Кулагин; Предисловие и научное редактирование Е.А. Суханова. Москва: Дело, 1992. 142 с.
11. Лапач В.А. Система объектов гражданских прав в законодательстве России: Диссертация доктора юридических наук / В.А. Лапач. Ростов-на-Дону, 2002. 537 с.
12. Право будущего: Интеллектуальная собственность, Инновации, Интернет: Ежегодник. Т. 1 / Ответственный редактор Е.Г. Афанасьева. Москва: ИНИОН РАН, 2018. 207 с.
13. Радько Т.Н. Теория государства и права: Учебник / Т.Н. Радько. 2-е изд. Москва: Проспект, 2010. 744 с.
14. Свирин Ю.А. Когерентность системы права / Ю.А. Свирин // Актуальные проблемы российского права. 2015. № 6(55). С. 50 — 55.
15. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы / Э.В. Талапина // Журнал российского права. 2018. № 2(254). С. 5 — 17.
16. Хабриева Т.Я. Право в условиях цифровой реальности / Т.Я. Хабриева, Н.Н. Черногор // Журнал российского права. 2018. № 1. С. 85 — 102.
17. Хачатуров Р.Л. Становление отраслей права Российской Федерации / Р.Л. Хачатуров // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. № 1(41). С. 91 — 97.
18. Шаргородский М.Д. О системе советского права / М.Д. Шаргородский, О.С. Иоффе // Советское государство и право. 1957. № 6. С. 101 — 110.
19. Шершеневич Г.Ф. Общая теория права. В 2 томах. Т. 1. Вып. 1: Учебное пособие (по изданию 1910 — 1912 гг.) / Г.Ф. Шершеневич; Автор предисловия М.Н. Марченко. Москва: Юридический колледж МГУ, 1995. 446 с.
20. Яковлев В.Ф. Гражданско-правовой метод регулирования общественных отношений: Учебное пособие / В.Ф. Яковлев; Научное редактирование Г.И. Петрищева. Свердловск, 1972. 212 с.
- 
- [1] Карцхия А.А. Цифровое право как будущее российской цивилистики // Право будущего: Интеллектуальная собственность, Инновации, Интернет: ежегодник. Т. 1 / Отв. ред. Е.Г. Афанасьева. М.: ИНИОН РАН, 2018. С. 26 — 40.
- [2] Зорькин В.Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума. URL: <https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html>.
- [3] Там же.
- [4] Карцхия А.А. Цифровое право как будущее классической цивилистики.

- [5] Зорькин В.Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума. Паваскья Г. Т.
- [6] Иванов А.Ю. Законотворчество и правовая основа цифрового будущего: вызовы и решения. Аналитические материалы к рабочим мероприятиям форума, 1 — 3 июля 2019 г. Москва. 2019. С. 18 — 25.
- [7] Агарков М.М. Ценность частного права // Сборник трудов профессоров и преподавателей Государственного иркутского университета. Вып. 1. Иркутск, 1920. С. 4.
- [8] Иванов А.Ю. Законотворчество и правовая основа цифрового будущего: вызовы и решения.
- [9] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. N 2(254). С. 5 — 17.
- [10] Там же.
- [11] Лапач В.А. Система объектов гражданских прав в законодательстве России: Дис. ... д-ра юрид. наук. Ростов н/Д., 2002. С. 20.
- [12] Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. N 1. С. 85 — 102.
- [13] Там же.
- [14] Алексеев С.С. Общие теоретические проблемы системы советского права. М.: Госюриздат, 1961. С. 48; Он же. Предмет советского социалистического гражданского права // Ученые труды. Серия "Гражданское право". Свердловск, 1959. Т. 1. С. 258.
- [15] Яковлев В.Ф. Гражданско-правовой метод общественных отношений. Свердловск, 1972. С. 64 — 84.
- [16] Шаргородский М.Д., Иоффе О.С. О системе советского права // Советское государство и право. 1957. N 6. С. 104. Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март
- [17] Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности.
- [18] Крючкова Н.В. Саморегулирование как дискретная институциональная альтернатива регулирования рынков: Дис. ... д-ра экон. наук. М., 2005. С. 14.
- [19] Зорькин В.Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума.
- [20] Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности.
- [21] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы.
- [22] Алексеев С.С. Частное право: научно-публицистический очерк. М.: Статут, 1999. С. 23 — 27.
- [23] Хачатуров Р.Л. Становление отраслей права Российской Федерации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. N 1(41). С. 91 — 97.
- [24] Кулагин М.И. Предпринимательство и право: опыт Запада. М.: Дело, 1992. С. 101.
- [25] Там же.
- [26] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы.
- [27] Свирин Ю.А. Когерентность системы права // Актуальные проблемы российского права. 2015. N 6.
- [28] Шершеневич Г.Ф. Общая теория права. М.: Юридический колледж МГУ, 1995. Т 2. Вып. 4. С. 446.
- [29] Свирин Ю.А. Когерентность системы права.
- [30] Радько Т.Н. Теория государства и права. М.: Проспект, 2010. С. 386.
- [31] Карцхия А.А. Правовое регулирование гражданского оборота с использованием цифровых технологий: Дис. ... д-ра юрид. наук. М., 2018. С. 280.
- [32] Иванов А.Ю. Законотворчество и правовая основа цифрового будущего: вызовы и решения.

## № 9. Электронный бюджет. Понятие, правовой статус и порядок функционирования.

Портал «Открытые бюджеты» ([budget.egov.kz](http://budget.egov.kz)) – компонент проекта «Открытое правительство», создан для обеспечения прозрачного формирования бюджета и развития общественного контроля над расходованием бюджетных средств.

Согласно Закону «[О доступе к информации](#)» на портале государственные органы и учреждения законодательной, исполнительной и судебной ветвей власти, местного государственного управления и самоуправления размещают бюджетную отчетность, консолидированную финансовую отчетность, результаты государственного аудита и финансового контроля, а также проводится публичное обсуждение проектов бюджетных программ и отчетов об их реализации.

Комментарии, замечания и предложения может оставлять каждый гражданин Республики Казахстан, заинтересованный в вопросах расходования бюджета.

### Работа с порталом

Для того, чтобы ознакомиться с информацией о реализации бюджетных программ, необходимо нажать на вкладку «Бюджетные программы» и выбрать соответствующий подраздел: «[Проект](#)», «[Утвержденные программы](#)» или «[Отчеты о реализации](#)».

В открывшемся окне появится список всех доступных документов выбранной категории, который можно отфильтровать по центральным государственным и местным исполнительным органам.

Перейдя на страницу интересующей бюджетной программы, вы ознакомитесь с её полным описанием, каждый пункт которого доступен для

комментирования. Также, здесь можно скачать исходный документ в формате Excel:

Для комментирования необходима авторизация, которая в свою очередь требует наличия регистрации на портале электронного правительства eGov.kz. Подробности этой процедуры описаны в разделе «[Регистрация нового пользователя на портале](#)» электронного правительства.

В разделе «[Материалы](#)» собраны данные по консолидированной финансовой отчетности, бюджетной отчетности государственных органов, и информации о результатах государственного аудита и финансового контроля.

Консолидированная финансовая отчетность в свою очередь состоит из следующих документов:

- Консолидированный бухгалтерский баланс;
- Консолидированный отчет о результатах финансовой деятельности;
- Консолидированный отчет о движении денег (прямой метод);
- Консолидированный отчет об изменениях чистых активов/капитала;
- Пояснительная записка к консолидированной финансовой отчетности.

Бюджетная отчетность включает в себя:

- Отчеты об исполнении местных бюджетов;
- Отчеты об исполнении республиканского бюджета;
- Отчеты об исполнении государственного бюджета;
- Отчеты об исполнении консолидированного бюджета;
- Отчеты об исполнении бюджетов областей;
- Отчеты о реализации бюджетных программ;

- <sup>Папаскув Г. Т.</sup> Отчеты о реализации стратегического плана;
- Отчеты о поступлениях и расходах каждого государственного органа; использования Национального Фонда РК.

На странице отчета отображается тип бюджета, наименование ГО, дата утверждения и актуальности, сам отчет, ссылка на скачивание документов.

В разделе «[Архив](#)» собраны все проекты, утвержденные программы и отчеты о реализации бюджетных программ, по которым уже прошли публичные обсуждения.

[Лекция по учебной программе семинара по курсу "Открытое правительство"](#)

## ИНФОРМАЦИОННАЯ СИСТЕМА ГОСУДАРСТВЕННОГО ПЛАНИРОВАНИЯ

### ИС ГП

Информационная система государственного планирования (бюджетного планирования) (далее – ИСПП) предназначена для информационной поддержки деятельности уполномоченного органа и направлена на создание эффективного механизма, способствующего решению задач в сфере бюджетного планирования.

### Цель

Полная автоматизация процедуры бюджетного планирования в части автоматизации процессов формирования бюджетных заявок государственных органов, исключая бумажный документооборот.

### Задачи

ведение единой бюджетной классификации с применением новых методов и принципов;

централизованное ведение коэффициентов и нормативов, необходимых для расчета каждого государственного органа;

централизованное формирование и доведение лимитов расходов и лимитов на новые инициативы до каждого государственного органа;

централизованное формирование прогноза штатного расписания на трехлетний период планирования;

централизованное формирование бюджетных заявок с мест возникновения затрат с автоматической консолидацией на вышестоящих уровнях;

прикрепление пояснительных документов и обоснований к каждому виду расходов;

централизованный доступ к данным для вышестоящих уровней на любом этапе формирования бюджета;

автоматизированное формирование заключений по бюджетным заявкам администраторов бюджетных программ;

автоматизированные процедуры подготовки заключений рабочего органа для рассмотрения на РБК;

автоматизированная процедура балансировки доходов и расходов и формирования проекта Закона о РБ;

автоматизированное формирование аналитической и регламентной отчетности;

бесбумажный документооборот за счет применения механизмов ЭЦП на каждом этапе формирования бюджета и, как следствие, снижение срока формирования и утверждения бюджета.

### Проделанная работа

В рамках исполнения Плана реализации проекта «Развитие Информационной системы государственного планирования (Бюджетное планирование)» (далее – План), утвержденного Вице-министром <sup>43</sup> Министерства финансов РК Енсебаевым Р.С., разработанного в рамках исполнения

протокольного поручения Заместителя Премьер-Министра РК от 13 октября 2017 года по вопросам информатизации Правительства и переходу на безбумажный документооборот, а также реализации пункта 50 Плана мероприятий по цифровизации Министерства финансов РК по оказанию государственных услуг госорганам и бизнесу, в 2019 году проведены следующие мероприятия:

Обучение более 250 сотрудников АБП по пользованию новым функционалом;

Создана единая техническая поддержка пользователей по многоканальному телефонному номеру +7 (7172) 91-94-44;

Тиражирование и внедрение ИСГП на все центральные государственные органы с обеспечением доступа в сети Интернет по адресу [planning.gov.kz/isbp/](http://planning.gov.kz/isbp/), которые успешно завершили ввод данных по формированию республиканского бюджета на 2019-2022 годы в электронном формате;

Актуализирована ЕБК в соответствии с приказом Министра финансов Республики Казахстан от 18 сентября 2014 года № 403 «Некоторые вопросы Единой бюджетной классификации Республики Казахстан» с учетом обновлений по состоянию на 18.04.2019 года;

Подключено около 4000 пользователей, более 1000 ГУ, 35 АБП.

История

2021

Развитие Информационной системы государственного планирования (II этап), в том числе:

разработка модуля «Прогнозная консолидированная финансовая отчетность» (2-ой этап);

-разработка нового модуля «Государственные инвестиционные проекты» в части функционала по автоматизации процессов заполнения и корректировки форм Паспортов ГИПов, их утверждения и передачи в бюджетную заявку;

реализация интеграций с другими информационными системами МФ РК, а также с ГБД ЮЛ и ИС Госэкспертизы;

Модификация функционала подсистемы «Стратегическое планирование» по модулям «Национальные проекты», «Концепция развития», «План развития государственных органов», «Программа развития регионов»;

Проведение пилота в подсистеме «Стратегическое планирование»;

Обучение 441 сотрудника АБП и их структурных подразделений по пользованию функционалом подсистемы «Стратегическое планирование» ИСГП (БП) (300), по модулю «ФУПФ» (141);

Модификация функционала модулей «Бюджетная заявка», «Балансировка», «Штатное расписание» и «РБК».

2020

Развитие Информационной системы государственного планирования (I этап);

Создание новых модулей: Открытые бюджеты, Формирование и уточнение планов финансирования, Прогнозная консолидированная финансовая отчетность;

Подсистема: Стратегическое планирование.

2019

Модернизация ИСГП с учетом новых требований;

Тиражирование на все центральные государственные органы;

Модификация функционала ИСГП по итогам тиражирования;

Подготовка бюджета на сопровождение обновленной версии ИСПП и внедрение в республиканских государственных учреждениях;

к Системе было подключено около 4000 пользователей, более 1000 ГУ, 35 АБП.

2018

Ввод в эксплуатацию Системы на платформе Open Source (СУБД на PostgreSQL);

Сопровождение и администрирование системы;

Пилотная эксплуатация обновленной Системы (версии 2.0, в рамках исключения бумажного документооборота);

Подготовка нормативно-правовой основой для перехода на безбумажное бюджетное планирование.

2017

Проведение испытаний и аттестация ИСПП на соответствие требованиям информационной безопасности;

Ввод ИСПП в промышленную эксплуатацию на платформе Oracle;

Общее количество пользователей системы 260 пользователей и участвующих государственных учреждений 30.

2007

Создание, сопровождение, администрирование системы ИСПП осуществлялось на платформе Oracle.

## **№ 10. Организация финансового контроля в условиях цифровизации финансовых правоотношений.**

Введение и постановка проблемы

Цифровизация финансового контроля,

представляющая собой «комплексную правовую и институциональную

трансформацию»<sup>3</sup>, в целом

положительно сказывается на развитии

финансового законодательства.

Обеспечивающие государственное

управление информационные системы и цифровые сервисы [3] упрощают порядок

сбора, обработки и хранения информации о финансово-хозяйственной деятельности

подконтрольных субъектов, а также приво<sup>3</sup>

Digital Transformation of Tax and Customs Administrations. World Bank, Washington, DC. URL:

<https://openknowledge.worldbank.org/handle/10986/37629> (дата обращения:

20.04.2022). дят к сокращению

административных процедур, долгое время нивелирующих обязательственный характер финансовых правоотношений.

Вместе с тем ключевая цель развития финансового контроля, заключающаяся в

формировании эффективной модели взаимодействия контролирующих и

подконтрольных субъектов, пока не

достигнута. В частности, не вписывается в

параметры финансового контроля рынок

цифровых финансовых услуг, основанный на регуляторных «песочницах»,

бросающих вызов существующему

правовому регулированию. А основанные

на информационных системах новые

инструменты контрольно-надзорной

деятельности фактически приводят к

формированию закрытой системы

взаимодействия контролирующих и

подконтрольных субъектов. Например, на

сегодняшний день отсутствует единая база

по мотивированным мнениям налоговых

органов, 5 Цифровизация финансового

контроля: правовое регулирование

Правовая информатика № 3 – 2022

сформированным в рамках взаимно

согласительных процедур при проведении

горизонтального налогового мониторинга.

Внедрение информационных систем в

механизм осуществления контроля не

является панацеей в борьбе с

неэффективными инструментами

государственного управления. Требуют

конкретизации и приведения в соответствие с принципами государственного управления составляющие систему обратных связей формы осуществления финансового контроля, к числу которых относятся мониторинг, надзор, аудит, бухгалтерский и статистический учет и др. Эти и другие проблемы в сфере осуществления финансового контроля являются предметом острых политических дискуссий, научных исследований и требуют разрешения. Публичный финансовый контроль Финансовый контроль, представляющий собой «...разновидность государственно-властных полномочий, осуществляемых органом государства в публично-правовом порядке»<sup>4</sup> — явление емкое и многоликое. Финансовому контролю посвящено большое количество научных исследований. Заметим, однако, что этот институт изучается как вид управленческой деятельности, который, как любая деятельность, вообще не является предметом науки права. По меткой оценке В.М. Сырых, только те или иные отношения, но не контрольная деятельность как таковая служат объектом юридического анализа [14]. В силу этой причины правоотношения, возникающие в ходе финансового контроля, остаются малоизученными, что негативно сказывается как в целом на правовом регулировании, так и на эффективности цифровых методов контроля. Поэтому успех цифровизации финансового контроля во многом зависит от точности учета особенностей складывающихся здесь правоотношений и отражения этих особенностей в применяемых юридических конструкциях. Главный дефект господствующей конструкции

финансового контроля — ориентация на проверку как на контрольную деятельность, охватывающую действия (бездействие) подконтрольного субъекта. Таким образом, осуществление контроля, вытекающее из всех его функций, ограничивается возможностью совершения неких технических действий — проверочных мероприятий. К ним на практике относят простую проверку, выездную проверку, документальную проверку, рейды, контрольные закупки, инспекционные визиты и др. Между тем потенциальный инструментарий финансового контроля значительно шире, он может и должен строиться на принципиально иной методологической базе. Далеко не случайно в последнее время в практику входит ограничительное планирование прове<sup>4</sup> Предприятие. Закон. Управление / Под ред. М. К. Юкова. М. : Юрид. лит-ра, 1989. С. 173. рок (по принципу — не более такого-то количества за период времени) и даже мораторий на их проведение. На первый взгляд, это противоестественно: ведь ограничениями лимитируется деятельность органов финансового контроля, специально для этого государством созданных. Мы же считаем, что речь идет о перераспределении функций контроля между различными органами, а также о необходимости диверсификации методов его осуществления. Исторически финансовый контроль формировался в нашей стране как безусловное право некоего органа или должностного лица потребовать объяснений, представив документы, затребовать те или иные доказательства от контролируемого субъекта, обязанности последнего выполнить требования контролера, а также право контролера интерпретировать имеющиеся сведения, давать им экономическую, правовую или политическую оценку и право реализации

результатов путем докладов, представлений, обобщений, актов, направляемых в соответствующие органы управления или другие контрольные или следственные органы или непосредственно в суды. При этом публичный интерес всегда превалировал над интересом частным, а взаимоотношения органа контроля и подконтрольного субъекта в той или иной мере строились на презумпции виновности подконтрольного. Сменяющие друг друга исторические эпохи если и изменили эти отношения, то только юридическим «приспособлением» условий работы подконтрольного субъекта под возможные запросы контролера (обязанность вести бухгалтерский учет, хранить денежные средства в кредитных учреждениях, осуществлять учет движения ценностей и др.). Будь то контроль полноты платежей в бюджеты различных уровней, слежение за распределением бюджетных ассигнований, совершение государственных расходов, предоставление и возврат кредитов, любые инвестиционные программы, валютные расчеты и даже проверка осуществления финансового контроля — все основывается на проверке как ведущей форме финансового контроля. Зададимся теперь вопросом — в чем существо и цель возникновения контрольных правоотношений? Ответ может быть простым и однозначным — в получении достоверной информации о деятельности подконтрольного субъекта, а сами контрольные отношения есть не что иное, как информационные правоотношения<sup>5</sup> [8].

Посредством этой констатации мы вправе приравнять контроль в целом и финансовый контроль в частности к

Папаскья Г. Т.

Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март

цифровизация которых существенно повышает достоверность, объективность и оперативность [9] получения необходимой информации в целях управления, позволяет освободить ее сбор и обработку от субъективизма и возможного противодействия ее полупу5 Digital Transformation of Tax and Customs Administrations. World Bank, Washington, DC. URL: <https://openknowledge.worldbank.org/handle/10986/37629> (дата обращения: 20.04.2022). 6 Правовое регулирование в информационном обществе Правовая информатика № 3 – 2022 чению со стороны подконтрольного субъекта, а также в значительной мере упрощает и удешевляет как сам процесс контроля, так и порядок реализации данных, полученных путем контроля. Нет сомнения в том, что финансовый контроль, осуществляемый посредством получения объективных цифр и алгоритмов, непременно упразднит контроль людей над людьми, каким бы объективным и достоверным он (контроль) не старался быть. Законодательство о контроле недавно обогатилось фундаментальным актом — Федеральным законом от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»<sup>6</sup>, которым, прежде всего, создана методологическая база контрольной деятельности как особой формы правового регулирования управленческих отношений, в том числе определены исходные начала для перевода государственного контроля на цифровой метод осуществления. Однако этот закон, не распространяющий свое действие на контрольные отношения в финансовой сфере, закрепляет узкий подход к пониманию государственного контроля (надзора), определив его как деятельность контрольных (надзорных) органов, направленную на предупреждение,

выявление и пресечение нарушений <sup>Папаскья Г. Т.</sup> обязательных требований, ~~осуществляемую в пределах~~ полномочий указанных органов. Вместе с тем в финансовом законодательстве и финансово-правовой доктрине понятие государственного финансового контроля имеет более широкую трактовку [4], охватывая собой ряд самостоятельных форм управления бюджетными ресурсами. Контроль в широком смысле является механизмом обратных связей, осуществляемых в форме надзора, мониторинга, аудита, бухгалтерского и статистического учета. Иными словами, в основе построения современной модели государственного финансового контроля лежит перераспределение функций контроля между различными органами, а также дифференциация методов его осуществления. Совершенствование государственного финансового контроля потребует внедрения новых и обновления применяемых контрольных механизмов. Прежде всего следовало бы обратить внимание на бухгалтерский учет, подрастерявший в условиях рыночной экономики свою публичную направленность и ставший более частноправовым институтом, чем цели, вызвавшие его создание в рамках планового хозяйствования, в том числе в связи с исчезновением отраслевой (министерской) организации бухгалтерского учета. В условиях цифровизации должен обрести большую мощь аудит, понимаемый как инструмент обеспечения интересов собственников (инвесторов) ~~хозяйствующих субъектов, основанных на складочном капитале, прежде всего в~~ акционерных обществах. Каждый 6 Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март Предприятие. Закон. Управление / Под ред. М. К. Юкова. М. : Юрид. лит-ра,

1989. С. 173. инвестор-миноритарий должен быть наделен возможностью ~~беспрепятственного получения~~ информации по всем интересующим вопросам общества. Значительные возможности заложены и в такой форме контроля, как мониторинг [12]. Скорее всего, речь должна идти о гармоничном взаимодействии банковского, финансового мониторинга с бухгалтерским учетом в хозяйствующих субъектах и органах с распределительными функциями. Особенно актуален мониторинг в регулировании денежного обращения, цель которого состоит в искоренении обналичивания и отмывания денежных средств. Одной из форм осуществления государственного контроля является надзор за эффективностью управления отдельными экономическими комплексами. Обозначенный подход к пониманию природы надзора был сформирован еще в рамках финансово-контрольной реформы, проведенной в XIX веке, когда на учреждения Государственного Контроля были возложены функции правительственного надзора за хозяйственными операциями предприятий, требовавших от государства крупных расходов<sup>7</sup>. Статистический учет и отчетность [11] — инструмент управления, возможный только в условиях цифровой реализации, в настоящий момент времени выполняет важные функции. Думается, что статистика может в значительно бóльшей степени, нежели сейчас, использоваться в финансовом контроле, если решить ряд организационных вопросов доступа к статистической информации. В условиях цифровой среды развитие получают универсальные формы осуществления государственного контроля, архитектура которых позволяет контролирующим органам посредством применения обозначенных выше функций контроля в

режиме реального времени отслеживать финансово-хозяйственные операции подконтрольных субъектов и в случае необходимости корректировать условия осуществления финансовых обязательств. В частности, одной из универсальных форм финансового контроля выступает закрепленный Налоговым Кодексом РФ горизонтальный налоговый мониторинг, позволяющий налоговым органам в рамках режима информационного взаимодействия корректировать условия исполнения налоговых обязательств [1, 13]. Нетрудно заметить, что названные формы финансового контроля носят преимущественно «бесконтактный» характер и осуществляются без использования организационной формы проверки. Конечно же, это не значит, что проверки и, в частности, выездные проверки следует упразднить вообще; проверки будут осуществляться, но преимущественно в виде комплексных расследований по наиболее одиозным и требующим выводов принципиального характера ситуациям. 7 Иловайский С. И. Учебник финансового права. 5-е (посмерт.) изд. / Под ред. Н. П. Яснопольского. Одесса : Изд. Е. С. Иловайской, 1912. 604 с. 7 Цифровизация финансового контроля: правовое регулирование Правовая информатика № 3 – 2022 Финансовый контроль, выступая в качестве важнейшего канала обратных связей центров управления с управляемыми субъектами, действующими преимущественно в автономном режиме, приобретает ведущее значение во всем механизме хозяйствования. Исследуемые формы обратных связей, составляющих государственный финансовый контроль, подвергаются:

Папаскья Г. Т.

Трансформация субъекта

регулированию, направленному на создание правового режима информации, соответствующей требованиям объективности и достоверности [9], во-вторых, специальному правовому регулированию, которое нацелено на конкретизацию осуществления каждой формы контроля и, в-третьих, цифровой трансформации, представляющей собой переход механизма экономического управления в новое качество (см. рисунок). Вместе с тем за рамками процесса цифровизации следует оставить некоторые сферы информационной деятельности, в том числе оперативно-розыскную деятельность, уголовное судопроизводство и др., которые предполагают личную, интеллектуальную, творческую деятельность правоприменителя, не вписывающуюся в параметры цифровых алгоритмов. Иной подход приведет к нарушению конституционных гарантий защиты прав граждан. Правовые проблемы цифровой трансформации финансового контроля Исследуя механизм финансового контроля как одну из форм управления бюджетными ресурсами и доходами, ученые-правоведы нередко задавались вопросом о том, «...относятся ли к финансовым правоотношениям юридические связи по осуществлению финансового контроля и налогового администрирования?» [5]. Еще несколько десятилетий назад ответ на этот вопрос мог быть неоднозначным, поскольку контрольно-организационные отношения, обеспечивающие развитие финансовых обязательств, по основаниям возникновения и содержанию близки к организационным отношениям, охватываемым сферой действия административного права. Однако на сегодняшний день сомнения при ответе на поставленный вопрос вряд ли возникнут,<sup>43</sup> поскольку в условиях формирования цифровой модели финансового контроля

Актуальные проблемы российского права. 2021. Т. 16, № 3 (124) март

контрольно-организационные отношения настолько «вплетаются» в ткань финансовых обязательств, что осуществление последних не может происходить в отрыве от инструментов контрольно-надзорной деятельности. Например, введение упрощенной автоматизированной системы налогообложения, которая с 1 июля 2022 г. в качестве эксперимента применяется в Москве, Татарстане, Московской и Калужской областях, позволяет налоговым органам автоматически определять элементы налогообложения на основе данных контрольно-кассовой техники. А построенная на цифровых технологиях архитектура горизонтального налогового мониторинга фактически предоставляет контролирующим субъектам возможность в режиме реального времени корректировать условия осуществления налоговых обязательств. Внедрение единой системы управления общественными финансами — электронный бюджет, единой информационной системы в сфере закупок, государственной информационной системы о государственных и муниципальных платежах и др. нацелено на обеспечение

Правовое регулирование в информационном обществе Правовая информатика № 3 – 2022 прозрачности и открытости осуществления операций в сфере управления бюджетными ресурсами и доходами. Избегая

Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март

подробного описания особенностей функционирования информационных систем, обеспечивающих

осуществление финансовых операций, заметим, что цифровая модель финансового контроля, представляющая собой не что иное, как «механизм по управлению информацией»<sup>8</sup>, в целом положительно сказывается на развитии финансового законодательства, приводит к упрощению сбора, обработки и хранения информации о финансово-хозяйственных операциях субъектов финансовых правоотношений и, как следствие, к сокращению административных процедур, обеспечивающих взаимодействие контрольных органов и контролируемых субъектов. Вместе с тем активный процесс цифровизации пока не позволяет преодолеть все препятствия на пути формирования эффективной модели взаимодействия субъектов контрольно-организационных правоотношений. Например, развитие налогового мониторинга, в рамках которого контрольный орган получает доступ к информационным системам организации, привело к формированию закрытой системы взаимодействия налогоплательщиков и налоговых органов, основанной на мотивированных мнениях контролирующих органов, единая база данных которых отсутствует. Помимо сказанного, в ряде случаев закрепленные в Налоговом кодексе (НК) РФ условия осуществления налоговых обязательств усложняются административными процедурами и не вписываются в параметры цифровой модели управления бюджетными ресурсами. Возникает ситуация, когда параллельно с информационными системами, обеспечивающими администрирование налогов и позволяющими без участия налогоплательщика определить элементы налогообложения, продолжает применяться заявительный порядок возврата (зачета) излишне уплаченных налогов, сборов, таможенных платежей,

право на осуществление которого ограничено <sup>Папаскья Г. Т.</sup> трехлетним сроком давности, действует заявительный порядок применения налоговых льгот, не утрачивают актуальность споры о применении срока давности взыскания недоимки и др. Фактически происходит неравномерное развитие элементов механизма налогообложения, в рамках которого процедура взыскания налога с точки зрения правового регулирования и эффективности работы информационных систем опережает процесс определения элементов его юридического состава. Успешная цифровая трансформация форм реализации финансового контроля невозможна в отрыве от проведения работы по совершенствованию существующих инструментов государственного управления в фискальной, бюджетной сфере, в области денежного обращения и др. Например, не способствует развитию финансового контроля, основанного на рискориентированном методе [2], разветвленная система 8 Афанасьев В. Г. Научное управление обществом: (Опыт системного исследования). 2-е изд., доп. М. : Политиздат, 1973. 391 с. экономических санкций, построенная на «принципе сплошного контроля»<sup>9</sup>. Иными словами, выстраиваемая модель осуществления государственного контроля требует изменить подход к применению мер имущественной ответственности к субъектам финансовых правоотношений посредством смещения инициативы по уплате в бюджет экономических санкций на участников гражданского оборота. Обозначенное направление может быть реализовано посредством <sup>Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март</sup> использования обязательственного метода применения имущественной ответственности за нарушение

финансового законодательства, что позволит создать иной механизм наложения экономических санкций, корреспондирующий рискориентированному подходу осуществления государственного финансового контроля. Препятствуют созданию эффективной модели взаимодействия контролирующих и подконтрольных субъектов сформированные в правоприменительной практике паллиативные институты регулирования контрольно-надзорной деятельности. В частности, речь идет о применении контрольными органами административных процедур, форм контроля, не предусмотренных налоговым законодательством и являющихся альтернативой предусмотренным НК РФ налоговым проверкам. Например, в настоящее время прослеживается активное использование налоговыми органами не установленных НК РФ форм предпроверочного анализа, порядок применения которых закреплен Приказом ФНС России от 27 февраля 2015 г. № ММВ-8-2/13 «О проведении пилотного проекта по развитию на региональном уровне методов побуждения налогоплательщиков к добровольному исполнению налоговых обязательств», который не опубликован и не зарегистрирован в Министерстве юстиции РФ в качестве нормативного акта, однако упоминается 10 судами при разрешении споров, связанных с процедурами налогового администрирования и налогового контроля. На основании изложенного становится очевидным, что внедрение информационных систем и цифровых сервисов в механизм финансового контроля не является панацеей в борьбе с не предусмотренными финансовым законодательством контрольно-надзорными процедурами, а <sup>43</sup> также с неэффективными инструментами управления бюджетными ресурсами.

Успешное разрешение обозначенных проблем <sup>Лапаскья Г. Т.</sup> зависит от выявления причин происходящего, которые кроются в противоречивом характере финансово-правовых норм в части определения объема полномочий контрольных органов, а также в пренебрежении ключевыми принципами организации государственного управле<sup>9</sup> Федеральным законом от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изменениями на 6 декабря 2021 г.) // Собрание законодательства Российской Федерации. 2020. № 31. Ст. 5007. 10 См., например: Решение Арбитражного суда г. Москвы от 5 октября 2020 г. по делу № А40-211149/18-115-4949; Постановление Арбитражного Суда Московского округа от 31 октября 2019 г. по делу № А41-394/2019. 9

Цифровизация финансового контроля: правовое регулирование Правовая информатика № 3 – 2022 ния. Прежде всего речь идет о противоречивых положениях НК РФ при определении полномочий ФНС России. Устанавливая в п. 2 ст. 4 НК РФ запрет контрольно-надзорного органа на принятие нормативных правовых актов, регулирующих отношения в сфере налогообложения и сборов, в других статьях Кодекса законодатель делегирует это право контролирующему субъекту. Изложенное приводит к негативным последствиям, выражающимся в смещении государственных функций между федеральными органами исполнительной власти, наделению контрольно-надзорного органа <sup>нормотворческими полномочиями, что</sup> <sup>Актуальные проблемы российского права. 2021. Т. 16. № 3 (124) март</sup> в конечном счете выражается в разрастании объема правоприменительной практики,

направленной на применение налоговыми органами не предусмотренных законом административных процедур и форм осуществления налогового контроля. Учитывая сказанное, цифровая трансформация финансового контроля должна сопровождаться принятием комплекса мер, направленных на исключение параллельных правовых институтов регулирования контрольно-надзорной деятельности посредством: устранения внутренней несогласованности содержащихся в НК РФ правовых норм в части определения объема полномочий налоговых органов; сокращения объема подзаконных нормативных правовых актов, регулирующих фискальные отношения, с помощью применения функционального подхода к управлению развитием экономики<sup>11</sup>, нацеленного на распределение государственных функций между федеральными органами исполнительной власти. В целом цифровые инструменты финансового контроля, с учетом необходимой корректировки финансового законодательства по обозначенным выше направлениям, являются достаточно эффективными в отношении реального сектора экономики и способствуют развитию финансовой системы государства в положительном ключе. Вместе с тем правовое регулирование финансового контроля цифровых финансовых инструментов вызывает серьезные трудности, разрешение которых пока не имеет четко обозначенных направлений. Фактически возникает проблема встраивания технологических процессов в правовое поле. Отставание правового регулирования в исследуемой сфере во многом обусловлено особенностями функционирования цифровых бизнес-моделей, экономическая деятельность которых по ряду аспектов противоречит ключевым принципам права, поскольку

она связана с «...коммерциализацией персональных данных пользователей цифровых платформ и использованием их в качестве нематериальных активов»<sup>12</sup>. Такое направление деятельности цифровых компаний идет

11 Бачило И. Л. Функции органов управления. Правовые проблемы оформления и реализации. М. : Юрид. лит-ра, 1976. 200 с. 12 Tax Challenges Arising from Digitalisation — Interim Report 2018 (inclusive framework on BEPS). URL: <https://www.oecd.org/tax/beps/taxchallenges-arising-from-digitalisation-interim-report-9789264293083-en.htm> (дата обращения: 15.04.22). вразрез с целями реализации механизма правового регулирования, направленного прежде всего на обеспечение защиты неотъемлемых прав, которые «сами по себе есть и сила, и власть, ибо все то, что с ними несогласно, противоестественно, т. е. противно законам природы, а значит, обречено на вымирание и гибель» [6, с. 39]. Особого внимания в условиях развития цифровизации и глобализации экономических процессов заслуживает задача осуществления контроля за оборотом криптовалюты, которая активно используется для перемещения капитала через границы, конкурирует с законными средствами платежа в цепочке расчетных операций<sup>13</sup> [10], способствует размыванию налогооблагаемой базы, что влечет за собой значительные риски и издержки для государства в части денежного суверенитета, политического пространства и макроэкономической стабильности. В докладе Конференции ООН по торговле и развитию (ЮНКТАД), направленного на совершенствование контроля за функционированием криптовалютной

системы, предлагаются следующие меры: обязательная регистрация криптобирж и цифровых кошельков; введение налога на транзакции криптовалют; ограничение или запрет рекламы, криптобирж и цифровых кошельков; создание общедоступной платежной системы, направленной на введение в оборот цифровой валюты центральных банков государств<sup>14</sup>. Учитывая подходы, обозначенные в докладе ЮНКТАД, заметим, что одним из ключевых инструментов контроля за совершением финансовых операций, включая операции с криптовалютой, является механизм налогообложения, выполняющий роль своеобразного фильтра, с помощью которого происходит легализация доходов, поступивших в распоряжение налогоплательщика. Вместе с тем в законодательстве РФ о налогах и сборах пока не конкретизированы правила налогообложения доходов от операций с криптовалютой [7], которые, согласно разъяснениям<sup>15</sup> Минфина России, учитываются при определении налоговой базы по налогу на прибыль (доходы) в общем порядке. Такой поверхностный подход к механизму фискального обложения доходов от оборота криптовалюты объясняется тем, что предусмотренная НК РФ конструкция налогообложения нацелена на операции с законными средствами платежа, а на сегодняшний день на законодательном уровне не урегулирован процесс «превращения» криптовалюты в фиатные деньги. 13 Clemens Graf von Luckner, Carmen M. Reinhart, Kenneth Rogoff. Decrypting New Age International Capital Flows. URL: <https://openknowledge.worldbank.org/bitstream/handle/10986/36345/Decrypting-New-Age-International-Capital-Flows.pdf?sequence=1&isAllowed=y> (дата обращения: 15.04.22). 14 All that glitters is not gold: The high cost of leaving

cryptocurrencies unregulated. United Nations Conference on trade and development. Policy brief. No. 100, June, 2022. URL: [http://unctad.org/system/files/official-document/presspb2022d8\\_en.pdf](http://unctad.org/system/files/official-document/presspb2022d8_en.pdf) (дата обращения: 20.08.22). 15 Письма Минфина РФ от 24 августа 2020 г. № 03-03-06/1/73953, от 20 августа 2019 г. № 03-04-05/63704. 10 Правовое регулирование в информационном обществе Правовая информатика № 3 – 2022 Для сравнения следует отметить, что в Республике Казахстан применяется иная модель контроля доходов участников криптовалютного рынка, основанная на введении платы за цифровой майнинг, которая исчисляется исходя из фактических объемов потребленной электрической энергии, установленной ставки платы и введения дифференцированных ставок налога на цифровой майнинг<sup>16</sup>. Подобным же образом контроль функционирования криптовалютного рынка происходит и в Республике Беларусь<sup>17</sup>. Российское законодательство об электроэнергетике устанавливает дифференцированную систему ценообразования<sup>18</sup>, однако вопросы, связанные с взиманием платы за потребление электроэнергии в повышенном размере с лиц, осуществляющих цифровой майнинг в России, пока приводят к спорам между потребителями и энергоснабжающими организациями<sup>19</sup>. На разрешение обозначенной проблемы направлен Приказ ФАС РФ от 27 мая 2022 г. № 412/22 «Об утверждении Методических указаний по расчету тарифов на электрическую энергию (мощность) для населения и приравненных к нему категорий потребителей, тарифов на услуги по передаче электрической энергии, поставляемой населению и

приравненным к нему категориям потребителей»<sup>20</sup>, на основании которого в целях борьбы с «серыми» майнерами субъектам Российской Федерации предоставлено право принимать решения об установлении социальной нормы потребления электрической энергии. Приведенные примеры применения правовых средств контроля за функционированием криптова<sup>16</sup> Параграф 11 Кодекса Республики Казахстан от 25 декабря 2017 г. № 120- VI ЗРК «О налогах и других обязательных платежах в бюджет (Налоговый кодекс)»; Закон Республики Казахстан от 11 июля 2022 года № 135-VII ЗРК «О внесении изменений и дополнений в Кодекс Республики Казахстан «О налогах и других обязательных платежах в бюджет» (Налоговый кодекс) и Закон Республики Казахстан «О введении в действие Кодекса Республики Казахстан «О налогах и других обязательных платежах в бюджет» (Налоговый кодекс)». 17 Так, на основании Постановления Министерства антимонопольного регулирования и торговли Республики Беларусь и Министерства энергетики Республики Беларусь от 27 сентября 2021 г. № 62/57 в отдельную тарифную группу потребителей электроэнергии отнесены организации, осуществляющие цифровой майнинг. 18 Как регулировать майнинг в России? URL: <http://www.csr.ru/upload/iblock/fe5/is5zwilpf79vf70lrdep9o17xjck2jiz.pdf> (дата обращения 20.07.22). 19 См.: Решение Арбитражного суда Иркутской области от 5 октября 2018 г. по делу № А19-15918/2017. 20 Приказ ФАС РФ от 27 мая 2022 г. № 412/22 «Об утверждении Методических указаний по расчету тарифов на электрическую энергию (мощность) для населения и приравненных к нему категорий потребителей, тарифов на услуги по передаче электрической энергии, поставляемой населению и приравненным

к нему категориям потребителей». URL: <http://www.pravo.gov.ru> позволяют прийти к выводу о целесообразности трансформации конструкции налогообложения в сторону смещения инициативы по формированию публичных денежных фондов с государства на бизнес, в результате чего участники гражданского оборота будут заинтересованы в добросовестном исполнении налоговой обязанности и в получении права доступа на рынок цифровых услуг. Это имеет ключевое значение для создания эффективной модели взаимодействия контролирующих и подконтрольных субъектов в условиях развития цифровой экономики. Выводы 1. Контроль в широком смысле является информационным процессом с механизмом обратных связей, осуществляемых в форме надзора, мониторинга, аудита, бухгалтерского и статистического учета, а современная модель государственного финансового контроля основана на перераспределении функций контроля между различными органами, а также на дифференциации методов его осуществления. 2. Формы обратных связей, составляющих государственный финансовый контроль, подвергаются, в первую очередь, общему правовому регулированию, направленному на создание правового режима информации, соответствующей требованиям объективности и достоверности, а во-вторых, специальному правовому регулированию, которое направлено на конкретизацию порядка осуществления каждой формы контроля. 3. Цифровизация должна подвергаться отработанные и применяемые на практике формы обратных связей, основанные на требованиях

объективности, достоверности и актуальности информации. Не могут подвергаться цифровой трансформации некоторые сферы информационной деятельности, в том числе оперативно-розыскная деятельность, уголовное судопроизводство и др., которые предполагают личную, интеллектуальную, творческую деятельность правоприменителя, не вписывающуюся в параметры цифровых алгоритмов. 4. Особое внимание следует уделить проблеме разграничения государственных функций между федеральными органами исполнительной власти, а также вопросам конкретизации в финансовом законодательстве прав и обязанностей контрольных органов, порядка проведения ими мероприятий финансового контроля. Это позволит исключить формирование паллиативных правовых институтов регулирования контрольно-надзорной деятельности, в результате чего контролирующие органы применяют не предусмотренные законом формы и методы финансового контроля. Рецензент: Исаков Владимир Борисович, доктор юридических наук, профессор, заслуженный юрист Российской Федерации, действительный государственный советник Российской Федерации 1 класса, заведующий кафедрой теории права и сравнительного правоведения Национального исследовательского университета «Высшая школа экономики», г. Москва, Российская Федерация. E-mail: visakov@hse.ru 11 Цифровизация финансового контроля: правовое регулирование Правовая информатика № 3 – 2022 Литература 1. Васянина Е.Л. О правовой природе государственного контроля в финансовой сфере // Современное общество и право. 2021. № 3. С. 86—94. 2. Ващекина И.В., Ващекин А.Н. Информационное взаимодействие в системе борьбы с

«отмыванием» преступных доходов: Папаскья Г. Т. риск-ориентированный подход // Правовая информатика. 2018. № 4. С. 4—14. DOI: 10.21681/1994-1404-2018-4-04-14 . 3. Государство и право в новой цифровой реальности : монография / Под общ. ред. И.А. Конюховой-Умновой, Д.А. Ловцова. М. : ИНИОН РАН, 2020. 259 с. ISBN 978-5-248-00959-6. 4. Грачева Е.Ю. Проблемы правового регулирования государственного финансового контроля. М. : Юриспруденция, 2000. 192 с. 5. Запольский С.В. К вопросу о природе финансовых правоотношений: информационная составляющая // Финансовое право. 2007. № 8. С. 9—13. 6. Зорькин В.Д. Право против хаоса : монография. 2-е изд., испр. и доп. М. : Норма: ИНФРА-М, 2019. 368 с. 7. Кучеров И.И. Актуальные вопросы налогово-правового регулирования сферы цифровой экономики // Вестник Нижегородской академии МВД России. 2019. № 4 (48). С. 167—175. 8. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1. 9. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8. 10. Ловцов Д.А. Имплементация «цифровых» прав в экономике: информационно-правовые аспекты // Российское правосудие. 2020. № 10. С. 42—53. DOI: 10.37399/issn2072-909X.2020.10.42-53 . 11. Ловцов Д.А., Богданова М.В., Лобан А.В., Паршинцева Л.С. Статистика (компьютеризированный курс) / Под ред. Д. А. Ловцова. М. : РГУП, 2020. 400 с. ISBN 978-5-93916-834-2. 12. Прошунин М.М. Правовое регулирование финансового мониторинга (российский и

зарубежный опыт) : монография. М. : Рос. акад. правосудия, 2010. 344 с. 13.

Публичная власть: система, компетенции : монография / Под общ. ред. М.Н. Кобзарь-Фроловой. Воронеж : Научная книга, 2021. 237 с. 14. Сырых В.М. Застарелые недуги позитивистской доктрины права // Государство и право. 2014. № 2(63). С. 38—44.

### **№ 11. Цифровая форма платежных средств и государственный финансовый контроль в цифровой среде. Особенности использования криптовалют.**

31 октября 2008 г. пользователь под псевдонимом Satoshi Nakamoto выложил описание криптовалюты биткойн как новой электронной денежной системы, основными достоинствами которой являются защита от мошеннических операций, независимость от каких-либо организаций, возможность анонимного использования, неподвластность инфляции. В соответствии с терминологией Группы разработки финансовых мер борьбы с отмыванием денег, криптовалюта является одним из видов виртуальных валют и «означает основанную на математических принципах децентрализованную конвертируемую валюту, которая защищена с помощью криптографических методов, т. е. использует криптографию для создания распределенной, децентрализованной и защищенной информационной экономики». В целом число криптовалют составляет более трех тысяч. Наиболее популярной среди них продолжает оставаться биткойн – цифровая валюта, созданная и работающая только в сети интернет. Эмиссия валюты происходит посредством работы миллионов компьютеров по всему миру, используя определенную программу. Вместо привычной централизованной иерархии используется технология блокчейн,

предполагающая хранение данных обо всех транзакциях не на одном сервере, а на компьютерах, подключенных к платежной системе. Эти альтернативные деньги имеют predetermined максимальный запас: количество биткойнов растет с заданной скоростью со снижением до 2140 г., когда предложение биткойнов станет фиксированной цифрой в 21 млн монет. Транзакции биткойна осуществляются сетью peer-to-peer, где для совершения операций между людьми финансовые посредники не требуются. 41 Несмотря на то, что виртуальные валюты распространены в мире широко, правовая база этого явления разработана слабо, классификация виртуальных валют отсутствует. Некоторые их классифицируют на: – конвертируемые валюты (Bitcoin, E-Gold, Liberty Reserve и др.), которые на отдельных биржах обладают эквивалентной стоимостью в фиатной валюте и могут быть обменены на фиатную валюту и обратно; – неконвертируемые валюты (Q Coins), служащие только для использования в виртуальных сферах и которые официально не могут быть обменены на фиатную валюту. Виртуальные валюты еще делятся на: – централизованные – имеющие единого эмитента (E-Gold, Liberty Reserve, Perfect Money), контролирующего всю систему. Администратор эмитирует валюту, вводит правила ее использования, ведет и хранит реестр транзакций и может изымать валюту из обращения. Курс такой валюты может быть плавающим, определяться спросом и предложением либо фиксированным, привязанным к фиатной валюте или золоту. Децентрализованные валюты (Bitcoin, Ethereum, Litecoin, Ripple), – валюты, у которых отсутствует единый

администратор и нет централизованного контроля. Информация о передаче прав собственности передается через сеть способом, который обеспечивает по прошествии короткого периода времени подтверждение транзакций, безопасность и целостность передачи стоимости. Многие продавцы товаров и услуг по всему миру с некоторого времени стали принимать платежи в биткойнах, среди которых есть крупные компании с мировым именем, а также магазины, университеты, авиакомпании. Поэтому количество физических и юридических лиц, использующих биткойн, непрерывно растет. Это строительные предприятия, рестораны, агентства недвижимости, юридические фирмы и онлайн-сервисы. Колоссальный успех биткойна состоит еще и в том, что с 2010 г. он котируется на отдельных мировых биржах по отношению к мировой валюте – доллару США – и некоторым другим национальным валютам. Существует еще одна причина, вследствие которой биткойн приобрел необычайную популярность, – это интерес спекулятивных инвесторов к высокой волатильности биткойна и других криптовалют. В период с 01.01.2017 г. по 01.01.2018 г. совокупная рыночная капитализация криптовалют выросла с 18,3 млрд до 598,0 млрд долл., при этом ежедневный объем торгов вырос с 140,0 млн до 24,8 млрд долл. Рыночная капитализация рынка криптовалют достигла рекордного максимума 07.01.2018 на уровне 828,5 млрд долл. После ажиотажа начала 2018 г. криптоиндустрия перешла от роста к падению. Этот процесс проходил жестко, привел к обвалу рынка, потере средств и заинтересованности инвесторов, реорганизации многих проектов (рис. 4.5). 42 Рис. 4.5. Капитализация рынка криптовалют с 01.05.2017 г. по 01.11.2019 г., млрд долл. Обмен цифровыми деньгами и их купля-

продажа за фиатные деньги  
Папаскья Г. Т.  
совершаются на криптовалютных биржах, под которыми понимается интернетресурс, осуществляющий торги в режиме реального времени. Такие площадки являются довольно востребованными не только среди инвесторов, но и обычных пользователей, позволяя совершать сделки, получать полезную информацию о том, как торговать и т. д.

#### 4.4. Правовое регулирование криптовалют в различных странах

На данный момент единые стандарты в регулировании виртуальных валют отсутствуют и центральный банк каждой страны использует собственные подходы. Наиболее типичные из них три: – формальное разрешение, включающее рекомендации для населения, касающиеся рисков использования виртуальных валют; – специально разработанные законы, регулирующие обращение виртуальных валют; – полный запрет обращения на территории государства. К странам, которые официально признали криптовалюту и разрабатывают правовые нормы для ее регулирования, относятся Австралия, Беларусь, Великобритания, Германия, Канада, Норвегия, Россия, Сингапур, Скандинавские страны, США, Чехия, Швейцария, Швеция, Эстония, Южная Корея, Япония. Страны, которые считают криптовалюту нелегальной и запретили ее использование, – Алжир, Бангладеш, Боливия, Вьетнам, Индонезия, Исландия, Киргизия, Ливан, Непал, Эквадор. Другие страны держат нейтралитет в данном вопросе, их правительства сильно не вмешиваются, но и не запрещают использование криптовалют. 43 Однако при видимом состоянии нейтралитета такие страны прощупывают почву, чтобы наложить

законодательные нормы на использование криптовалют и тем самым взимать с нее не только налоги, но и ограничивать обращение в правовом поле. В конце 2017 г. Президент Беларуси подписал Декрет № 8, создающий правовые условия для развития блокчейн-проектов и оборота криптовалют. Это сделало возможным предоставлять услуги виртуальных бирж и обменных пунктов резидентам ПВТ, привлекать денежные средства с помощью ИСО, ввести в легальное поле деятельность майнеров. В конце 2018 г. администрация ПВТ, Национальный банк, Департамент финансового мониторинга Комитета государственного контроля опубликовали набор нормативных документов и требований для предприятий, связанных с криптовалютой.

#### 4.5. Перспективы и риски применения криптовалют в финансовой системе государства

Перспективы развития криптовалют можно выразить следующими тезисами: будет происходить постепенное внедрение электронных денег в жизнь обычных людей; децентрализованные системы не станут заменой банкам, но будут друг друга дополнять; для повышения безопасности придется пожертвовать определенными благами; стабильной ситуации в ближайшие годы можно не ждать. Уже скоро можно будет использовать всевозможные криптовалюты в качестве официального средства оплаты. Данная перспектива с каждым днем становится все более реальной, а повышающийся интерес со стороны политических и банковских систем со всего мира благоприятствует этому. Постоянно растущий курс криптовалют побуждает людей накапливать криптовалюту, надеясь на этом заработать. Возможность получения спекулятивной прибыли отвлекает инвесторов от реального сектора. Другой проблемой является волатильность криптовалют. За каждым ростом следуют

обрушения курса, пусть и не такие сильные, но все же довольно чувствительные. В реальной экономике валюта с таким непостоянным курсом имеет проблемы использования. Третьей проблемой является так называемая гонка вооружений. Все, кто эмитирует криптовалюты, пытаются увеличить мощность своего оборудования. Затраты на гонку вооружений покрываются эмиссией, но со временем число добываемых единиц криптовалют неизбежно сократится, и тогда окупать стоимость оборудования придется тем, кто платит комиссии за транзакции, либо очень сильно поднимется цена криптовалюты. Четвертая проблема – энергозатраты. Добыча биткойнов требует дорогостоящего и энергоемкого компьютерного оборудования. Ежегодно на добычу биткойнов расходуется 73,1 тераватт-час, что составляет 0,33 % от мирового потребления электричества. 44 Рис. 4.6. Индекс потребления энергии майнингом биткойна

Страна	Процент от потребляемой энергии
Общая энергия, расходуемая сегодня на добычу биткойнов	1,8 %
США	7,5 %
Россией	22,1 %
Великобританией	107,1 %

и Чехией. Если бы все майнеры стали отдельной страной, то она в ноябре 2019 г. заняла бы 40-е место в мире по объему потребления электроэнергии (в конце 2017 г. – 61-е место). Выводы по теме 4. Невозможно однозначно утверждать, хороши или вредны криптовалюты, привнесут ли они что-то новое в современную экономику или станут еще одним видом электронных денег, привязанным к курсу фиатных валют. Несомненно, что в криптовалютах заложен огромный потенциал, который, с одной стороны, может дать мощный

толчок мировой экономике, с другой – затормозить ее развитие. Как и любая другая инновация, криптовалюты несут новые риски, в том числе из-за нелегальной деятельности, но эта же технология предлагает революционные возможности.

## № 12. Особенности договорного регулирования в условиях цифровой экономики

*Постановка проблемы в общем виде и ее связь с важными научными и практическими задачами. Стремительное развитие современных технологий, основанных на информационных новациях (технология распределенного реестра, смарт-контракты и пр.), сопровождается коренными изменениями во всех сферах жизни*

общества. Этот факт должен учитываться в процессе законотворчества и в правоприменительной деятельности. Обеспечение ускоренного внедрения цифровых технологий в социальной сфере и экономике – одна из приоритетных целей развития Российской Федерации на период до 2024 года (п. 1 Указа Президента РФ № 204 от 07.05.2018 года «О национальных целях и стратеги-

---

ческих задачах развития РФ на период до 2024 года»). В соответствии с абз. 1 п. 11 данного Указа Правительство РФ и органы государственной власти субъектов РФ должны сформировать систему правового регулирования цифровой экономики и внедрить гражданский оборот, основанный на цифровых технологиях. Новая система правового регулирования должна основываться на гибком подходе в каждой сфере [1]. Таким

образом, актуальной проблемой в настоящее время является формирование системы правового регулирования, способствующей развитию цифровой экономики в Российской Федерации.

*Анализ последних исследований и публикаций, в которых рассматривались аспекты этой проблемы и на которых обосновывается автор; выделение неразрешенных ранее частей общей проблемы.* По настоящей проблематике имеются отдельные научно-правовые исследования, в особенности, посвященные институту договора в условиях цифровизации (например, работы

Камалая В.М. [7], Новикова Р.В. [9], Сафаргалеева Л.И. [10], Шапсуговой М.Д. [11], Юламановой А.А. [12] и пр.). Тем не менее, настоящие исследования не затрагивают вопросов цифровизации целой правовой подотрасли – договорного права.

#### МЕТОДОЛОГИЯ

*Формирование целей статьи.* Целью настоящей статьи является определение основных тенденций по трансформации договорного права в условиях цифровизации экономики.

*Постановка задания.* Цель предопределила следующие задачи исследования: 1) проанализировать с правовой точки зрения внесенные в гражданское законодательство изменения в части договорного регулирования, трансформирующегося в условиях цифровизации экономики; 2) сравнить институт смарт-контрактов с существующими институтами электронных сделок, автоматизированных сделок, регулируемых международным законодательством; 3) рассмотреть основные модели автоматизированных сделок, применяемых в деловой практике; 4) выявить логику правовых изменений законодателя и сравнить с тенденциями трансформации договорного права.

*Используемые в исследовании методы, методики и технологии.* При написании данного исследования был использован диалектический метод познания договорных отношений, включающий в себя анализ основных тенденций трансформации института договора в условиях цифровизации. Использование диалектического

подхода также заключается в применении формально-юридического и сравнительно-правового методов при анализе международно-правовых актов.

#### РЕЗУЛЬТАТЫ

*Изложение основного материала исследования с полным обоснованием полученных научных результатов.* Федеральный проект «Нормативное регулирование цифровой среды» предусматривает поэтапную разработку и реализацию законодательных инициатив по снятию барьеров, которые препятствуют развитию цифровой экономики. Кроме того, в рамках реализации данного федерального проекта планируется создать благоприят-

ное правовое поле для реализации проектов цифровизации в российской юрисдикции.

— Параллельно ведется работа над концептуальными актами, призванными обеспечить возможность для создания новой, более эффективной системы управления инновациями, в т. ч. посредством развития регуляторных

песочниц, а также площадок для организационного и технологического пилотирования новых цифровых технологий [2].

зированных) договоров. В п. 1.4 федерального проекта «Нормативное регулирование цифровой среды» обращается внимание на необходимость разработки и принятия федерального закона, в котором будет уточнено понятие «электронный документ», определены процедуры хранения документов (в т. ч. электронных), а также процедуры хранения и использования электронных дубликатов (образа) документов.

Для реализации указанного федерального проекта необходимо было пересмотреть и изменить некоторые классические положения Гражданского Кодекса РФ, в т. ч. о форме сделки.

В соответствии с действующим гражданским законодательством, заключение договора в письменной форме осуществляется двумя способами: путем обмена документами (телеграммами, письмами, телефаксами, электронными документами) и путем составления одного документа, подписываемого сторонами (п. 2 ст. 434 ГК РФ).

Следует отметить, что ГК РФ не устанавливает обязанности сторон по использованию при заключении договоров в электронной форме каких-либо определенных технических устройств или информационных технологий. Виды применяемых технических устройств и информационных технологий определяются сторонами на свое усмотрение. К примеру, они могут быть согласованы в рамочном договоре, заключенном сторонами, устанавливающим условия и порядок заключения соглашений в электронной форме.

В п. 3 ст. 434 ГК РФ закреплена общая фикция письменной формы. Она будет считаться соблюденной, если письменное предложение о заключении договора было принято путем совершения стороной, получившей оферту, действий по исполнению указанных в ней условий договора (уплата определенной суммы; выполнение работы; оказание услуги; отгрузка товара), если что-либо иное не предусматривается законом, иными нормативно-правовыми актами или не указано непосредственно в оферте (п. 3 ст. 438 ГК РФ). Эволюция формы сделок обуславливается тем, что в современной практике многие договоры уже давно заключаются через интернет (посредством электронной почты или интернет-сайтов). Заключение договора с помощью электронной почты соответствует предусматриваемому законом механизму «обмена документами», представляя собой способ заключения договора в письменной форме. Заключение договоров через интернет-сайты имеет некоторые особенности. В данном случае используется два варианта заключения договоров:

1. Click-wrap. Пользователь может предварительно ознакомиться с условиями договора и при согласии с ними, кликнуть на соответствующую кнопку («Принимаю условия», «Я согласен» и т. д.).

2. Browse-wrap (web-wrap). Пользователю предоставляется возможность перейти по гиперссылке и ознакомиться с условиями. Или же на мониторе высвечивается надпись о том, что, продолжая пользоваться данным интернет-сайтом, он принимает условия соглашения. В данном случае пользователь не выражает согласия с условиями в явной форме.

Если в договоре не указано что-либо иное, то местом заключения договора, оформленного посредством сети интернет, будет считаться место нахождения или жительства субъекта, которым была направлена оферта, то есть предложение о заключении договора (ст. 443 ГК РФ).

Отечественные исследователи придерживаются разного мнения по поводу соответствия соглашений «click-wrap» требованию о письменной форме сделки. Так, к

В федеральном проекте (п. 1.3) обращается внима- примеру, Витко В.С. говорит об отсутствии такого со-ние  
Папачо. Необходимость принятия федерального закона, ответственности. Свою точку зрения он аргументирует ссыл-  
которым будет предусматриваться регулирование ста- кой на действовавшую ранее редакцию п. 3 ст. 1286 ГК  
туса сделок, совершаемых в письменной (электронной) РФ, где говорилось о возможности изложения договор-  
форме, а также статуса самоисполняемых (автомати- ных условий на экземпляре компьютерной программы

(в действующей редакции — п. 5 ст. 1286). Также Витко В.С. отмечает, что соглашение заключается не в порядке, предусмотряемом п. 3 ст. 438 ГК РФ, поскольку в данном случае отсутствует письменное предложение правообладателя о заключении лицензионного договора. В связи с этим, данные соглашения должны считаться ничтожными (недействительными), так как письменная форма не соблюдена [3].

По мнению Волос Е.П. [4] такое соответствие имеет место. В обоснование своей позиции он приводит положения, закрепленные в п. 3 ст. 434 и п. 3 ст. 438 ГК РФ. При заключении соглашения «click-wrap» имеет место предложение о заключении договора, исходящее от провайдера или правообладателя [5]. Такое предложение излагается в письменной форме и может расцениваться как оферта, так как в нем содержится указание на юридически обязывающий характер и намерение субъекта, направившего оферту, считать себя связанным им при

его акцепте пользователем. В связи с тем, что соглашение содержит указание на то, что, нажимая на кнопку «я согласен», пользователь выражает свое согласие с договорными условиями, то совершение таких действий можно рассматривать как действия по выполнению условий, указанных в оферте (т. е. как акцепт письменной оферты конклюдентными действиями) [6].

Таким образом, главная загвоздка здесь в вопросе о квалификации соответствующих действий правообладателя, подрядчика, исполнителя, продавца, именно как письменной оферты.

Обратим внимание на то, что наличие письменной оферты при заключении click-wrap-соглашений не подлежит оспариванию, если такое предложение соответствует признакам ст. 435 ГК РФ, то есть является достаточно определенным, выражает намерение оферента считать себя заключившим договор с пользователем, принявшим предложение, а также содержит в тексте существенные условия договора.

Как правило, подобные контракты квалифицируются в качестве договоров, заключенных в письменной форме в соответствии с п. 3 ст. 434 и п. 3 ст. 438 ГК РФ.

В случае с совершением сделок по модели browser-wrap (web-wrap) ситуация осложняется тем, что пользователем не выражается прямого (явного) согласия с предложенными условиями. В значительной степени это зависит от способа визуализации соответствующих данных на интернет-сайте, поэтому действия пользователя не в каждом случае расцениваются как акцепт. Таким образом, вряд ли можно говорить о возможности определения общего правила о соответствии либо несоответствии таких соглашений требованию о письменной форме сделки. Решить данный вопрос можно только с учетом фактических обстоятельств конкретного дела.

В рассматриваемом положении национальной программы «Цифровая экономика Российской Федерации» содержится фраза «урегулирование статуса совершаемых в письменной (электронной) форме сделок». Данная формулировка порождает вопросы, касающиеся правового режима соответствующих сделок и соотношения электронной и письменной формы. Можно ли рассматривать электронную форму сделок в качестве самостоятельной? Либо она является подвидом письменной формы? Если электронная форма — подвид письменной формы, актуальное проблемное правоприменение в ст. 160 ГК РФ и 434 ГК РФ? Или это новая разновидность реализации фикции письменной формы, предусмотряемой п. 3 ст. 434 ГК РФ?

Повсеместный переход к электронному документообороту требует надлежащего правового регулирования. Данная задача постепенно решается и в России, и в

электронных сообщений в международных договорах» (была принята резолюцией Генассамблеи ООН 60/21 от 23.11.2005 года) указано, что договор или сообщение не могут считаться недействительными на том основании, что они имеют форму электронного сообщения [7]. Конвенция ООН не содержит требований, обязывающих стороны использовать электронные сообщения и принимать их. Однако согласие на это может быть выведено из поведения стороны.

В ст. 9 Конвенции ООН указывается, что сделки, совершаемые с помощью электронных сообщений, квалифицируются в качестве разновидности письменной формы сделок. Если национальным законодательством установлено требование о письменной форме договора, то данное требование считается соблюденным путем представления электронного сообщения, если содержащиеся в нем данные доступны для дальнейшего использования.

В Типовом законе ЮНСИТРАЛ об электронной торговле от 1996 года используется понятие «data message» («сообщение данных»). Это понятие трактуется как информация, подготовленная, хранимая, полученная или отправленная при помощи оптических, электронных и иных аналогичных средств, включая электронный обмен данными, телефакс, телекс, телеграмму, электронную почту и т. д. [8]

В ст. 11 Типового закона ЮНСИТРАЛ отмечается, что, если сторонами не определено что-либо иное, то оферта и ее акцепт могут быть произведены посредством сообщения данных. В таком случае договор будет считаться действительным.

По поводу письменной формы в ст. 6 рассматриваемого закона закреплено правило, согласно которому, когда национальное законодательство содержит требование об обязательном представлении информации в письменной форме, данное требование будет считаться выполненным посредством сообщения данных, если такие данные являются доступными для дальнейшего использования.

Модельные правила европейского частного права (Draft of Common Frame of Reference, DCFR) не содержат упоминания об электронных сообщениях. В этом документе раскрыто понятие «электронная подпись», под которой предлагается понимать информацию, закрепленную в электронной форме (которая присоединена к другим данным и логически объединена с иными сведениями в электронной форме), используемую в качестве способа идентификации (1-1:107(3)). Слово «электронный» используется в контексте оптических, беспроводных, магнитных, цифровых, электронных, электромагнитных и аналогичных технических возможностей (1-1:107(5)). [9]

В Модельных правилах отдельно указывается на то, что, если договор должен быть заключен посредством электронных средств, то сторона, которая предложила условия, не согласованные специально, вправе ссылаться на них в отношениях со своим контрагентом, если данные условия были доведены до него в текстовой форме (1-1:103 (2)). В рассматриваемом акте также отмечается, что заявление будет признано имеющим письменную форму, если оно сформировано в форме текста, состоящего из знаков, разборчиво изображенных на любом материальном носителе (1-1:106). В ст. 1-1:106 Модельного закона раскрывается категория материального носителя и текстовой формы. Под материальным носителем подразумевается носитель, на котором информация сохраняется с условием обеспечения возможности ознакомления с нею в будущем, а также ее воспроизводимость в неизменном виде. Текстовая форма — это

международной практике. Следовательно, при решении рассматриваемого вопроса целесообразно учитывать иностранную и международную практику, отраженную в унифицированных документах частного права. текст, выраженный при помощи букв алфавита и других печатных знаков, позволяющих прочесть, записать и воспроизвести на материальном носителе информацию, которая содержится в тексте [10].

В ст. 8 Конвенции ООН «Об использовании элек-

На основании обзора международных правовых до-

критерия соответствия информации в электронной форме требованиям письменной формы выступает воспроизводимость и доступность информации для дальнейшего использования.

Понятие «электронная форма сделки» встречается в национальном законодательстве некоторых стран. Так, в национальном законодательстве Сингапура отражены подходы, закрепленные в Конвенции ООН и Типовом законе ЮНСИТРАЛ. Акт об электронных транзакциях от 2010 года (The Electronic Transactions Act, ETA) содержит понятие «electronic record» («электронная запись», «электронный документ»). Понятие «электронная форма сделки» в данном акте не используется [11].

В Соединенных Штатах модельные подходы отражены в Едином законе США от 1999 года об электронных сделках. В соответствии с этим законом, стороны могут согласовать использование «electronic form» (электронной формы), электронных средств безопасности, электронной подписи и установить содержание сделки [12].

Исходя из § 126a (Elektronische Form) Германского гражданского уложения (ГГУ), сделки, в отношении которых установлено требование о соблюдении письменной формы, могут совершаться в электронной форме и подписываться квалифицированной электронной подписью. В § 312c ГГУ предусмотрена возможность заключения сделок дистанционным способом.

Вопрос, связанный с регламентацией порядка совершения сделок с использованием цифровых технологий, решался в ходе рассмотрения законопроекта № 424632-7

«О внесении изменений в часть первую, вторую и третью Гражданского кодекса Российской Федерации», внесенного в Госдуму РФ 26.03.2018 года. В настоящее время соответствующий закон принят и вступил в силу 01.10.2019 года (Закон № 34-ФЗ от 18.03.2019 г.).

Указанный законопроект дорабатывался и корректировался на разных этапах его рассмотрения. Например, в ходе второго чтения были учтены существенные замечания, отраженные в заключении Совета при Президенте РФ по кодификации и совершенствованию гражданского законодательства от 17.01.2019 г.

Положения п. 1 ст. 160 ГК РФ были дополнены абз.

2, где указывается, что письменная форма сделки будет считаться соблюденной и в случае совершения лицом сделки при помощи электронных и других технических средств, позволяющих воспроизвести содержание сделки (договора) на материальном носителе в исходном (неизменном) виде [7]. Требование о наличии подписи будет считаться исполненным при использовании любого способа, позволяющего достоверно определить субъекта, выразившего волю. При этом законом, соглашением

сторон или нормативно-правовыми актами может предусматриваться специальный способ достоверного определения субъекта, выразившего волю.

Примечательно, что в окончательном варианте закона отражена формулировка, характеризующая соответствующие технические средства как такие, которые позволяют воспроизвести содержание сделки на материальном носителе в неизменном виде. Именно это положение обладает огромным значением для предотвращения нарушения прав участников оборота, включая потребителей. Решение законодателя включить данное положение в закон в окончательном варианте является

лицо, выразившее волю, законом, иными правовыми актами и соглашением сторон может быть предусмотрен специальный способ достоверного определения лица, выразившего волю») отметим, что системность данного решения, по всей видимости, будет завершена после совершенствования закона об идентификации. Представляется, что совершенствование данного закона будет происходить на основе законопроекта «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» [11]. Предлагается дополнить этим законопроектом положения Закона № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» понятиями «идентификатор», «идентификация, аутентификация лица»; ввести понятие «цифрового профиля» и его регулирование; внести ряд корреспондирующих изменений в другие федеральные законы (например, в Закон «Об основах охраны здоровья граждан в РФ», Закон «О персональных данных», Закон «О связи»).

Некоторые изменения были внесены и в п. 2 ст. 434 ГК РФ. Теперь здесь указано, что заключение договора в письменной форме возможно путем составления одного документа, подписанного сторонами (в т. ч. электронного), либо путем обмена телеграммами, письмами, электронными документами и иными данными в согласии с правилами, закрепленными в абз. 2 п. 1 ст. 160 ГК РФ.

Из предыдущей редакции описания обмена документами законодатель исключил телефаксы и телексы, которые уже почти не используются на практике, а также термин «электронный документ».

В соответствии с содержанием абз. 2 п. 2 ст. 434 ГК РФ (в ред. Закона № 42-ФЗ от 08.03.2015 года), утратившего силу 01.10.2019 г., электронный документ, передаваемый по каналам связи – это данные, подготовленные, хранимые, полученные или отправленные при помощи оптических, магнитных, электронных и других аналогичных средств, в т. ч. обмен информацией в электронном виде и через электронную почту.

Начиная с 01.10.2019 года, при толковании положений гражданского законодательства об электронных документах, которых стало больше, необходимо руководствоваться положениями Закона № 149-ФЗ от 27.07.2006

года «Об информации, информационных технологиях и о защите информации». Под электронным документом здесь понимается документированная информация, которая представлена в электронной форме, т. е. в виде, пригодном для человеческого восприятия с использованием электронных и технических средств, а также для обработки в информационной системе и передачи по информационно-телекоммуникационной сети (п. 11.1 ст. 2 Закона № 149-ФЗ).

## ВЫВОДЫ

*Выводы исследования.* Основываясь на вышеизложенном, приходим к выводу, что российский законодатель решил отказаться от ранее предложенного подхода о выделении специальной категории «электронная форма сделки» (известной американскому и германскому праву). Как можем видеть, были восприняты подходы, отраженные в Типовом законе ЮНСИТРАЛ и в Конвенции ООН. Был введен еще один случай фикции письменной формы договора, так как при заключении сделок при помощи технических и электронных средств такая форма только «считается соблюденной». Решить этот вопрос

между на

родных документов, которые были рассмотрены [5].

В окончательном варианте Закона не было учтено замечание, указанное в вышеупомянутом заключении

можно путем внесения дополнений в п. 3 ст. 438 ГК РФ. Данный пункт может быть дополнен нормой, согласно которой, акцептом может считаться, как исполнение договора, так и совершение других указанных в офер-



гражданского законодательства о письменной форме сделки предусмотрено две ее вариации (обмен документами и один документ, подписанный сторонами), а так-же две основные фикции письменной формы (совершение сделки при помощи технических или электронных средств; акцепт действием на письменную оферту).

Перспективы дальнейших изысканий в данном направлении. Таким образом, внесенные в 2019 году изменения в гражданское законодательство в части регулирования смарт-контрактов позволяют констатировать факт трансформации договорного права. В настоящее время паспортом национальной программы «Цифровая экономика» предусматривается внесение изменений в отраслевое законодательство (например, банковское, финансовое) в части договорного регулирования. При их принятии необходимо отслеживать изменение тенденций (в т.ч. в деловой практике) с целью формирования эффективного регулирования договорных отношений. Указанное должно стать предметом последующих исследований.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Goncharov A.I., Goncharova M.V. Digital tokens in the tools of modern foreign trade activities by economic entities of the brics jurisdictions // *Legal Concept*. 2019. Т. 18. № 3. С. 31-42.
2. Бирюкова М.И., Белоусов А.Л. Правовые риски использования смарт-контрактов в банковской деятельности // *Вектор экономики*. 2019. № 11 (41). С. 60.
3. Волос А.А. К вопросу о правовом значении смарт-контрактов // *Правовая политика и правовая жизнь*. 2019. № 3. С. 67-71.
4. Волос Е.П. К вопросу о применении смарт-контрактов в различных сферах // *Евразийская адвокатура*. 2019. № 3 (40). С. 105-110.
5. Голикова Е.А. Смарт-контракт как новый механизм организации договорных отношений // *Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 4: Промышленные технологии*. 2019. № 1. С. 18-19.
6. Ивлев Д.И. Последствия внедрения цифровых прав в Российской Федерации // *Образование и право*. 2019. № 9. С. 46-49.
7. Камалян В.М. Понятие и правовые особенности смарт-контрактов // *Юрист*. 2019. № 4. С. 20-27.
8. Кувшинова В.В., Дарсавелидзе И.В. Цифровые инновации в экономике: социально-правовые аспекты // *Вестник Санкт-Петербургской юридической академии*. 2019. № 4 (45). С. 57-64.
9. Новиков Р.В. К вопросу о понятии и сфере применения смарт-контрактов // *Пермский юридический альманах*. 2019. № 2. С. 431-440.
10. Сафаргалеев Л.И. Смарт-контракт - программный код, а не договор // *Хозяйство и право*. 2019. № 5 (508). С. 21-34.
11. Шапсугова М.Д. Обзор основных подходов к пониманию правовой природы смарт-контракта // *Финансовая экономика*. 2019. № 9. С. 417-422.
12. Юламанова А.А. Правовые проблемы заключения и исполнения смарт-контрактов // *Юридический факт*. 2019. № 50. С. 24-28.

### **№ 13. Трудовые отношения в финансово-цифровой среде. Особенности использования смарт-контрактов. Проблемы ведения электронного документооборота.**

Цифровая экономика вызывает крупные социально-экономические сдвиги в сфере трудовых отношений, меняя тип профессиональной деятельности и характер самого труда. Новый характер труда связан с повышением его квалификации, постоянным обучением и развитием творческих способностей. Переход к цифровой экономике предполагает существенные изменения трудовых отношений, появление «дистанционных отношений» между работниками и их работодателями. Идет процесс формирования гибкого рынка труда. Классическая модель полной занятости изжила себя, так же как пожизненная работа на одного работодателя. Рынок труда стимулирует создание новых высокопроизводительных рабочих мест путем увеличения удельного веса нетипичных форм трудовой занятости, которые становятся все более востребованными. Развитие рынка труда на основе цифровых

...им сетевых форм. При дистанционном контакте работодатели и исполнители активно используют ИКТ: например, переводчик, выполнивший заказ для издателя, может отослать готовый текст по электронной почте. Если в традиционной экономике между работником и руководителем существуют вертикальные экономические связи «управление – подчинение», то в цифровом секторе руководитель уже не столько начальник, сколько человек, координирующий работу людей, находящихся на большом расстоянии друг от друга. Соответственно вертикальные связи заменяются горизонтальными. Одним из следствий этого является децентрализация трудовой деятельности. Значительно ослабляется зависимость работника от руководства компании. В цифровой экономике достаточно иметь компьютер и выход в интернет, чтобы высококлассный специалист стал относительно независимым и даже имел возможность формировать портфель заказов, согласовывать объем и сроки выполнения работ, а также размер собственного вознаграждения. Развитие трудовых отношений в цифровой экономике способствует замене постоянного штата временными исполнителями. Только в США в 2018 г. насчитывалось 56,7 млн человек, работающих в фриланс-режиме, что составляет 36 % от работающего населения страны. Одним из наиболее распространенных видов трудовых отношений в цифровой экономике является работа на дому, главная особенность которой – выполнение работы у себя дома вместо перемещения в офис на период рабочего дня. Кроме этого, популярна работа во время отпуска (в поезде, в самолете), работа на иностранного работодателя без выезда за рубеж (например, работа на дому оффшорных программистов) и т. п. Крупные компании США, в том числе Amazon, IBM, Apple, Wells Fargo и другие, постоянно предлагают удаленную работу с частичной или полной занятостью. Последние данные по США показывают, что максимальную гибкость рабочих мест обеспечивает финансовый сектор: 57 % работников этой отрасли могут работать на дому. Кроме того, почти половина людей, занятых в сфере профессиональных, деловых и информационных услуг, могут работать удаленно. Рис. 13.1.

Преимущества занятости в цифровой сфере Занятость в цифровой сфере дает индивиду преимущества (рис. 13.1).

13.2. Цифровые навыки и компетенции В цифровой экономике требуются новые навыки и компетенции. Для работодателей в настоящее время среди молодых специалистов становятся приоритетными так называемые мягкие навыки (soft skills): личные качества и социальные навыки, например, умение работать в команде, любознательность, Преимущества цифровой занятости Снижение времени и затрат на транспорт Возможность работы в привычной домашней обстановке Оптимизация распределения времени между работой, досугом и общением с семьей Новые перспективы для участия в общественной жизни Возможность сохранения навыков и квалификации Гибкий график труда Широкая сеть полезных связей и контактов Лучший доступ к полезной информации Новые

мышление, способность решать сложные задачи, взаимодействовать с разными людьми и правильно расставлять приоритеты. При этом роль формальных дипломов и сертификатов об образовании значительно снизилась. Google, Apple и IBM уже не требуют дипломов о высшем образовании при приеме на работу, достаточно релевантного опыта. Новые условия труда требуют новых навыков – цифровых. Цифровые навыки – это совокупность навыков использования цифровых устройств, коммуникационных приложений и сетей для поиска и управления информацией, создания и распространения цифрового контента, взаимодействия и сотрудничества, а также для решения проблем – в контексте эффективной и креативной самореализации, обучения, работы и социальной активности в целом. В классификации, принятой в Канаде, цифровые навыки включают следующие категории: 1. Основополагающие, фундаментальные навыки, включающие базовую грамотность, письмо, использование документов и счета, без которых могут быть успешно выполнены только низкоквалифицированные работы. 2. Трансверсальные навыки включают в себя в основном передаваемые и гибкие навыки, такие как работа в команде, непрерывное обучение, решение проблем и развитие отношений. 3. Цифровые технические навыки – использование компьютера и программного обеспечения, применения мер сетевой безопасности и др. 4. Навыки цифровой обработки информации – когнитивные навыки высокого уровня в отношении обработки информации, например, поиск и синтез информации; оценка, применение, создание и передача информации. Использование новейших цифровых технологий, требования новых условий конкуренции заставляют компании по-другому относиться к подбору, подготовке, переподготовке и удержанию кадров. Специалисты с цифровыми навыками становятся ключевым ресурсом в конкурентной стратегии фирмы. Согласно исследованию, проведенного по заказу британского правительства, уже к 2022 г. примерно 22 % новых рабочих мест в глобальной экономике будет создано благодаря новым цифровым профессиям. В обозримом будущем основная ставка будет делаться на рекрутировании персонала, обладающего необходимыми цифровыми навыками. Более того, 73 % недавно опрошенных компаний уже сегодня испытывают серьезные проблемы при поиске таких квалифицированных специалистов. Осознавая эту угрозу, многие компании совместно с ведущими вузами и колледжами активно развивают специальные образовательные и тренинговые программы. Особую популярность приобретают курсы и программы онлайн-обучения для повышения цифровых компетенций собственного персонала. 116 13.3.

Изменения на рынке труда и занятость На любом этапе социально-экономического развития страны рынок труда является наиболее чувствительным индикатором и реактором изменения рыночной

## конъюнктуры. При возникновении глобальных экономических шоков рынок

реагирует высвобождением наименее конкурентоспособных кадров, при росте экономики рынок сигнализирует о росте спроса на востребованных специалистов через повышение уровня оплаты труда. Предполагают два сценария развития рынка труда в условиях цифровизации экономики (рис. 13.2 и 13.3). Рис. 13.2. Оптимистический прогноз развития рынка труда в цифровой экономике Рис. 13.3. Пессимистичный прогноз развития рынка труда в цифровой экономике

Возможный сценарий Производство не будет нуждаться в людях, однако они будут необходимы для сферы человеко-ориентированных услуг Люди цифровой эры будут обеспечивать производство, хранение, переработку и реализацию информации, создание уникальных знаний, а также управление ими Будут развиваться технологии глобализации труда, база которой сосредоточится на онлайн-управлении роботизированной техникой (ботами) Возможный сценарий В ходе цифровизации производства вещи станут теснее общаться друг с другом, а между людьми станет нарастать отчуждение Цифровизация может породить негативный эффект, когда цепочка создания продукта сведется к минимуму, достаточен охват проектирования, 3D-печати и доставки К 2030 г. рабочей силы будет количественно меньше, она будет старше, формально более образованной, с тенденцией вымирания 50 % профессий, не известно насколько обучаема

117 Еще в 2016 г. экономисты и социологи серьезно задумались над угрозой массовой потери людьми работы из-за роботов, когда китайский производитель электроники Foxconn принял на работу 40 тыс. роботов и сократил 60 тыс. чел. Многие эксперты считают, что страхи перед тотальной автоматизацией сильно преувеличены. Они предполагают, что роботы возьмут на себя низкооплачиваемый труд и рутинные операции. Это сделает производственные процессы более эффективными, исключит вероятность человеческой ошибки и поможет людям выделять время на более творческую работу. Эксперты агентства Moody's уверены, что внедрение робототехники поможет решению демографических проблем на рынке труда ЕС и Японии (увеличение доли населения старше пенсионного возраста при сокращении рабочей силы). Однако темпы мировой роботизации недвусмысленно говорят о том, что мы постепенно идем к безлюдной промышленности. В некоторых обзорах утверждается, что более половины всех ныне существующих рабочих мест либо изменятся, либо полностью исчезнут (табл. 13.1). Таблица 13.1 Оценки воздействия цифровых технологий на занятость Организация Прогнозная оценка ОЭСР В среднем по ОЭСР: 9 % рабочих мест с высоким риском автоматизации в течение ближайших пяти лет. Низкий риск полной автоматизации, но значительная доля (от 50 % до 70 %) автоматизированных задач, подверженных риску

— Всемирный банк Две трети всех рабочих мест в развивающихся странах подвержены автоматизации Всемирный экономический форум Глобальное

Международная организация труда АСЕАН-5: 56 % рабочих мест подвержены риску автоматизации в ближайшие 20 лет Оксфордский университет 47 % работников в США с высоким риском замены рабочих мест автоматизацией PricewaterhouseCoopers 38% рабочих мест в США, 30 % рабочих мест в Великобритании, 21 % в Японии и 35 % в Германии подвержены риску автоматизации McKinsey 60 % всех профессий имеют не менее 30 % технически автоматизированных видов деятельности Роланд Бергер Западная Европа: к 2035 г. 8,3 млн рабочих мест будут потеряны в промышленности против 10 млн новых рабочих мест, созданных в сфере услуг Клаус Шваб Ликвидация к 2020 г. около 5 млн рабочих мест в 15 крупнейших развитых и развивающихся странах мира В докладе Всемирного экономического форума The Future of Jobs 2018 говорится о том, что человеческая доля работы, выраженной в человеко-часах, снизится с 71 % в 2018 г. до 48 % к 2025 г. Машины и алгоритмы увеличат свой вклад 118 в конкретные задачи в среднем на 57 %. Например, к 2022 г. 62 % задач организации поиска, обработки и передачи информации будут выполняться машинами по сравнению с 46 % сегодня. Новые исследования ОЭСР 2018 г. показывают, что 14 % всех рабочих мест имеют высокий риск автоматизации. Еще 32 % рабочих мест могут иметь значительные изменения в ближайшем будущем. Поскольку проще всего автоматизировать те виды работ, которые требуют выполнения предсказуемых повторяющихся физических операций, в первую очередь этот процесс коснется рабочих мест, требующих средней квалификации. Они будут замещаться низкооплачиваемыми (когда автоматизация представляется экономически нецелесообразной) и высокооплачиваемыми (когда необходимы навыки создания и применения цифровых инструментов) рабочими местами. Вероятные последствия: расслоение населения по уровню доходов, рост безработицы, а также снижение уровня доходов и жизни людей в населенных пунктах с ограниченными возможностями для трудоустройства (так называемых моногородах). Согласно докладу The Future of Jobs 2018, к 2022 г. 75 млн нынешних рабочих мест будут ликвидированы в результате будущего разделения труда между людьми и машинами, но также будет создано дополнительно 133 млн новых рабочих мест. Несмотря на значительные изменения, перспективы в области занятости в целом позитивны, а рабочие места с ярко выраженными человеческими навыками по-прежнему будут востребованы. Таблица 13.2 Новые и исчезающие профессии Новые профессии Исчезающие профессии Аналитики данных Специалисты по искусственному интеллекту и машинному обучению, большим данным, цифровой трансформации Профессионалы в области маркетинга и продаж Специалисты по организационному развитию Разработчики и аналитики программного обеспечения и приложений Специалисты по автоматизации

информационной безопасности Специалисты по электронной торговле и социальным медиа Специалисты и инженеры по робототехнике Специалисты по цифровому маркетингу и стратегиям Операторы ввода данных Исполнительные секретари Бухгалтеры и аудиторы Налоговые инспекторы Работники почтовой службы Банковские служащие Финансовые аналитики Агенты по продажам и торговые посредники Брокеры Кассиры Рабочие сборочных конвейеров Водители автомобилей и фургонов Установщики и ремонтники электронного и телекоммуникационного оборудования Продавцы в магазинах Специалисты по статистике, финансам и страхованию Адвокаты

119 Вымирание профессий в период цифровой трансформации ставит необходимость перед государством разработки новой программы, которая выступит связующим звеном между спросом/предложением рынка труда и цифровой грамотностью общества. Хотя трудно детально предсказать потенциальные изменения, которые могут повлиять на рынок труда в предстоящие годы, важно, чтобы директивные органы повышали его устойчивость и адаптируемость. С 2018 г. по инициативе ОЭСР на постоянной основе функционирует форум G7 Future of Work, где анализируется, как демографические изменения, глобализация и цифровизация влияют на количество и качество работы и что это означает для рынка труда, навыков и социальной политики. На форуме публикуются стратегии, передовые методы и опыт стран G7 в решении новых проблем на рынке труда.

13.4. Реформирование системы образования в условиях цифровой экономики Основной подход к современному образованию можно определить так: высокопрофессиональная подготовка, владение современными цифровыми технологиями, языковая подготовка, непрерывность образования.

1. Адаптация системы образования к изменениям на рынке труда под влиянием цифровизации. Для успешного развития цифровой экономики система образования и переподготовки кадров должна обеспечивать экономику специалистами, востребованными цифровой эпохой.
2. Переобучение абсолютно всех преподавателей и учителей с целью освоения цифровых образовательных технологий. Должны быть предприняты решительные меры для профессионального развития преподавателей в области цифровой трансформации. Необходимо сконцентрировать внимание на изменении работы институтов и центров повышения квалификации преподавателей, которые должны базироваться на современных ИТ-программах.
3. Смешанное обучение. Необходимо сократить число аудиторных лекций и их продолжительность минимум вдвое, сведя их к дискуссиям, обсуждению домашних заданий, выполненных в форме презентаций, и ответам на вопросы по теме. Обучение следует адаптировать также к такой реалии, как работа без отрыва от учебы.
4. Интеграция

университеты дают сверхсовременное, но недостаточно системное и фундаментальное образование, классические университеты далеки от современного образования и новых технологий преподавания. 5. Повышение уровня цифровой и предпринимательской грамотности абсолютно всех школьников и студентов. За время обучения все школьники и студенты должны подготовиться к работе в условиях цифровой трансформации общества и рыночной экономики, т. е. должны научиться вести цифровое предпринимательство в своей сфере. Школы и университеты должны нести ответственность за превращение обучаемых в активных цифровых граждан. 120 6. Всеобщая информатизация образования. ИТ-образование должно быть буквально в каждом предмете – сегодня нет науки, не использующей информационные технологии. На первых курсах всех специальностей должен изучаться современный курс «Информационные технологии», включающий в себя интернет вещей, облачные вычисления, большие данные, блокчейн и т. п. 7. Внедрение в вузах систем разноскоростного обучения. Сегодня при значительной доле платных и иностранных студентов скорость обучения не может быть одинаковой, поэтому необходимо упразднить переводы с курса на курс и разрешить обучаться вместо четырех лет столько, сколько потребуется. Аргументом в пользу такого типа обучения также является новая система адаптивного образования, которая позволяет менять сложность и содержание курсов в зависимости от интеллектуального уровня студента. 8.

Трансформация вузов в цифровые университеты. Сами вузы и их структура управления должны подвергнуться цифровой трансформации. Разрозненные усилия отдельных служб и факультетов необходимо интегрировать в единую систему взаимодействия вуза и внешнего мира с использованием всего спектра сетевых каналов коммуникации. 9. Преподаватели и руководство вузов должны общаться в социальных сетях. Вся воспитательная и идеологическая работа со студентами должна быть перенесена в социальные сети, которые помогают мгновенно распространять информацию о событиях, происходящих в коллективе, лучших публикациях, грантах, поездках за рубеж, мировых профессиональных достижениях; это средство объединения студентов и выпускников, содействующих получению первого рабочего места. 10. Университеты должны стать драйверами цифровой трансформации экономики и общества. Важно, чтобы структура университетов, их технопарки и бизнес-инкубаторы совместно с преподавателями способствовали зарождению и становлению университетских молодежных стартапов. Цифровая трансформация белорусского образования. Для того чтобы адаптация рынка труда к революционным изменениям прошла успешно, важно, чтобы Беларусь заблаговременно выработала действенные

— **ответы на вызовы цифровой эпохи.** Достигнутых успехов пока недостаточно, чтобы говорить о готовности белорусской системы образования к решению

государства по адаптации системы образования к потребностям цифровой экономики может стать обновление устаревших программ профессионального образования и повышения квалификации для ликвидации пробелов в цифровых навыках, необходимых в современной экономике. Следует сосредоточить внимание на развитии у обучаемых личностных, социальных навыков и навыков решения межпредметных задач, ориентированных на практику, а также на применении современных методик, форматов 121 и инструментов обучения, включая цифровые образовательные средства и форматы удаленного образования. Важно развивать взаимодействие образовательных и исследовательских организаций между собой, с бизнес-сообществом и с государственными органами, чтобы обеспечить актуальность образовательных программ и сократить время адаптации образовательной системы к требованиям рынка. Помимо модернизации системы подготовки кадров, необходимо также обеспечивать возможность их самореализации в Беларуси. Для обеспечения профессионального развития высококвалифицированных кадров в Беларуси нужно совершенствовать платформы взаимодействия студентов и потенциальных работодателей, создавать благоприятные условия для развития технологических компаний и стартапов, а также принимать меры по повышению качества жизни в стране в целом. Для расширения кадрового потенциала в области цифровых технологий Беларусь также может по примеру других стран разработать программу привлечения специалистов из-за рубежа. Выводы по теме 13. Проблемы занятости населения в условиях цифровой экономики приобретают новый смысл: человеческий и социальный капитал рассматриваются в качестве ключевых источников богатства, что требует концептуального переключения сознания людей с позиций максимизации прибыли на позиции максимизации полезности. Период вхождения в цифровую экономику требует быстрого реагирования на изменения на рынке труда, вложений в человеческий капитал и деятельность по его качественному улучшению, адаптации к новым условиям, программных мер со стороны государства. Цифровые технологии трансформируют современный сектор образования в направлениях: высокопрофессиональная подготовка, владение ИКТ, языковая подготовка, непрерывность образования.

#### **№ 14. Правовые основы обеспечения и защиты прав в финансово-цифровой среде. "Цифровая" криминалистика.**

В Казахстане активно разрабатываются проекты нормативных правовых актов разного уровня, регулирующих процессы цифровизации, информатизации, использования технологий, обработки информации и пр.

— Без сомнения, такой процесс закономерен, поскольку цифровая

трансформация отраслей и развитие инновационной экономики являются

Национальным планом развития РК до 2025[1] года предусмотрены отдельные задачи и направления по внедрению цифровизации, включая: создание инфраструктуры, позволяющей внедрить аналитику на основе искусственного интеллекта и Big data, автоматизация и цифровизация предприятий базовых отраслей, цифровая трансформация многих сфер жизнедеятельности.

Постановлением Правительства РК утверждена Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы[2], которая определяет оптимальные пути решения насущных вопросов в области оказания государственных услуг для населения и бизнес-сообщества, трансформация государственного управления и дальнейшее развитие отраслей экономики с использованием возможностей цифровых технологий.

Реализация всех мероприятий и процессов в сфере цифровизации и информатизации должна проводиться в строгом соответствии с нормативно-правовой основой. Как и в большинстве стран мира, в Казахстане пока не сформирована нормативно-правовая база, в должной мере регулирующая внедрение и развитие цифровых процессов. Самой важной же проблемой в аспекте правового регулирования цифровой среды в Казахстане является отсутствие законодательно определенной системы принципов и подходов, в соответствии с которыми разрабатывались бы регуляторные требования.

Концепцией правовой политики до 2030 года, утвержденной Указом Президента РК[3], определены следующие задачи:

1. Необходимость правового регулирования искусственного интеллекта и робототехники, прежде всего, в целях определения ответственности за вред, причиненный их действиями, а также решением проблемы определения принадлежности права интеллектуальной собственности на произведения, созданные с участием искусственного интеллекта. Проработки вопроса о возможности наделения роботов правовым статусом и, как следствие, возможности привлечения искусственного интеллекта к юридической ответственности.

2. Пересмотр положений законодательства о персональных данных и их защите в целях приведения его в соответствие с рядом базовых принципов, лежащих в основе этой отрасли законодательства.

3. Урегулирование вопросов недопустимости дискриминации при использовании технологии больших данных и ограничения для неконтролируемого применения гаджетов с целью отслеживания граждан.

Безусловно, основным актом, которым будут определены принципы и подходы к регулированию, а также основополагающие правовые институты и конструкции регулирования цифровой среды, должен стать Цифровой кодекс РК, принятие которого запланировано на 2024 год (п. 4 Плана действий по реализации Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 – 2029 годы). Однако, не дожидаясь момента принятия Цифрового кодекса, разработка проектов НПА разного уровня проводится в режиме нон-стоп. Так, в Закон РК «Об информатизации» за последние три года изменения вносились 12 законами. При этом, отдельные нормы и положения внедряются вне учета того, что в Казахстане, как и в мире на уровне научной доктрины многие вопросы правового регулирования цифровой среды пока не нашли решения. Так, к примеру, в Административный процедурно-процессуальный кодекс (ст. 43-2) внесено положение, определяющее, что «собственником данных, создаваемых, накапливаемых и приобретаемых за счет бюджетных средств, а также полученных иными способами, установленными законами РК, является государство», в то время как Гражданским кодексом РК информация (данные) не отнесены к объектам права собственности. К сожалению, это не единственная подобная ошибка.

ОЮЛ «Ассоциация Цифровой Казахстан» аккредитована в Министерстве юстиции РК, Министерстве торговли и интеграции РК, Министерстве цифрового развития, инноваций и космической промышленности РК, Агентстве РК по защите и развитию конкуренции. Одна из задач, которая стоит перед любой бизнес-ассоциацией – содействие формированию благоприятной правовой среды для предпринимательства. Члены АЦК – крупные казахстанские и иностранные компании, имеющие возможность проводить комплексные аналитические исследования и привлекать ведущих специалистов для подготовки рекомендаций по любым вопросам.

Мы признательны Нестеровой Елене Викторовне, известному казахстанскому цивилисту, за подготовку научного исследования по вопросам правового регулирования информации.

Серия научных публикаций, инициированных АЦК по разным вопросам — регулирования цифровой среды, будет продолжена.

Елена Бычкова

Управляющий директор

ОЮЛ «Ассоциация Цифровой Казахстан»

кандидат юридических наук

\*\*\*

Поводом к подготовке данного материала стали некоторые законодательные инициативы, обсуждаемые в настоящее время в Республике Казахстан, а также не всегда последовательные новеллы отечественного законодательства в сфере регулирования прав на информацию и управления данными.

Так, в июле 2022 года Закон РК «Об информатизации» был дополнен ст. 18-2, согласно п. 1 которой: «Для осуществления деятельности на территории Республики Казахстан собственники и (или) иные законные представители иностранной онлайн-платформы и (или) сервиса обмена мгновенными сообщениями, среднесуточный доступ к которым в течение месяца составляет более ста тысяч пользователей, находящихся на территории Республики Казахстан, назначают своего законного представителя по взаимодействию с уполномоченным органом в области средств массовой информации»[4]. При этом под онлайн-платформой данный законодательный акт понимает интернет-ресурс и (или) сервис обмена мгновенными сообщениями. А интернет-ресурс, в свою очередь, определяется как информация (в текстовом, графическом, аудиовизуальном или ином виде), размещенная на аппаратно-программном комплексе, имеющем уникальный сетевой адрес и (или) доменное имя и функционирующем в Интернете.

Оставляя за пределами настоящего рассмотрения вопросы практической реализации норм, предусмотренных ст. 18-2 Закона «Об информатизации», обращаем внимание на довольно нелепое использование законодателем классических гражданско-правовых категорий собственности и представительства в отношении такого неовещественного объекта — информации.

Этим же Законом по вопросам защиты детей в июле 2022 года Административный процедурно-процессуальный кодекс Республики Казахстан (АППК) был дополнен статьей 43-2, в соответствии с пунктом 3 которой установлено, что «собственником данных, создаваемых, накапливаемых и приобретаемых за счет бюджетных средств, а также полученных иными способами, установленными законами Республики Казахстан, является государство». При этом под данными в АППК понимается «информация в формализованном виде, пригодная для обработки».

Тем самым законодатель без какого-либо предварительного научного обоснования распространил вещно-правовой режим собственности на такое нематериальное благо, как информация, что, разумеется, не согласуется со многими положениями раздела 2 Гражданского кодекса РК о праве собственности и иных вещных правах. Так, в содержание понятия имущества в рамках ст. 188 Гражданского кодекса РК законодатель закладывал исключительно овеществленную собственность (телесные вещи / *res corporales*). Как отмечалось в изданном в 1998 году Комментарии к Общей части Гражданского кодекса, «имущество понимается не в широком смысле как имущественные права, а в узком - вещи, наличные деньги и документарные ценные бумаги. Соответственно электронные денежные средства, бездокументарные ценные бумаги, работы, услуги, объективированные результаты творческой интеллектуальной деятельности, фирменные наименования, товарные знаки и иные средства индивидуализации изделий, имущественные права и некоторое другое имущество не регламентируются правилами раздела 2 ГК»[5]. Указанная позиция сохранилась и в новейшем Комментарии 2022 г.: «Вещный характер права собственности исключает применение норм о собственности к другим отношениям, где объектом выступает не вещь, а иные виды имущества (деньги, права требования права, результаты творческой деятельности и иные объекты, кроме как по аналогии закона)» [6].

Может быть, законодотворцы, распространяя режим государственной собственности на данные, тем самым пытались наделить государственные органы правомочиями по своему усмотрению совершать в отношении такой информации любые действия, предусмотренные пунктом 3 статьи 188 Гражданского кодекса - в том числе отчуждать информацию в собственность другим лицам, передавать им, оставаясь собственником, реализовывать правомочия по владению, пользованию и распоряжению информацией, отдавать информацию в залог и обременять ее другими способами, распоряжаться информацией иным образом? О поспешности и

... беспочвенности такой попытки свидетельствует, прежде всего, то

обстоятельство, что разработчики указанных новелл не учли норму п. 7 ст. 192 Гражданского кодекса и проигнорировали Закон РК «О государственном имуществе». Так, еще в 2011 году в связи с принятием в Казахстане Закона РК «О государственном имуществе» в статью 192 Гражданского кодекса, посвященную праву государственной собственности был внесен пункт 7, согласно которому «положения настоящей статьи применяются соответственно к иным, кроме права собственности, гражданским правам на государственное имущество, если иное не предусмотрено законодательным актом Республики Казахстан о государственном имуществе или не противоречит существу гражданских прав». Тем самым в дополнение к вещному праву государственной собственности было закреплено право государства на иные имущественные права, например, обязательственные, корпоративные права и так далее. При наличии данной нормы и в условиях невозможности распространения права собственности на неовещественное имущество, введение статьи 43-2 в АППК представляется по меньшей мере странным: если уж так хотелось владеть информацией достаточно было качественно законодательно проработать ее включение в виде отдельного объекта неимущественных прав государства с соответствующей регламентацией в Законе «О государственном имуществе».

Помимо описанных выше неудачных законодательных решений, в законодательстве об информатизации встречаются и другие, не согласующиеся с основополагающими правовыми установками положения. Так, Закон «Об информатизации», который регулирует общественные отношения в сфере информатизации между государственными органами, физическими и юридическими лицами при создании, развитии и эксплуатации объектов информатизации, а также при государственной поддержке развития отрасли информационно-коммуникационных технологий, содержит норму о том, что владельцем объектов информатизации является «субъект, которому собственник объектов информатизации предоставил права владения и пользования объектами информатизации в определенных законом или соглашением пределах и порядке». Под объектами информатизации указанный Закон понимает электронные информационные ресурсы[7], программное обеспечение[8], интернет-ресурс[9] и информационно-коммуникационную инфраструктуру[10]. В итоге, с учетом нормативно закрепленных дефиниций перечисленных здесь объектов, получается, что законодатель подчинил общему режиму разнопорядковые объекты: неовещественное имущество (информацию, которая входит в состав информационных ресурсов),

— овещественное имущество (материальные носители данных, сервера и

линии связи) и объекты исключительных прав (программное обеспечение; информация, составляющая объект права интеллектуальной собственности).

Думается, законодатель должен учитывать степень разработанности того или иного правового явления в отечественной гражданско-правовой доктрине, а не плодотворить революционные нормы в области вещных прав без какого-либо предварительного научного осмысления. Но к сожалению, наметилась прямо противоположная тенденция. Так, в развитие одиозных положений ст. 43-2 АППК об управлении данными в конце 2022 года был разработан законопроект «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам государственной статистики и управления данными», целями которого продекларированы повышение эффективности принятия решений в сферах государственного управления, развитие экономики и научно-аналитической деятельности на основе достоверных данных с широким использованием альтернативных источников.

Наиболее дискуссионной новеллой законопроекта является предложение о введении понятия «альтернативных данных», к которым относится любая информация, собранная и обработанная гражданами и юридическими лицами, в том числе персональные данные. Иными словами, статистическое ведомство планирует получить в свое распоряжение не только информацию, которую можно отнести к статистической, но и любую другую информацию. При этом такие «альтернативные данные» предполагается получать на безвозмездной основе и в соответствии с неким графиком (!).

Внедрение положений о возможности использования в целях статистики данных, не проверенных должным образом, а также внедрение дополнительной обязанности по предоставлению таких данных напрямую нарушает принцип государственной статистики: «использование всех видов источников информации с учетом качества, своевременности, затрат и нагрузки на респондентов» (пп. 5) ст. 5 Закона «О государственной статистике»), в то время как в ст. 14-3 Закона «О правовых актах» прямо указано, что «нормы законов не должны противоречить принципам, установленным в них, а в случае противоречия принципам должны приводиться в соответствие с ними».

В соответствии с Концепцией правовой политики Республики Казахстан до 2030 года [11], «С учетом международного опыта будет проработана необходимость кодификации законодательства в сфере информационно-коммуникационных технологий, связи, обработки данных, цифровых активов, автоматизации промышленности, информационной безопасности, 43

... машинного обучения и искусственного интеллекта, защиты прав субъектов персональных данных». Хотелось бы, чтобы намеченная проработка началась с теоретических исследований, а не с разработки очередного срочного законопроекта.

А между тем, в доктрине распространение на информацию вещных прав является весьма дискуссионным. Так, М.К. Сулейменов полагает, что бестелесное имущество, к которому относится информация, не может быть объектом права собственности: «право собственности – это вещное право. Нельзя его распространять на имущественные права. Это противоречит Гражданскому кодексу»[12].

В свое время еще Г.Ф. Шершеневич писал, что: «Распространять понятие о вещных правах на права, не имеющие своим объектом вещи, представляется теоретически неудобным. Порядок возникновения, перехода, прекращения вещных прав рассчитан именно на материальное их содержание, и потому распространение этих правил на совершенно иную область может создать нежелательное смешение понятий в теории и практике»[13].

Альтернативную точку зрения, которая представляется сегодня весьма перспективной, высказал профессор Ю.Г. Басин, полагавший, что «независимо от наших привычных представлений и привычной лексики, новые элементы фактически охватываются правом собственности в общих, пока еще спорных границах этого понятия. И в этих границах следует различать по специфике объектов, содержанию правомочий и способам их защиты от возможных и совершившихся нарушений несколько разновидностей права собственности»[14]. Автор предложил наряду с классическим правом овеществленной собственности разграничивать также право собственности на предметные символы вещей и благ; право собственности на зафиксированные надлежащим образом, без использования предметных носителей фиксации, оборотные активы; право интеллектуальной собственности на произведения творческой деятельности (с дальнейшим внутренним разделением). Соответствующее концептуальное предложение профессора Ю.Г. Басина требует своего развития, особенно, в части осмысления правовой природы прав на информацию. Но, к сожалению, в Казахстане такого рода комплексные исследования пока не проводились.

На постсоветском пространстве также пока нет какого-либо устоявшегося единого подхода к вопросу о распространении вещных прав на информацию. Так, например, И.Л. Бачило считает, что «Гражданско-правовую защиту документированной информации, представляющей собой одновременно нематериальный объект (информация) и овеществленный предмет

т... (собственно документ, содержащий информацию), можно осуществлять с помощью институтов интеллектуальной собственности и вещной собственности»[15]. Данную позицию поддерживает и С.В. Петровский, по мнению которого «Право собственности может быть установлено только на материальный носитель информации (бумажный, магнитный или иной) как на разновидность имущества»[16].

По мнению О.В. Гаврилова, «Термин «информационная собственность» в какой-то перспективе имеет право на жизнь. Но надо учитывать сложность аргументации. Дело в том, что в юридической науке есть понятие «юридической фикции» (например, интеллектуальная собственность есть юридическая фикция). Это конструкция, явно противоречащая действительности, но она полезна по ряду причин»[17].

А.Г. Карташян отмечает, что «В силу невозможности распространения вещных прав на саму информацию, информация в гражданском праве может быть объектом только обязательственных, исключительных либо корпоративных правоотношений»[18].

Т.З. Шалаева полагает, что «Для современного этапа развития права собственности наблюдается характерное расширение его предметной области – наряду с вещью появляется, к примеру, предприятие как имущественный комплекс. Режим права собственности под влиянием логики последовательной рецепции распространился на нематериальные объекты: имущественные права и нематериальные блага, нераскрытую информацию»[19]. С практической точки зрения, распространение на информацию режима вещных прав порождает также вопросы о реализации собственнических правомочий и их защите. Ясно ведь, например, что предъявить виндикационный иск в отношении похищенной информации не удастся. Как справедливо отметил Ю.Г. Басин в указанном выше исследовании, «Универсальным способом защиты прав хозяина во всех видах собственности служит признание за ним права хозяйской власти над объектом и возмещения убытков, причиненных собственнику неправомерным поведением третьих лиц. Другие способы зависят от характера нарушенных правомочий и действий нарушителя.

Различные виды права собственности объединены и такими признаками, как необходимость за свой счет поддерживать надлежащее состояние объекта, нести риск случайных убытков, вызванных уничтожением или повреждением объекта собственности либо причиненных в связи с такими объектами другим лицам. На собственника возлагаются все законные обременения объекта правами третьих лиц»[20].

В контексте поднятой тематики о правовом режиме информации обращает на себя особое внимание содержание Модельного информационного кодекса для государств - участников СНГ, принятого на тридцать восьмом пленарном заседании Межпарламентской Ассамблеи государств - участников СНГ (постановление № 38-6 от 23 ноября 2012 года)[21]. Так, Модельный кодекс не предусматривает права собственности на информацию и, тем более, не наделяет какими-либо собственническими полномочиями государство или государственные органы. При этом в Модельном кодексе регламентируются, в частности, отношения, связанные с созданием, распространением, использованием, хранением и уничтожением (утилизацией) информации. Подобный консервативный подход, заложенный в Модельном информационном кодексе, представляется гораздо более предпочтительным для удовлетворения текущих нужд правоприменительной практики в области оборота и защиты информации, нежели выстраивание новой теории вещных прав на фундаменте того сырого нормативного материала, который Республика Казахстан имеет сейчас.

[1] Указ Президента Республики Казахстан от 15 февраля 2018 года № 636 «Об утверждении Национального плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан»

[2] Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы»

[3] Указ Президента Республики Казахстан от 15 октября 2021 года № 674 «Об утверждении Концепции правовой политики Республики Казахстан до 2030 года»

[4] Закон РК 3 мая 2022 года № 118-VII ЗРК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам защиты прав ребенка, образования, информации и

[5] Комментарий к Гражданскому кодексу Республики Казахстан (Общая часть). Ответственные редакторы: Сулейменов М.К., Басин Ю.Г. // ИС «Параграф». URL: [https://online.zakon.kz/Document/?doc\\_id=1019750&sub\\_id=1880000&pos=2690;-54#pos=2690;-54](https://online.zakon.kz/Document/?doc_id=1019750&sub_id=1880000&pos=2690;-54#pos=2690;-54)

[6] Гражданский кодекс Республики Казахстан (Общая часть): Комментарий (постатейный). В четырех книгах. Книга 3. Статьи 188-258. Издание четвертое, исправленное и дополненное, с использованием судебной практики / Отв. ред. М.К. Сулейменов. – Алматы, 2022. – С. 17.

[7] Данные в электронно-цифровой форме, содержащиеся на электронном носителе и в объектах информатизации

[8] Совокупность программ, программных кодов, а также программных продуктов с технической документацией, необходимой для их эксплуатации

[9] Информация (в текстовом, графическом, аудиовизуальном или ином виде), размещенная на аппаратно-программном комплексе, имеющем уникальный сетевой адрес и (или) доменное имя и функционирующем в Интернете.

[10] Совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним

[11] Указ Президента Республики Казахстан от 15 октября 2021 года № 674

[12] «Гражданское законодательство Республики Казахстан: прошлое, настоящее, будущее» (М.К. Сулейменов, доктор юридических наук) <https://zangerlf.com/ru/publications/257>

[13] Шершеневич, Г.Ф. Учебник русского гражданского права: (По изд. 1907 г.) / Г.Ф Шершеневич; Вступ. ст. Суханова Е.А. – М.: СПАРК, 1995. – 556 с.

[14] Басин Ю.Г. К вопросу о понятии права собственности. Гражданское законодательство: Статьи. Комментарии. Практика. Вып. 17. – Алматы: ЮРИСТ, 2003. - С. 37-39.

— [15] Бачило И.Л. Информационное право: основы практической информатики. Учебное пособие. – М., 2003. – С. 241.

[16] Петровский С.В. О проекте Федерального Закона «Об информации, информатизации и защите информации» // Юрист. – 2005. – № 6. – С. 89.

[17] Гаврилов, О.В. Актуальные проблемы информационного права / О.В. Гаврилов // Материалы круглого стола / Труды по интеллектуальной собственности. – Москва.: ИМПЭ, 2000. – Т.2. – С.100

[18] Карташян А.Г. Гражданско-правовой режим коммерческой информации: Автореф. дисс. канд. юрид. наук. – М., 2007. С. 14.

[19] Шалаева Т.З. Право собственности и исключительные права на информационные ресурсы: проблемы двуединой природы // Репозиторий Брестского Государственного университета им. П.С.Пушкина. URL: <https://rep.brsu.by/bitstream/handle/123456789/3213>

[20] Басин Ю.Г. Указ.соч. - С. 38.

[21] ИС «Параграф». URL:

[https://online.zakon.kz/Document/?doc\\_id=31307564&pos=6;-106#pos=6;-106](https://online.zakon.kz/Document/?doc_id=31307564&pos=6;-106#pos=6;-106)

**№ 15. Уголовно-правовая охрана отношений, возникающих в связи с развитием финансово-цифровой среды.**

Общие замечания об объекте уголовно-правовой охраны в цифровую эпоху. Современный мир развивается очень динамично, каждые 5 лет изменяют

сложившийся уклад достаточно существенно, настолько, что это становится заметно практически невооруженным глазом. Причем меняется не только, что называется, оформление, «картинка», «обложка», меняется и, если можно так сказать, угол зрения, восприятие трансформаций, происходящих с социальной

реальностью. Если в середине прошлого века говорили об атомной промышленной революции, то на рубеже веков и в начале XXI века говорят уже об информационной, а теперь уже и о цифровой революции.

Информационные технологии, цифровые технологии, информационные ресурсы, цифровая реальность, виртуальная реальность, цифровая экономика и т.п. стали неотъемлемым

элементом современной жизни. По сути, человечество творит третью природу,

в дополнение к первой — собственно природе, и второй — культуре —

природу виртуальную. Причем это уже не фантастика и не плод воображения — футурологов, это вполне существующая реальность, с которой мы

и контактируем ежедневно, ежечасно и ежеминутно. С другой стороны, это

уже

и не просто оболочка, новая форма привычного содержания, это не замена рукописных книг печатными изданиями, например. Нет, если бы цифровая техника использовалась исключительно для набора, передачи и воспроизводства информации, то так бы и было, но уже даже на сегодняшний день совершенно другая ситуация.

Может показаться, что компьютерная техника лишь упрощает человеку выполнение его привычных задач, выступает всего лишь особым рода рабочим

288 Работа выполнена при финансовой поддержке РФФИ (научный проект № 20-011-00121

«Теория общего, особенного и единичного в уголовном праве России: методологические, технико-юридические и прикладные аспекты»).

220

инструментом, вроде других орудий труда. Но даже если не брать в расчет активные стремления и успехи ученых в части разработки систем искусственного

интеллекта — самообучающегося программного обеспечения, в целом, виртуальная, сетевая среда это уже не просто орудие труда, аналог телефонов и тому

подобное, а это действительно самостоятельная реальность. Социальные сети — Фейсбук, ВКонтакте, Одноклассники, Инстаграм и другие, — это уже определенное время не просто одно из средств связи, а некий самостоятельный

виртуальный мир, в котором люди проводят значительное количество времени,

решают деловые и личные вопросы, работают, отдыхают, смотрят видео и фото, добавляют свои, ничего подобного про телефонную связь сказать было нельзя. Более того, значительная часть профессиональных сообществ также переместилась в виртуальную среду, в ней заседают ученые, политики, торговцы,

менеджеры, верующие разных конфессий, государственные служащие и т.д.

Уже не один год существует особая виртуальная валюта — биткойны — не имеющая овеществленных аналогов и при этом активно занимающая

самостоятельное место среди прочих валют. И это если не учитывать, что большинство банковских операций перевелось в виртуальную форму, сейчас

— уже сложно себе представить торговую операцию, которая предусматривала

наличные деньги. Нельзя забывать и про целую «вселенную» видеоигр,

которые уже прочно превратились из локальных в сетевые. Часть этих игр, помимо

прочего, стала неотъемлемой частью самих социальных сетей. Причем даже жителю российской глубинки все перечисленное знакомо не понаслышке, он в этом активно участвует, практически живет.

Получается, что даже без учета искусственного интеллекта, виртуальный мир — это не просто набор инструментов — прикладных программ для работы

с информацией — а это именно отдельный мир, своего рода второе общество, социум, в котором люди вступают в общественные отношения через посредника — компьютерную технику (понимаем в предельно широком смысле и как

собственно компьютеры, и как разнообразные гаджеты), а иногда и в принципе

контактируют с техникой практически как с человеком. Человечество, отчасти

221

само того не понимая, шагнуло в новую эпоху, и переход этот сравним с переходом от присваивающей экономики к производящей (неолитическая революция) или с переходом от ручного труда к машинному (промышленная революция). Цифровая революция создала новый тип общественных отношений

и независимо от того, желаем ли мы признать этот факт или нет, мы вынуждены

с ним считаться, в особенности если учесть, что это уже не просто количественные изменения в социальной реальности, а ее новое качественное состояние.

При характеристике этих новых социальных отношений, впрочем, не обойтись без нескольких «допустим», дабы не упрощать, не огрублять проблему, поскольку это не прибавит возможностей для ее решения, а отвлечет

внимание от сущностных ее аспектов. Первое допущение касается того вопроса, что в современном мире немало обществ и территорий, где нет элементарного электричества, не то что Интернета или социальных сетей.

Логика ответа

на самом деле проста: тот факт, что до сих пор не все народы Земли обладают письменностью, и далеко не все жители владеют элементарной грамотностью,

не опровергает того факта, что современная культура, или культура модерна, — является культурой письменной. Это исключения, не влияющие на

и идентификацию мира постмодерна и теперь уже постпостмодерна как мира цифровой виртуальной реальности.

Второе допущение, по сути, связано с первым, и опирается на то, что новая цифровая реальность существует, только пока есть электроэнергия и Интернет,

отключи, условно говоря, рубильник, или отруби большой кабель — и нет никакой цифровой реальности. Однако как глобальная энергетическая система,

так и всемирная паутина уже развиты настолько, что готовы к какому-то рода перепадам и продуманы на сегодняшний день пути резервного электропитания,

а также пути резервного выхода в информационно-телекоммуникационные сети. Кроме того, наш мир без электричества уже сам по себе приобретет иное

качество, цифровая же реальность опирается на развитую энергосистему, массовую интернетизацию населения, а также на преимущественно городской характер современной культуры. Это своего рода следующий уровень развития

222

трех названных ранее возникших предпосылок — электрификации, интернетизации и урбанизации. Даже для городской части незападных культур характерны

те же самые закономерности развития виртуальной цифровой реальности — Китай, Индия, Япония, Россия и другие страны являют наглядные тому примеры.

Наконец, третье допущение сравнительного плана представляет вопрос: есть ли принципиальная разница между виртуальной цифровой реальностью и текстовой реальностью письменной культуры? Ведь автор письменного текста также, по сути, создает вымышленный мир, населяет его героями, они взаимодействуют и т.п. Касается это не только художественных, но и любых других

текстов, существуют даже особые концепции в рамках лингвистической философии, согласно которым текст, будучи создан, начинает жить самостоятельной

жизнью без оглядки на автора. Но в отличие от цифровой реальности, текст достаточно статичен, недаром ведь бытует поговорка «что написано пером, не вырубишь и топором». Безусловно, в зависимости от контекста один и тот же текст может быть прочитан по-разному, однако само содержание текста при

этом не меняется, а меняется лишь его интерпретация. Что касается

— виртуального цифрового мира, мира электронного, то он находится в

состоянии постоянной динамики, исходные программные коды и протоколы,

конечно, тоже

тексты, но они закладывают алгоритмы с множеством развития событий изначально и изначально полилогичны. Мы, конечно, можем представить диалог

автора и читателя посредством текста, но содержание письменного единой написанного текста остается неизменным, виртуальная же реальность качественно отличается от письменной текстовой реальности именно потому, что

она изначально изменчива и допускает различные варианты поведения субъектов. Ведь в отличие от текста цифровая реальность — это еще и среда взаимодействия ее участников, которые могут вести себя каким угодно образом. Поэтому при описании перехода от письменной культуры к культуре электронноцифровой мы должны учитывать, что произошло не просто количественное

увеличение объемов передаваемой информации, а качественно изменился характер взаимодействия в процессе обмена этой информацией.

223

Таким образом, можно сделать вывод, что новая цифровая реальность создала новый тип общественных отношений — отношения, осложненные виртуальным цифровым элементом. А появление нового типа общественных отношений не может не оказать влияние на объекты уголовно-правовой охраны. Аксиомой юридической науки является утверждение о том, что всякая самостоятельная отрасль права с собственным набором средств юридического опосредования объективной действительности имеет собственный предмет правового регулирования. Специфика уголовного права состоит в том, что в значительной

части предмет уголовного правового регулирования — это объект уголовноправовой охраны, который представляет собой те общественные отношения,

в защите которых социум заинтересован именно уголовно-правовыми средствами, в первую очередь путем установления уголовно-правового запрета общественно опасного поведения под угрозой применения наказания в случае его

нарушения, а во вторую очередь, если указанный запрет все же не сработал, то

в возложении на виновное лицо уголовной ответственности как с реальным применением уголовного наказания, так и без оно, но, например, с применением иных мер уголовно-правового характера. Есть еще и небольшой

сегмент

возникающих на основании преимущественно норм об обстоятельствах,

исключающих преступность деяния. Среди этих обстоятельств к сфере цифровой

реальности может иметь отношение, например, обоснованный риск. Однако преимущественно уголовное право в процессе регулятивного воздействия осуществляет уголовно-правовую охрану общественных отношений, и нормальным состоянием для общества можно считать, когда это право с охранительной

задачей справляется и запреты не нарушаются.

Появление особого рода общественных отношений не может не повлиять и на объект уголовно-правовой охраны: на сегодняшний день он должен отражать существование цифровой виртуальной реальности. Фатальная проблема,

правда, состоит в том, что отечественная уголовно-правовая наука на сегодняшний день не располагает адекватными методами познания этой реально-

224

сти, поскольку ее собственная догматическая методология соответствует, по меткому замечанию И.Л. Честнова, XVII–XVIII вв., когда ни о какой цифровой реальности речи не было. О чем говорим? Все дело в том, что основной метод уголовно-правового познания — юридико-догматический, причем опирается он на классические схемы, выработанные еще дореволюционной уголовноправовой теорией. Это изучение текстов уголовного закона, как будто это откровение Бога Яхве, данное Моисею на горе Синай на Скрижалях завета. Хотя

с позиций науковедения изучение текста уголовного закона вообще не имеет отношения к научному познанию, это обыкновенная догматика, которой вполне

успешно занимались средневековые пандектисты, глоссаторы и постглоссаторы, читая и комментируя свой *ratio scripta* — Дигесты Юстиниана. Может быть,

для своей эпохи это и было выдающимся достижением методологии правопознания, но на сегодняшний день осмысливать уголовно-правовую догматику

как научный метод познания несколько странно.

Социально-правовой, статистический, сравнительно-правовой методы также мало решают проблему, поскольку все они завязаны на догматике, отталкиваются от норм действующего уголовного-правового закона. В чем это реально

проявляется: мы определяем объект уголовно-правовой охраны, не исходя — из реально существующих общественных отношений, а исходя из текста

уголовного закона. что в нем зафиксировано, то и охраняем. Безусловно, для

... правоприменителя это необходимая и достаточная точка зрения (хотя тоже

далеко

не всегда), но ученый — не правоприменитель, он исследует реальность, а не текст. Реальность предполагает несколько иной алгоритм, который сначала

определяет познание групп общественных отношений, затем выделяет среди них те, что являются наиболее ценными, требующими уголовно-правовой охраны, далее выделяет среди них те, которые могут быть в силу своего содержания и природы быть подвергнутыми такой охране, а уже затем, отталкиваясь

от техники уголовного законодательства и системного характера уголовного права России, формулируются нормы-запреты.

225

При этом необходимо согласиться с А.Э. Жалинским и признать вторичный характер уголовно-правовых предписаний по отношению к регулятивному законодательству: уголовное право как максимум должно запрещать только то,

что уже подпадает под запрет в других отраслях права, но как минимум не должно запрещать то, что регулятивным законодательством прямо разрешено. В любом случае, прежде чем должен быть сформулирован и закреплен уголовно-правовой запрет, необходимо, чтобы регулятивное законодательство

в данной сфере было достаточно развитым и определяло в целом пределы юридического вмешательства в общественную жизнь. Исходя из специфики сферы

виртуальной цифровой реальности, мы вряд ли вообще можем говорить о формировании сколько-нибудь устойчивой для нее законодательной базы, но по меньшей мере должно быть осуществлено концептуальное осмысление этой

сферы в ее связи с правом, разработана и утверждена Концепция правового регулирования в цифровой сфере, а уже только потом в рамках этой концепции

определяются уголовно-правовые запреты.

Но это — в идеале. Правовая реальность, существующая на сегодняшний день, также требует к себе внимания и оценки, чем мы и займемся. Следует отметить, что отношения УК РФ и виртуальной цифровой реальности можно охарактеризовать как «сложные и напряженные». Дело в том, что уголовно-правовые запреты посягательств в этой сфере в действующем уголовном законе есть,

но они разрозненны, разбросаны по разным главам и даже разделам

— Уголовного

кодекса, зачастую носят несистемный характер, хотя по сути призваны охранять набор однородных объектов. Это говорит о том, что пока в уголовном законодательстве вопрос об уголовно-правовой охране отношений в цифровой сфере не получил концептуального закрепления и осмысления. Законодатель пытается решить сиюминутные проблемы, вводит новые статьи, модернизирует старые, но системного регулирования (охраны) не наблюдается. Некоторые аспекты объекта преступлений в сфере компьютерной информации. Первое, что бросается в глаза при юридико-догматическом анализе УК РФ на предмет регулирования цифровой сферы — это самостоятельная глава 28 «Преступления в сфере компьютерной информации», существующая в кодексе с момента его принятия и включающая на сегодняшний день целых четыре статьи. Остановимся пока на положениях этой главы. Прежде всего определим ее внутрисистемный статус в рамках отрасли уголовного права. Законодательно глава 28 включена в раздел IX «Преступления против общественной безопасности и общественного порядка», следовательно, структурно охраняемая данной главой сфера относится к сфере общественной безопасности и общественного порядка. Акцент делается на взаимосвязи защиты компьютерной информации от общественно опасных на нее посягательств в рамках охраны безопасного состояния общества в целом. Такой регламентацией уже изначально, при разработке и принятии Уголовного кодекса РФ, закладывалось понимание информатизации социума в современных условиях общественной жизни как неотъемлемой его части, не просто как тенденции, а как уже существующей реальности. Но такое внутрисистемное расположение видится адекватным только на первый взгляд. Общепринятой выступает точка зрения, что основанием разбивки статей Особенной части УК РФ на главы и разделы, т.е., по сути, главным принципом классификации преступлений выступает объект преступления. Причем структура отражает так называемую вертикальную классификацию объектов преступления, где общий объект охватывает все охраняемые уголовным законом ценности, блага, общественные отношения, родовой объект отражается в наименовании раздела Особенной части УК РФ, и представляет собой

объект преступления — это группа охраняемых уголовным законом

однородных общественных отношений, которые возникают по поводу близких по своему содержанию ценностей или благ. А.В. Наумов отмечает, что родовой (специальный) объект представляет собой группу однородных благ (интересов), на которые посягает однородная группа преступлений<sup>289</sup>. Н.И. Коржанский

289 См.: Наумов А.В. Российское уголовное право. Общая часть: курс лекций. 6-е изд., перераб. и доп. М.: Проспект, 2018. С. 344.

227

практически таким же образом определяет родовой объект как отдельную группу однородных общественных отношений, составляющих определенную область общественной жизни — собственность, личность и т.п.<sup>290</sup> Родовой объект применительно к преступлениям в сфере компьютерной информации, таким

образом, традиционно трактуют как общественную безопасность и общественный порядок в целом, в масштабах всего общества. Возникает вопрос, является

ли сфера компьютерной информации составной частью безопасности общества

в целом, либо каким-то ее элементом, и не выходит ли она за рамки данного родового объекта преступления. Полностью можно было бы прочесть наименование объекта данной главы так: Преступления в сфере компьютерной информации против общественной безопасности и общественного порядка.

Следующим уровнем объекта преступления выступает видовой объект, который в структуре Особенной части УК РФ соответствует главам.

«Видовой

объект является частью того или иного родового объекта, обособляя внутри него некоторую совокупность социальных ценностей (благ), обладающих общими

характеристиками»

291

. «Видовой объект преступления, являясь составной частью родового объекта и объединяя совокупность родственных и взаимосвязанных общественных отношений, положен в основу деления преступлений на главы Особенной части УК РФ»

292. Аналогичную трактовку видového объекта преступления можно встретить и в других источниках<sup>293</sup>. Из такой логики

исходят в литературе, определяя видовой объект преступлений в сфере компьютерной информации. «Видовым объектом данных преступлений

отношения по безопасному производству, хранению, использованию или распространению информации и информационных ресурсов либо их защиты.  
Ино-

290 См.: Энциклопедия уголовного права: в 35 т. Т. 4. Состав преступления. / отв. ред.

В.Б. Малинин. СПб.: Издание профессора Малинина, 2010. С. 135.

291 Российское уголовное право. Общая часть: учебник / под ред. Г.А.

Есакова. М.: Проспект,

2019. С. 73.

292 Уголовное право. Общая часть: учебник для вузов / под общ.ред. В.В.

Векленко. М.:

Юрайт, 2019. С. 115.

293 См. например: Уголовное право России. Общая часть: учебник / под ред.

В.В. Лукьянова,

В.С. Прохорова, В.Ф. Щепелькова. 3-е изд., испр. и доп. СПб.: Изд-во С.-

Петербур. ун-та, 2018.

С. 143.

228

гда коротко его еще определяют термином «информационная безопасность»

294

Причем, как видим, здесь родовой и видовой объекты искомой группы преступлений очень хорошо согласуются. Отталкиваясь от такого понимания видового объекта преступлений главы 28 УК РФ, можно было бы назвать ее «преступления против информационной безопасности», поскольку наименование

«преступления в сфере компьютерной информации» гораздо шире и охватывает, например, не только посягательство на информационную безопасность, но

и мошенничество в сфере компьютерной информации, присвоение авторства, некоторые виды подлогов и уголовно наказуемых подделок и др. Такое заужение видового объекта обусловлено, конечно, спецификой объекта родового,

но всех возможных посягательств в сфере компьютерной информации не охватывает.

Следует также отметить, что если проанализировать объективную составов, предусмотренных ст. 272-274.1 УК РФ, то они далеко не так гладко

корелируют с объектом «информационная безопасность». Если ст. 274.1, относительно недавно введенная в УК РФ, определенно предусматривает

— посягательство на информационную безопасность, то три традиционных  
состава этой главы, наряду с информационной безопасностью, могут иметь

~~... общественные отношения иного качества. Если проанализировать, например,~~  
стартовую статью  
данной главы — ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», то его объективная сторона включает в себя деяние, а также ряд его последствий. Само деяние — это непосредственно сам неправомерный доступ к компьютерной информации, содержание которого, а равно как иных признаков состава, дается на сегодняшний день в «Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», утвержденных Генеральной прокуратурой России. В этом документе, в частности, сказано, что неправомерный доступ к компьютерной информации — это незаконное либо

294 Российское уголовное право. Особенная часть: учебник для вузов / под ред. В.С. Комиссарова. СПб.: Питер, 2008. С. 532.

229 не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее). Доступ, как видим, может быть любым, главное — чтобы он был незаконным либо без разрешения собственника. Использование полученной таким образом информации может осуществляться и сугубо в личных целях, что не говорит о посягательстве на информационную безопасность, а затрагивает, скорее, какие-то конституционные права. Таким образом, точнее все-таки видовой объект главы 28 УК РФ определять как «отношения в сфере компьютерной информации, обеспечивающие законный порядок ее создания, модификации, манипуляции с ней и ее уничтожения». А в таком смысле он не вполне вписывается на сегодняшний день в объект родовой. Следует признать более правильной позицию авторов научного проекта Уголовного кодекса РФ под руководством Н.А. Лопашенко, которые для такого рода посягательств

—предусмотрели раздел, а не главу.—

Прежде чем перейти к анализу самого низкого с позиции уголовного закона уровня абстракции объекта преступления, представляется необходимым рассмотреть позицию В.Д. Филимонова относительно отношений, образующих объект преступления. Он выделяет два вида общественных отношений — охраняемое уголовным правом общественное отношение и охраняющее общественное отношение. «Охраняемое уголовным правом общественное отношение состоит в потребности конкретного человека жить, обладать здоровьем и телесной неприкосновенностью и соответствующей ей необходимости для других лиц воздерживаться от действий, способных причинить им вред. Юридическая форма этого общественного отношения состоит в праве каждого человека на жизнь, здоровье и телесную неприкосновенность и в правовой обязанности других лиц не совершать действий, направленных на причинение вреда этим 230 правоохраняемым объектам»

295. Охраняемое общественное отношение, таким образом, являет собой элемент социальной реальности, который берется под защиту уголовным правом и составляет сущность объекта его охраны. Но, как утверждает Вадим Донатович Филимонов, содержательно не исчерпывает и выделяет еще одно отношение в структуре объекта уголовно-правовой охраны.

«Охраняющее общественное отношение — отношение между государством и лицами, обязанными воздерживаться от указанных действий. Оно заключается в потребности государства обеспечить охрану жизни, здоровья и телесной неприкосновенности гражданина и в необходимости всех других членов общества воздерживаться от причинения им вреда. Правовое содержание этого общественного отношения составляют исходящий от государства запрет совершать действия, способные причинить вред жизни, здоровью и телесной неприкосновенности гражданина, и его право наказывать в соответствии с законом нарушителей этого запрета, а с другой стороны — обязанность остальных граждан соблюдать установленный государством запрет и в случае его нарушения подвергнуться предусмотренным законом мерам наказания»

296

Охраняющее общественное отношение, таким образом, вытекает из факта принятия и вступления в силу уголовно-правового запрета и обеспечивает своим

существованием защиту охраняемого общественного отношения. И то, и другое

отношение В.Д. Филимонов относит к объекту преступного деяния.

Интересен

нам и вывод ученого относительно того, что в конечном счете представляет собой объект уголовно-правовой охраны. «Сущностью объекта уголовно-правовой охраны (объекта преступления) является достигнутый на данном этапе развития общества уровень единства личных, общественных и государственных

интересов. Этот уровень единства интересов выражает ту меру социальной справедливости, которая нашла воплощение в охраняемых уголовным правом общественных отношениях»

297

.

295 Филимонов В.Д. Охранительная функция уголовного права. СПб.: Юридический центр

Пресс, 2003. С. 32.

296 Там же. С. 33.

297 Там же. С. 39.

231

Применим теперь предложенную В.Д. Филимоновым конструкцию объекта уголовно-правовой охраны к интересующим нас преступлениям в сфере компьютерной информации. Представляется, что вопрос с охраняющими отношениями решится довольно просто, когда будут введены соответствующие

уголовно-правовые запреты, он и на сегодняшний день может считаться решенным, поскольку четыре таких запрета в уголовном законе сформулированы

и производят на свет соответствующие охранительные уголовно-правовые отношения, которые защищают определенную область общественных отношений

в сфере компьютерной информации. Гораздо сложнее выступает проблема охраняемых отношений, поскольку они не обладают, в отличие от охраняющих,

нормативно-оценочной предзаданностью. Искусство и мудрость законодателя

— состоят в определении круга отношений, подлежащих уголовно-правовой

уголовноправовой охраны и предмета правового регулирования.

Классическое определение последнего дается С.С. Алексеевым: «Предмет правового регулирования — это разнообразные общественные отношения, которые объективно,

по своей природе могут «поддаваться» нормативно-организационному воздействию и в данных социально-политических условиях требуют такого воздействия, осуществляемого при помощи юридических норм, всех иных юридических средств, образующих механизм правового регулирования»

298. Специфика

уголовного права состоит в том, как указывает А.Э. Жалинский, что оно призвано охранять те общественные отношения, которые уже были урегулированы

иными отраслями права, «уголовная ответственность может наступить только в случае наличия в иных отраслях формально выраженного запрета»

299

При этом уголовное право не может запрещать то, что прямо разрешено в регулятивном отраслевом законодательстве, и в идеале должно запрещать то, что

уже запрещено в регулятивном законодательстве. А.Э. Жалинский указывает,

298 Алексеев С.С. Общая теория права: в 2 т. Т. I. М.: Юрид. лит., 1981. С. 292.

299 См: Уголовное право: учебник: в 3 т. Т. 1. Общая часть / под общ. ред. А.Э. Жалинского.

М.: Городец, 2011. С. 315.

232

что последнее правило предусмотрено и активно используется в немецком уголовном праве<sup>300</sup>. Таким образом, мы возвращаемся к одному из выдвинутых

первоначально тезисов: прежде чем определять круг уголовно-правовых запретов в цифровой сфере, необходимо создать нормативную основу функционирования этой сферы в регулятивных отраслях права.

Для уровня уголовного закона базовой ступенью абстракции в части объекта выступает так называемый непосредственный объект преступления или, иначе говоря, объект, выступающий составной частью отдельно взятого состава

преступления. Строго говоря, замечание Н.И. Коржанского о том, что объект в составе нельзя считать непосредственным в силу его абстрактности и

— ~~видового характера, он будет, скорее, выступать как раз видовым объектом, а~~

... вот объект отдельного преступления будет непосредственным, имеет под собой вполне

логичное основание. Традиционная, однако, для отечественной уголовно-правовой доктрины, позиция непосредственный объект соотносит с конструкцией состава преступления, регламентированного соответствующей статьей Особенной части УК РФ. Во избежание терминологической путаницы есть смысл ввести категорию единичного (отдельного) объекта преступления, тогда непосредственный объект займет определенное ему место в юридической конструкции состава преступления, а единичный объект будет представлен в составе реально совершенного единичного преступления.

Здесь уместны рассуждения В.Н. Винокурова о вертикальной классификации объектов преступления, опирающиеся на категории общего, особенного и единичного. «При классификации объектов преступлений по «вертикали» речь идет о классификации понятий «объект преступления». Классификация объектов преступлений по «вертикали» основывается на категориях «общее»

— все общественные отношения, охраняемые уголовным законом, — общий объект преступления; «особенное» — общественные отношения, охраняемые нормами главы УК РФ, — родовой объект преступления; «единичное» — общественные отношения, отражающие один и тот же интерес их участников; «от-

300 Жалинский А.Э. Современное немецкое уголовное право. М.: Проспект, 2006. С. 179–180.

233

дельное» — социальные связи между конкретными участниками отношений. Непосредственный объект преступления как «отдельное» — это не понятие, а явление, как социальная связь между обезличенными и не персонифицированными субъектами отношений, проявляющаяся в последствиях преступления — потерпевшем и предмете преступления. Непосредственный объект преступления — «отдельное» соотносится с общим объектом — «общее», родовым — «особенное» и видовым — «единичное» так же, как часть и целое»

301

Не вдаваясь в подробный разбор, анализ погрешностей, противоречий и неточностей, заключенных в этих рассуждениях, которые, по-видимому, — проистекают в отсутствие на сегодняшний день разработанной теории

автором схему

после того, как рассмотрим, что предлагается понимать под непосредственным

объектом преступлений в сфере компьютерной информации.

Непосредственный объект неправомерного доступа к компьютерной информации (ст. 272 УК РФ) определяют как «общественные отношения, обеспечивающие правомерный доступ, создание, обработку, преобразование и использование охраняемой законом компьютерной информации самим создателем, а также потребление ее иными пользователями»

302

. «Непосредственным

объектом данного преступления выступают общественные отношения, обеспечивающие безопасность процессов хранения, обработки, предоставления информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей»

303. Интересную трактовку дает Полный курс

уголовного права, правда, применительно к ранее действовавшей редакции анализируемой статьи, но не утратившую гносеологического значения:

«Непо-

301 Винокуров В.Н. Объект преступления: доктринально-прикладное исследование: монография. М.: Проспект, 2019. С. 111.

302 См.: Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т.

Т. 2 / под ред. А.В. Бриллиантова. 2-е изд. М.: Проспект, 2016. С. 325; также см.: Уголовное

право. Особенная часть: учебник для вузов / под общ. ред. Л.М.

Прозументова. Томск: Издво Том. ун-та, 2019. С. 574 и др.

303 Комментарий к Уголовному кодексу Российской Федерации /

Университет прокуратуры

Российской Федерации; под общ. ред. О.С. Капинус; научн. ред. В.В.

Меркурьев. М.: Проспект, 2018. С. 1086.

234

средственный объект преступления — общественные отношения, обеспечивающие безопасность компьютерной информации и нормальную эксплуатацию

ЭВМ, системы ЭВМ или их сети. Дополнительным объектом могут выступать

общественные отношения, охраняющие права собственности на

компьютерную

обратить внимание на то, что выделяются не только основной, но и дополнительный объект преступления, чем подчеркивается сложный характер объекта

преступления, предусмотренного ст. 272 УК РФ.

Учитывая, что непосредственный объект преступления представляет собой, согласно трактовке В.Н. Винокурова, не только понятие, т.е. идеальный объект, составной элемент духовной, идеологической сферы, но и явление, стоящее за этим понятием, объект онтологической реальности, необходимо обозначить его структурно-содержательную специфику применительно к преступлениям в сфере компьютерной информации вообще и к неправомерному доступу к компьютерной информации в частности.

Структуру объекта преступления,

согласно Н.И. Коржанскому, составляют элементы общественного отношения — участники (люди), предметы отношений (реальные материальные предметы, вещи), а также социальные связи между участниками по поводу предметов. «Содержание общественных отношений можно определить как социально

значимое поведение, которое включает все виды социального поведения: как активную человеческую деятельность, так и запрещаемое или требуемое обществом бездействие»

305. В указанную структурную схему вполне вписывается регламентация непосредственного объекта неправомерного доступа к компьютерной информации в действующей редакции ст. 272 УК РФ. Здесь компьютерная информация выступает предметом отношений, пользователи, администраторы компьютерных систем — участниками отношений, социальная связь между участниками по поводу предмета — содержанием отношений.

304 Полный курс уголовного права. Т. IV. Преступления против общественной безопасности /

под ред. А.И. Коробеева. СПб.: Юридический центр Пресс, 2008. С. 388.

305 См.: Энциклопедия уголовного права: в 35 т. Т. 4. Состав преступления / отв. ред.

В.Б. Малинин. 2-е изд. СПб.: СПб ГКА, Издание профессора Малинина, 2010. С. 98.

235

Однако если мы представим те же самые отношения с участием искусственного интеллекта, т.е. особым образом сформулированная компьютерная

— информация, которая обладает способностью к самовоспроизведению,

самобучению, самосовершенствованию, т.е., по сути, способна выступать **43**

~~... качестве если не полноценного, то хотя бы квазиучастника общественных~~

отношений. Это, в свою очередь, ставит вопрос о статусе такого рода квазиучастника

отношений. Но даже если мы поддадимся транслируемому Д.А.

Керимовым<sup>306</sup>

скептицизму относительно информационных отношений и искусственного интеллекта<sup>307</sup>, то в любом случае общественные отношения в сфере компьютерной информации в части программного обеспечения помимо пользователей

осложнены достаточно специфическими участниками — администратором или

системным администратором, который обслуживает программное обеспечение,

поддерживает его работоспособность, исправляет проблемы и ошибки, а также

разработчиком (разработчиками) программного обеспечения, формирующим исходный код исполняемых файлов. Особая роль этих участников состоит в том, что их действия или бездействие способны, прежде всего, породить проблемы, нестабильность в работе программного обеспечения, либо создать условия для того, чтобы это программное обеспечение дестабилизировалось, на первый взгляд, само по себе. Природа, характер и содержательные составляющие таких отношений на сегодняшний день не получили регулятивного

опосредования и остается неясным, какую роль с точки зрения социального и правового нормативного регулирования играют пользователь, администратор,

разработчик, в одном они статусе, или различных, с другой стороны, какова роль программного продукта, и как соотносятся между собой программный продукт и продукт программы.

Причем это только поверхностный взгляд на проблему, при более глубоком рассмотрении можно установить еще более сложный характер отношений

<sup>306</sup> Керимов Д.А. *Методология права: предмет, функции, проблемы философии права*. 6-е

изд. М.: Изд-во СГУ, 2011. С. 496.

<sup>307</sup> Скептицизм этот, стоит сказать, основан на сегодняшний день на достаточно существенно

устаревших публикациях, на которые ссылается Д.А. Керимов, и ни одна из которых не датируется даже 1990 годом.

236

— в сфере компьютерной информации. Это позволяет утверждать, что и объект

интерпретируется применительно к предусмотренным в главе 28 УК РФ составам преступлений. Следует отметить, что и в рамках других составов данной главы объект определяется аналогично ст. 272 УК РФ. Так, непосредственным объектом создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ) «выступают общественные отношения, обеспечивающие безопасность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей». В подобной трактовке объект преступления, предусмотренного ст. 273 УК РФ, на наш взгляд, не соответствует ни реальному явлению, страдающему от данного преступления, ни понятию о нем, а представляет собой предельно общую для такого уровня (уровня непосредственных объектов) конструкцию, подходящую для любого состава главы 28. Как видим, приверженность традиционного понимания содержания объекта преступления в данном случае не позволяет понять своеобразие непосредственного объекта отдельного преступления. Специфику же непосредственного объекта по анализируемой статье можно определить исходя из описанной в диспозиции ч. 1 ст. 273 УК РФ объективной стороны состава преступления: создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (вредоносных компьютерных программ). Учение об объекте и предмете преступления, выступающее доктринальным на уровне Общей части уголовного права, позволяет в качестве предмета данного преступления рассматривать вредоносную компьютерную программу (в предельно широком смысле), воздействуя на которую путем ее создания, распространения или использования, причиняется вред объекту преступления. «В ст. 273 УК РФ речь идет о компьютерной программе, обладающей вредо-

носными свойствами, то есть способной несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или

...нейтрализовать средства защиты компьютерной информации. Вредоносной программой следует считать представленную в объективной форме совокупность данных и команд, предназначенных для компьютера и других средств

вычислительной техники в целях получения определенного результата в виде уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации»

308

Исходя из сказанного, объектом преступления, предусмотренного ст. 273 УК РФ, отталкиваясь от соотношения категорий общего, особенного и единичного,

следует считать общественные отношения, обеспечивающие нормальное функционирование информационно-телекоммуникационных и других электронных

систем, защищающие их от создания, распространения или использования вредоносных компьютерных программ.

Можно провести подобный анализ всех составов преступлений против компьютерной информации, предусмотренных, а равно и не предусмотренных

главой 28 УК РФ, закрепленных в других главах и разделах УК РФ, таких как, например, ст. 146, 147, 159.6 УК РФ и др. Общим будет выступать определенное противоречие между традиционно трактуемым объектом преступления

и уголовно-правовой охраны и реальным объектом, отвечающим требованиям

соотношения категорий общего, особенного и единичного и при этом соответствующим характеру и содержанию объективной стороны и специфике предмета. Последнее обстоятельство применительно к существующим в УК РФ составам преступлений в сфере компьютерной информации, по большому счету, вынуждает игнорировать правила соотношения общего, особенного и единичного,

которые мы выше приводили, ссылаясь на работу В.Н. Винокурова. В этом смысле позиция авторского коллектива разработчиков научного проекта УК РФ

под руководством Н.А. Лопашенко, представляется более адекватной и логич-

308 Комментарий к Уголовному кодексу Российской Федерации /  
Университет прокуратуры

— Российской Федерации; под общ. ред. О.С. Капинус; научн. ред. В.В.

Меркуров. М.: Проспект, 2018. С. 1089.

ной, нежели позиция действующего уголовного закона, поскольку в названном проекте преступления против компьютерной информации посвящен самостоятельный раздел.

Некоторые выводы. Мы намеренно ограничились в данной части работы исключительно проблемами составов преступлений, предусмотренных главой 28 УК РФ, и не обращались к другим составам. Во втором блоке, посвященном предмету, подход предполагается более широким. В рамках же общего учения об объекте преступления в цифровую эпоху с позиций диалектики общего, особенного и единичного, данная глава уголовного закона является наиболее иллюстративной и репрезентативной. Во-первых, она целиком предназначена для охраны цифровых отношений, но, как видим, во многом ее положения этой задаче неадекватны, прежде всего, ввиду непроработанности регулятивной отраслевой базы в рамках позитивных отраслей права, и также в силу достаточной консервативности содержания данной главы. Во-вторых, на примере главы 28 наглядно можно увидеть, насколько уголовный закон стоит далеко от объективных законов и категорий диалектики, в частности, от соотношения категорий общего, особенного и единичного, поскольку определяемый объективной стороной предусмотренных в указанной главе составов преступлений вред непосредственному объекту, не укладывается ни в рамки видового, ни в рамки родового объекта, а имеет самостоятельную специфику. Эти обстоятельства подчеркивают необходимость социального и правового нормативного опосредования цифровой реальности, поскольку только в этом случае возможна соразмерная и эффективная ее уголовно-правовая охрана. Также следует констатировать, что на сегодняшний день уголовное право нуждается в стройной и адаптированной под его технико-юридическую и системно-структурную специфику теории общего, особенного и единичного. Структура Особенной части УК РФ, традиционно завязанная на оправдавшей себя вертикальной классификации объектов преступлений, подчиняется законам взаимодействия указанных категорий: единичное не может принципиально выходить за рамки особенного

понятийного описания. Игнорирование этих закономерностей существенно затрудняет правоприменение, и в частности, логичную и непротиворечивую аргументацию занятой стороной позиции по уголовному делу. С одной стороны,

бытует мнение, что Уголовный кодекс и здравый смысл не всегда идут в одном

направлении, и в случае их размолвки нужно руководствоваться первым из них,

*Ignoratio non est argumentum*. Однако в современных условиях все усложняющейся реальности и ее юридической регламентации, иногда все же незнание —

это довод, и юридическая, на первый взгляд, ошибка, становится релевантной и влияет на решение вопроса о вине, а следовательно, об ответственности<sup>309</sup>

В том виде, в котором сформулированы уголовно-правовые предписания, они адресованы правоприменителям, но стоящие за ними уголовно-правовые запреты обращены к обычным гражданам, не имеющим, как правило, юридической

подготовки, следовательно, с другой стороны, эти запреты должны быть при прочих равных понятны своим адресатам, то есть, наряду с законодательной техникой, выполнять и требования здравого смысла<sup>310</sup>. Тогда и стоящие перед

уголовным правом задачи окажутся в большей степени выполнимыми, а объект

уголовно-правовой охраны реже будет превращаться в объект преступления.

Б) Предмет преступления в цифровую эпоху

С объектом преступления тесно связан предмет преступления. Предмет преступления относится к числу наименее разработанных уголовно-правовых понятий. Это понятие прошло достаточно долгий путь своего становления и развития. С изменением общественной жизни оно наполнялось новым содержанием, от признания в начале предметом преступления исключительно материальных вещей в хищениях чужого имущества до распространения этого понятия на информацию, виртуальные предметы в эпоху современного цифрового

общества. Полагаем, что раскрыть природу, признаки и дать определение предмета преступления невозможно без исследования истории этого вопроса.

<sup>309</sup> См. примеры: Флетчер Дж., Наумов А.В. Основные концепции современного уголовного

— права. М.: Юристъ, 1998. С. 367–408.

310. См. подробнее: Куликов Е. А., Беденков В. В. Негативная юридическая ответственность

и обыденное правосознание: грани соприкосновения // Право и политика. 2016. № 11.

С. 1414–1422.

240

Эволюцию взглядов на предмет преступления в российском уголовном праве можно разделить на три периода: дореволюционный (со второй половины

XIX в. до 1917 г.), советский и постсоветский (с 1917 г. до конца 1990-х гг.) и современный период (с конца 1990-х гг. до настоящего времени). Данные временные интервалы выделены с учетом выводов М. П. Бикмурзина, но уточнены исходя из этапов периодизации развития российского уголовного законодательства<sup>311</sup>

Обобщение результатов исследований, посвященных предмету преступления, позволяет утверждать, что во второй половине XIX в. — начале XX в.

большинство ученых (А. А. Жижиленко, П. Д. Калмыков, А. Ф. Кистяковский, Г. Е. Колоколов, В. Д. Спасович, П. П. Пусторослев, И. Я. Фойницкий и другие) не разграничивали понятия «объект» и «предмет» преступления<sup>312</sup>. Термины «объект» или «предмет» применялись без какого-либо уточнения к различным

явлениям и использовались в качестве синонимов. К примеру, И. Я.

Фойницкий

в работе о мошенничестве, написанной в 1871 г., предмет преступления определял как «отношения, охранение которых важно для государства, как организма юридического», а предмет мошенничества конкретизировал как «чужие

имущественные права»

313. В то же время далее в работе он называл предметом

мошенничества конкретные виды имущества и документы, дающие право на имущество<sup>314</sup>

Вместе с тем в трудах Л. С. Белогриц-Котляревского, Л. Е. Владимирова, Н. С. Таганцева, Н. Д. Сергиевского можно увидеть предпосылки для разграни-

311 М. П. Бикмурзин выделил три периода: дореволюционный (со второй половины XIX в.

до 1917 г.), советский (с 1917 г. до начала 1990-х гг.) и постсоветский (с начала 1990-х гг.

теоретико-правовой

анализ. М.: Юрлитинформ, 2006. С. 13.

312 Там же. С. 13–14; Кузнецов И.В. Понятие и виды предметов преступлений в уголовном

праве России: автореф. дис. ...канд. юрид. наук. Челябинск, 2007. С. 13;

Карнаухов А. Эволюция взглядов на объект преступления в доктрине уголовного права // Современные тенденции развития науки и технологий: сб. науч. трудов: в 5 ч. Ч. 2. М., 2017. С. 116.

313 Фойницкий И.Я. Мошенничество по русскому праву. Сравнительное исследование: в II ч.

Ч. II. М.: Изд-во СГУ, 2006. С. 10.

314 Там же. С. 27 (разд. II гл. I «Виды имущества, могущие быть предметом мошенничества»).

241

чения объекта и предмета в их современном понимании<sup>315</sup>. В частности, Н.С. Таганцевым обращалось внимание на «непосредственный объект нападения», Н.Д. Сергиевским — на «непосредственный предмет посягательства».

Н.С. Таганцев, характеризуя право в субъективном смысле как объект преступления, отмечал, что оно представляет такое же отвлеченное понятие, как и норма, а потому само по себе не может быть непосредственным объектом преступного посягательства, пока оно не найдет выражения в конкретно существующем благе. Субъективное право делается доступным для нападения предметом

только тогда, когда оно воплотилось в сочинении, картине, доме, поместье и т.п. Только право реализованное может быть объектом нападения<sup>316</sup>.

Объект

нападения у Н.С. Таганцева можно интерпретировать как предмет преступления. Н.Д. Сергиевский поставил вопрос «как бы о двойном объекте преступных

деяний», который образуют, во-первых, ближайшим образом, непосредственный предмет посягательства, а затем, во-вторых, отвлеченный интерес всего

общества, нарушаемый неисполнением соответствующего предписания закона. Только соединение обоих моментов образует понятие объекта: нарушение

нормы закона невозможно без посягательства на конкретные блага или интересы<sup>317</sup>

. Еще более определенно об объекте и предмете преступления высказался

— Л.Е. Владимиров. Он писал, что «отвлеченным предметом», по его

... «объектом преступления», называется то, государством защищаемое условие общежития (благо, интерес), которое подвергается нарушению со стороны известного рода преступлений. Так, «отвлеченным объектом» всех преступлений против собственности будет основное положение, что собственность неприкосновенна. «Индивидуальное проявление законом огражденного условия обще-

315 См.: Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ. М.: Юрлитинформ, 2006. С. 14; Карнаухов А. Эволюция взглядов на объект преступления в доктрине уголовного права // Современные тенденции развития науки и технологий: сб. науч. трудов: в 5 ч. Ч. 2. М., 2017. С. 116–117.

316 Таганцев Н.С. Лекции по уголовному праву. Часть Общая. Выпуск 1. СПб.: Государственная типография, 1887. С. 39–40.

317 Цит. по: Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ. М.: Юрлитинформ, 2006. С. 15.

242

жития», нарушаемое данным преступлением, например, жизнь А., имущество В., Л.Е. Владимиров определил «конкретным предметом преступления»  
318

.  
Для развития представлений о предмете преступления особое значение имеют труды А.Н. Круглевского<sup>319</sup>. В работе «Имущественные преступления»

он посвятил отдельный параграф учению об объектах преступлений<sup>320</sup>. Исследователь, обобщив имеющиеся в литературе того времени подходы к выделению различных объектов («юридического», «фактического», «непосредственного», «конкретного» и других) обосновал необходимость четкого разделения

понятий «объект юридической охраны» и «объект действия». «Объект юридической охраны», по выводу А.Н. Круглевского, — это нарушаемое деликтом

право, именно этот объект вправе претендовать на значение объекта преступления

321

. «Объект действия» признан ученым самостоятельным элементом деликта. В работе резюмируется: «Объектом действия признается предмет, относительно которого учинено преступление, или который должен быть создан преступлением для того, чтобы возникло характерное для данного деликта — посягательство на объект юридической охраны; предмет фактического

... субъекта; непосредственная цель действий индивида». «... Объект действия

легко может быть смешан другими явлениями, входящими в состав последнего,

именно со средствами его реализации. ... Средством деликта являются предметы, причинные свойства которых обуславливают собой возникновение тех событий, которые входят в состав преступного действия. Объектом действия является предмет, на который происходит воздействие субъекта, не сопровождающееся возбуждением его причинных свойств, воздействие, имеющее значение

318 Владимиров Л.Е. Учебник русского уголовного права. Общая часть. Харьков: Изд. типографии Каплана и Бирюкова, 1889. С. 62.

319 См. также: Новоселов Г.П. Учение об объекте преступления. Методологические аспекты.

М.: НОРМА, 2001. С. 13; Бикмурзин М.П. Указ. раб. С. 15–16.

320 § 2 Введения «Учение об объектах преступлений». Круглевский А.Н.

Имущественные

преступления. Исследование основных типов имущественных преступлений.

СПб.: Типография С.-Петербургской Одиной тюрьмы, 1913. С. 10–31 //

Национальная электронная

библиотека. URL: [https://rusneb.ru/catalog/000199\\_000009\\_003804840/](https://rusneb.ru/catalog/000199_000009_003804840/)

321 Там же. С. 12–14.

243

в иных отношениях»

322. Таким образом, в современном звучании «объект охраны» у А.Н.

Круглевского — это объект преступления, «объект действия» —

предмет преступления, а характеристика предмета преступления, данная ученым, актуальна и сегодня. К сожалению, взгляды А.Н. Круглевского не были

восприняты советским научным сообществом и даже активно критиковались<sup>323</sup>

.

На советский период приходится наибольшее количество исследований в области предмета преступления. Интерес к предмету преступления был обусловлен признанием концепции общественных отношений как объекта преступления в качестве общепризнанной. Общественные отношения как объект

преступления получили нормативное закрепление в Руководящих началах по уголовному праву РСФСР<sup>324</sup>. В частности, в ст. 3 определялось, что уголовное право имеет «...задачей — посредством репрессий охранять

— систему общественных отношений, соответствующую интересам трудящихся

а. в. ст. 5 при характеристике признаков преступления прямо указывалось, что оно «... есть нарушение порядка общественных отношений, охраняемого уголовным правом». По свидетельству А.А. Герцензона, особенностью «Руководящих начал» являлось именно то, что «... характеризую признаки состава преступления, они останавливаются на объекте преступления»

325. Выработка единой позиции в отношении объекта преступления актуализировала вопрос о предмете преступления и его соотношении с объектом. Временные границы и высказанные подходы к пониманию предмета преступления позволяют выделить следующие этапы в развитии учения о предмете преступления в советском и постсоветском уголовном праве.

322 § 2 Введения «Учение об объектах преступлений». Круглевский А.Н. Имущественные

преступления. Исследование основных типов имущественных преступлений. СПб.: Типография С.-Петербургской Одиной тюрьмы, 1913. С. 12–13 // Национальная электронная

библиотека. URL: [https://rusneb.ru/catalog/000199\\_000009\\_003804840/](https://rusneb.ru/catalog/000199_000009_003804840/)

323 Курс советского уголовного права: в 6 т. Т. 2: Часть Общая. Преступление / А.А. Пионтковский; под ред. А.А. Пионтковского, П.С. Ромашкина, В.М. Чхиквадзе. М.: Наука, 1970.

С. 129.

324 Руководящие начала по уголовному праву РСФСР: постановление НКЮ РСФСР

от 12.12.1919 // КонсультантПлюс. URL:

<http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ESU&n=4859#009940039775167175>

325 Уголовное право. Общая часть / под ред. А.А. Герцензона, Б.С.

Ошеровича, А.А. Пионтковского. Изд. 2-е, перераб. и доп. М.: Юрид. изд-во НКЮ СССР, 1939. С. 101.

244

1. В период с 1917 г. до конца 40-х гг. специальные исследования о предмете преступления отсутствовали. Вместе с тем в 30–50-х гг. XX в. в учебной и научной литературе получила закрепление идея о разделении объекта и предмета преступления. По мнению Б.С. Никифорова, их разделение прежде всего

«... возникло на почве ... признания объектом преступления общественных отношений»

326. Так, А.В. Лаптев в работе, посвященной составу преступления,

— писал: «Следует различать объект преступления и предмет преступления.

Предметом преступления будут те конкретные вещи, на которые

---

направлено  
преступление»

327. И подводил итог, что «...в любом преступлении мы видим и непосредственный предмет посягательства, и объект преступления»  
328

В учебнике уголовного права, изданном в 1939 г., в параграфе «Понятие объекта преступления» лишь отмечалось, что «...от объекта преступления необходимо отличать непосредственный предмет посягательства, в связи с которым совершается то или иное преступление. Например, ...объектом фальшивомонетничества ...является денежная и кредитная система, предметом же фальшивомонетничества являются советские денежные знаки, иностранная валюта и государственные ценные бумаги»

329. В учебнике, опубликованном в 1947 г., предмет преступления определялся практически аналогично. Подчеркивалось

то, что «...наряду с понятием объекта преступления как общественного отношения необходимо выделить и предмет преступления, в котором этот объект

находит свое конкретное и непосредственное выражение». «Предмет преступления — характеризует конкретный предмет или интерес, на который посягает

преступник (например, кошелек с деньгами, портфель с официальными документами, здание элеватора, пути сообщения и т. д.)»

330. Кроме того, в этом из-

326 Никифоров Б.С. Объект преступления по советскому уголовному праву. М.: Гос. изд-во

юрид. лит., 1960. С. 128.

327 Лаптев А.В. Состав преступления и квалификация уголовных дел / под ред. И.Т. Голякова. М.: Юрид. изд-во НКЮ СССР, 1939. С. 6.

328 Там же. С. 7.

329 Уголовное право. Общая часть / под ред. А.А. Герцензона, Б.С. Ошеровича, А.А. Пионтковского. С. 167–168 (автор параграфа В.Д. Меньшагин).

330 Уголовное право: учебник / под общ. ред. И.Т. Голякова. изд. 2-е, доп. М.: Юрид. изд-во

МЮ СССР, 1947. С. 67–68 (автор параграфа В.Д. Меньшагин).

---

245

дании предмет преступления был отнесен к разновидности объекта

преступления. Схематически виды объектов были изображены так: общий, специальный, непосредственный объекты и предмет преступления<sup>331</sup>

2. Период 50–80-х гг. XX в. отличает активное научное обсуждение проблемы «предмета преступления». В литературе, посвященной преимущественно объекту преступления, дискутируются вопросы о понятии, значении, видах предмета преступления, о его связи с объектом и месте в составе преступления.

По характеристике Б.С. Никифорова, в этот период «...возникли различные теории предмета преступления, деление преступлений на предметные и беспредметные, более или менее пространные перечни различных предметов преступлений, попытки установить соотношение предметов с объектами и т.д. Эти

попытки в свою очередь привели к построению различных определений предмета»

332. В.Я. Тацкий свел все высказанные взгляды на предмет преступления к двум позициям. «Первая предполагает рассмотрение предмета как правового

феномена, не находящегося с объектом преступления в органической связи.

В основе второй, напротив, лежат выводы о тождественности этих понятий и нецелесообразности самой разработки проблемы предмета преступления»<sup>333</sup>

С учетом природы предмета преступления в это время были обоснованы такие

значимые концепции: узкого понимания предмета, исключительно как материального феномена (вещи), и его широкой трактовки, признающей предметом

преступления и нематериальные (идеальные) явления. Однако в целях обобщения всех представлений о предмете преступления и их научного анализа более

удачным видится деление, предложенное М.П. Бикмурзиным. В зависимости от места, отводимого предмету в составе преступления, он обозначил два основных направления в исследовании этого признака: первое — признает пред-

331 Уголовное право: учебник / под общ. ред. И.Т. Голякова. изд. 2-е, доп. М.: Юрид. изд-во

— МЮ СССР, 1947. С. 68 (автор параграфа В.Д. Меньшагин).

332. Никифоров Б.С. Объект преступления по советскому уголовному праву.

М.: Гос. изд-во

юрид. лит., 1960. С. 128.

333 Таций В.Я. Предмет преступления // Правоведение. 1984. № 4. С. 52; См. также: Таций В.Я. Объект и предмет преступления в советском уголовном праве. Харьков: Выща шк.,

Изд-во при Харьков. гос. ун-те, 1988. С. 33.

246

мет признаком состава преступления, характеризующим объективную сторону

и независимым от объекта; второе — включает предмет в объект преступления,

как неразрывно связанный с последним<sup>334</sup>

Сторонниками первого направления, в частности, были А.А. Пионтковский, А.Н. Трайнин и Б.А. Куринов<sup>335</sup>. Их объединяло также то, что предмет преступления они определяли как вещь. При этом А.А. Пионтковский акцентировал внимание на том, что предмет преступления в отличие от непосредственного объекта необходимо выделять не во всех составах преступлений. «О предмете как элементе состава преступления в отличие от объекта преступления

можно и должно говорить лишь тогда, когда в отличие от объекта преступления

на него (предмет) не происходит посягательства». К примеру, предмет наличествует в составе взяточничества — это определенные материальные ценности,

в составе контрабанды — товарно-материальные ценности, незаконно перевозимые через границу. «При таком понимании предмета преступления он не относится к объекту, а принадлежит объективной стороне состава этих преступлений»

336. А.Н. Трайнин занимал схожую позицию. По его мнению, предмет преступления — это «...те вещи, в связи с которыми или по поводу которых совершается преступление»

337. Предмет ограничивается от объекта по тому

признаку, что объект терпит или может потерпеть ущерб от преступления, тогда как с предметом этого не происходит. Соответственно, объектом состава

взяточничества он называл «закономерную деятельность должностных лиц», предметом — «деньги или иное имущество»; объектом изготовления одурманивающих веществ — «здоровье граждан», предметом —

— одурманивающие

Предме-

334 Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ: автореф. дис. ...

канд. юрид. наук. Саратов, 2005. С. 13; Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ. М., 2006. С. 18.

335 Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ: автореф. дис. ...

канд. юрид. наук. Саратов, 2005. С. 13.

336 Курс советского уголовного права: в 6 т. Т. 2: Часть Общая.

Преступление. С. 119.

337 Трайнин А.Н. Общее учение о составе преступления. М.: Гос. изд-во юрид. лит., 1957.

С. 178–179.

338 Там же.

247

том посягательства он называл «... конкретные предметы материального мира (вещи, деньги, домашние животные, средства транспорта и т.д.), на которые направлено определенное общественно-опасное действие (бездействие) преступника»

339. Отрицательное изменение физических свойств и качеств предмета преступления является способом воздействия на непосредственный объект преступления. По его убеждению, «... такого рода трактовка понятия и правового

значения предмета преступления обуславливает необходимость рассмотрения этого элемента преступления в группе признаков состава, характеризующих объективную сторону преступления»

340

Взгляды на предмет преступления как признак объекта среди представителей второго направления его исследования крайне неоднородны. В рамках этого направления можно выделить несколько заслуживающих внимания позиций. Во-первых, в более ранних работах предметом предлагалось считать любой из элементов структуры общественного отношения как объекта преступления (материальные вещи, субъектов, их деятельность) (Н.А. Беляев, П.Н. Панченко, А.А. Герцензон, Г.А. Кригер)<sup>341</sup>. Так, Н.А. Беляев писал, что «... существование общественного отношения невозможно без его составных частей (элементов)». Элементами общественного отношения являются «... субъекты отношений, их деятельность, материальные вещи. Они и

— выступают в качестве предмета посягательства»

Выводы вышеуказанных ученых убедительно критиковались в научной литературе. В.Я. Тацкий верно отмечал, что в такой юридической конструкции произошла подмена объекта преступления его предметом. «При таком решении

339 Куринов Б.А. Научные основы квалификации преступлений. М.: Изд-во Моск. ун-та, 1984. С. 64.

340 Там же. С. 65.

341 См. Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ: автореф. дис. ...

канд. юрид. наук. Саратов, 2005. С. 13; Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ. М., 2006. С. 20–22.

342 Курс советского уголовного права: в 5 т. Часть Общая. Т. 1 / отв. ред. Н.А. Беляев,

М.Д. Шаргородский. Л.: Изд-во Ленингр. ун-та, 1968. С. 303–304 (автор параграфа Н.А. Беляев).

248

вопроса практически игнорируется служебная роль предмета как особого, в определенной мере самостоятельного признака преступления»

343

.

Во-вторых, в связи с изложенным выше выделим в качестве самостоятельной позицию Б.С. Никифорова. Ученый также выступил с критикой понимания предмета преступления как элементов общественного отношения и сделал кардинальный вывод о нецелесообразности выделения этого признака, поскольку

предмет — это всего лишь составная часть общественного отношения<sup>344</sup>. Он подчеркивал, что «...при более глубоком исследовании объекта именно как общественного отношения проблема предмета преступления ... по существу снимается, потому что устраняется необходимость в самостоятельном исследовании предмета преступления как явления, лежащего за пределами объекта

и ведущего самостоятельное по отношению к нему существование»

345

.

В-третьих, Н.И. Коржанским была высказана точка зрения о включении в предмет преступления двух элементов структуры общественного отношения:

— объекта и субъекта. «Предметом преступления следует признать

... объект, в котором проявляются общественные отношения и, воздействуя на который, субъект изменяет их. ...Под материальным объектом в данном определении понимаются как объект, так и субъект. ...Это обстоятельство необходимо учитывать потому, что общественные отношения могут быть нарушены воздействием как на материальный объект, так и на субъект отношения, то есть путем воздействия на любую сторону общественного отношения», — доказывал автор<sup>346</sup>

В рамках четвертого подхода объем понятия «предмет преступления» суживался до предмета (объекта) общественного отношения (В.К. Глистин, С.Ф. Кравцов, Е.В. Благов). В частности, С.Ф. Кравцов в диссертационном ис-

343 Таций В.Я. Предмет преступления // Правоведение. 1984. № 4. С. 53;  
Таций В.Я. Объект

и предмет преступления в советском уголовном праве. Харьков: Выща шк.,  
Изд-во при  
Харьков. гос. ун-те, 1988. С. 35.

344 Никифоров Б.С. Объект преступления по советскому уголовному праву.  
М.: Гос. изд-во  
юрид. лит., 1960. С. 129–133.

345 Там же. С. 130.

346 Коржанский Н.И. Объект и предмет уголовно-правовой охраны. М.: Изд-  
во Академии  
МВД СССР, 1980. С. 99.

249

следовании, посвященном предмету преступления, высказал веские доводы против включения в объем понятия «предмет преступления» субъекта общественного отношения, подчеркнув, что в таком представлении предмет поглощает принятый в уголовном и уголовно-процессуальном законодательстве термин «потерпевший», который означает субъекта отношения, подвергнувшегося посягательству<sup>347</sup>. Сам автор предмет преступления определял как «...материальный (вещественный) элемент общественного отношения, прямо указанный или подразумеваемый в уголовном законе, путем противоправного воздействия на который нарушается общественное отношение, то есть совершается посягательство на объект преступления». Характеризуя объем раскрываемого понятия, С.Ф. Кравцов отмечал, что материальность является — одной

... из главных черт предмета преступления. «Лишь вещи, имущество,

природные

богатства и другие материальные образования объективного мира» правильно именовать предметом преступления<sup>348</sup>

. Точку зрения, близкую к изложенной

выше, отстаивал В.К. Глистин, уточняя то, что в роли предмета преступления могут выступать материальные и нематериальные явления. Он полагал, что «... применительно к нуждам уголовного права все то, по поводу чего или в связи с чем существуют отношения, целесообразно называть предметом отношения, в отличие от объекта, которым обозначают само общественное отношение

как целостную систему». Так, «... в одних отношениях структурным элементом

являются вещи (тела, физические предметы, а точнее, их социальные свойства),

а в других — социальные или духовные блага, ценности»

349

.

Пятая позиция была разработана Е.А. Фроловым. Одной из задач диссертационного исследования объекта уголовно-правовой охраны он считал уточнение понятия предмета преступления и его значения.

Основываясь на предшествующем подходе, автор обосновал, что предмет преступления по своему содержанию уже объекта общественного отношения.

«К числу явлений, состав-

347 Кравцов С.Ф. Предмет преступления: автореф. дис. ... канд. юрид. наук. Л., 1976. С. 6–7.

348 Там же. С. 8–9.

349 Глистин В.К. Проблема уголовно-правовой охраны общественных отношений (объект и квалификация преступлений). Л.: Изд-во ЛГУ, 1979. С. 47–48.

250

ляющих понятие предмета преступления, следует относить только такие предметы или вещи, которые имеют материализованную оболочку и являются доступными для восприятия извне, доступными для измерения и фиксации»

350

.

Ученый пояснял, что воздействие на такие предметы оставляет внешние, объективные следы, поддающиеся фиксации, поэтому является

— свидетельством изменения общественного отношения. Это обстоятельство

... учитывает законодатель, закрепляя в норме права признаки предмета. В силу этого материальное образование (вещи, деньги, документы и т. п.), подвергающееся воздействию со стороны преступника, приобретает юридическое значение и становится тем, что принято именовать «предметом преступления». Таким образом, предмет преступления Е.А. Фролов определял как «...предметы (тела), которые служат материальным (вещественным) поводом, условием или свидетельством существования определенных общественных отношений и посредством изъятия, уничтожения либо видоизменения которых причиняется ущерб объекту уголовно-правовой охраны»

351. Заметим, что ранее подобные выводы о понятии предмета преступления и его соотношении с объектом общественных отношений были высказаны М.А. Гельфером<sup>352</sup>. Разницу между понятиями «объект отношения» и «предмет преступления» также видел Е.К. Каиржанов, но «в качественном отношении»: предмет преступления — более важный, ценный интерес, понимаемый как в виде материальной, так и идеальной социальной ценности<sup>353</sup>

В-шестых, значимой для учения о предмете преступления является концепция В.Я. Тацця. Размышляя над вопросом о том, что если предмет преступления представляет собой лишь определенную часть объекта, то вправе ли мы придавать ему свойства самостоятельного признака, автор пришел к выводу

350 Фролов Е.А. Объект уголовноправовой охраны и его роль в организации борьбы с посягательствами на социалистическую собственность: автореф. дис. ... д-ра юрид. наук. Свердловск, 1971. С. 28.

351 Там же. С. 28–29.

352 Гельфер М.А. Объект преступления. М., 1960. С. 16.

353 Каиржанов Е.К. Основные теоретические проблемы объекта уголовно-правовой охраны в СССР: автореф. дис. ... д-ра юрид. наук. Киев, 1975. С. 24.

251

о необходимости разграничения понятий «предмет общественного отношения»,

«предмет преступления» и «предмет преступного воздействия». В состав ~~любого общественного отношения~~ входит предмет общественного отношения

354

Предметом преступления, по выводу В.Я. Тация, следует считать «..любые вещи материального мира, с определенными свойствами которых закон связывает наличие в действиях лица признаков состава преступления». Предмет — это факультативный признак, относящийся к объекту преступления. Предмет преступления в отдельных случаях может совпадать с предметом общественного отношения, но может включать и те вещи, которые не входят в состав охраняемого общественного отношения, поскольку обладают вредными свойствами<sup>355</sup>

Предмет преступного воздействия необходимо понимать как «...элемент охраняемого уголовным законом общественного отношения, который подвергается непосредственному преступному воздействию», которому в первую очередь причиняется вред: субъекту, социальной связи или предмету общественного отношения. Выделение этого понятия значимо для выявления механизма причинения вреда объекту<sup>356</sup>. Таким образом, В.Я. Таций обосновал широкую концепцию понимания предмета преступления, учитывающую особенности конструирования законодателем составов конкретных преступлений. Именно необходимость придания правовой значимости в составе преступления определенной вещи, ее ценным или антиценным качествам обуславливает понимание и признание предмета преступления в качестве самостоятельного признака. 3. В постсоветский период (с начала 1990-х гг.) монографических исследований именно предмета преступления не проводилось. Предмет преступления фрагментарно рассматривался в работах, посвященных иным признакам состава-

354 Таций В.Я. Предмет преступления // Правоведение. 1984. № 4. С. 54–55; Таций В.Я. Объект и предмет преступления в советском уголовном праве. Харьков: Выща шк., Изд-во при Харьков. гос. ун-те, 1988. С. 41–47.

355 Таций В.Я. Предмет преступления. С. 55–57; Таций В.Я. Объект и предмет преступления

— в советском уголовном праве. С. 47–57.

356. Тацкий В.Я. Предмет преступления. С. 57; Тацкий В.Я. Объект и предмет преступления

в советском уголовном праве. С. 57–58.

252

ва преступления (объекту, преступному вреду) и конкретным составам преступлений. Однако анализ учебной литературы этого времени позволяет сделать вывод о том, что в уголовном праве стала доминировать концепция понимания предмета как материальной вещи и факультативного признака состава

преступления, относящегося к элементу (подсистеме) объекта преступления. Вместе с тем в числе дискуссионных остались вопросы о соотношении предмета преступления с предметом (объектом) общественного отношения и об объеме понятия «предмет преступления». В ряде учебников подчеркивалась исключительно материальная природа этого признака, без уточнения его

соотношения с предметом (объектом) общественного отношения<sup>357</sup>. В других — акцентировалось внимание на двух равнозначных свойствах предмета

преступления: во-первых, на его материализованной оболочке, доступности для

восприятия извне, для измерения и фиксации; и, во-вторых, на признании предмета преступления необходимой составной частью общественного отношения<sup>358</sup>. Некоторые авторы доказывали неразрывную связь предмета преступления с предметом общественного отношения на конкретных примерах, отмечая, например, тот факт, что при хищении деньги выступают в качестве предмета преступления, а при даче взятки они являются средством совершения преступления, поскольку не могут быть включены в структуру общественного отношения, выступающего объектом взяточничества<sup>359</sup>. И, наконец, отдельные

учебные издания определяли предмет преступления достаточно широко, как «материальную вещь объективно существующего мира, в связи или по поводу

которой совершается преступление», относя к числу предметов в том числе и вещи, изъятые из оборота, не входящие в охраняемые уголовным законом общественные отношения, им «чуждые»

360

.

357 Наумов А.В. Российское уголовное право. Общая часть. Курс лекций. М.: Изд-во БЕК, 1996. С. 153–154.

Ткачевского, Г.Н. Борзенкова. М.: Изд-во Моск. ун-та, 1993. С. 110–111 (автор параграфа И.М. Тяжкова).

359 Уголовное право России. Общая часть / под ред. В.П. Малкова, Ф.Р. Сундурова. Казань:

Изд-во Казанск. ун-та, 1994. С. 113 (автор параграфа Ф.Р. Сундуров).

360 Уголовное право России. Общая часть: учебник / отв. ред. Б.В.

Здравомыслов. М.: Юрист,

1996. С. 122–123 (автор параграфа В.Е. Мельникова).

253

В современный период, условной границей которого можно считать принятие и вступление в силу УК РФ361

, интерес к предмету преступления вновь

возрос. Предмет преступления получил разработку в качестве самостоятельной

научной проблемы в кандидатских диссертациях (М.П. Бикмурзина, И.В.

Кузнецова); а так же как и ранее, в работах, посвященных объекту (Г.П.

Новоселова, В.Д. Филимонова, В.Н. Винокурова, В.В. Мальцева); в

специальных исследованиях по Особенной части уголовного права,

конкретизирующих понятие

предмета преступления применительно к видам и отдельным составам

преступлений (А.Г. Безверхова, Л.А. Букалеровой, К.К. Грошикова, О.Е.

Спиридоновой, А.В. Суслопарова, В.В. Хилюты, А.В. Шульги и других); и в

многочисленных научных статьях. Общей характеристикой этого периода

следует признать то, что учение о предмете преступления получило развитие

с учетом реалий современного российского общества и обновленного

уголовного законодательства.

Сегодня в доктрине уголовного права при разработке понятия «предмет преступления» прослеживаются различные тенденции.

Во-первых, традиционное, сложившееся в советский период, определение предмета преступления как вещи материального мира, переосмысливается

учеными, поскольку оно не отвечает требованиям новейшего цифрового

(информационного) общества. По свидетельству А.В. Шульги, «...начало

нового тысячелетия специалисты в области философии, информатики,

политологии, социологии, экономики, юриспруденции и других наук

характеризуют как переход к информационному обществу, обладающему новой структурой, в которой

решающую роль играют отрасли, связанные с получением, распространением

и обработкой информации. Происходит процесс формирования общества

ново-

КонсультантПлюс. URL: <http://www.consultant.ru>

254

го типа — информационного»

362. Основу информационного общества составляет информация, орудием труда выступают информационные технологии<sup>363</sup>

Становление и развитие такого общества требует новых задач от государства, в их числе — обеспечение информационной безопасности средствами уголовного права. Законодатель включил в УК РФ составы преступлений, охраняющие общественные отношения в сфере различных видов информации.

Одним из признаков данных преступлений выступает та или иная информация:

«сведения о частной жизни лица, составляющие его личную или семейную тайну» (ст. 137), «тайна усыновления (удочерения)» (ст. 155), «сведения, составляющие коммерческую, налоговую или банковскую тайну» (ст. 183), «информация о событиях, фактах или явлениях, создающих опасность для жизни или

здоровья людей либо окружающей среды» (ст. 237), «компьютерная информация» (ст. 272, 273, 274), «сведения, составляющие государственную тайну»

(ст. 275, 276, 283 УК РФ) и другая. По подсчетам М.П. Бикмурзина, Особенная

часть УК РФ в редакции 2006 г. содержала 20 статей, в которые было включено

прямое указание на информацию, и 18 статей, признающих уголовно наказуемым изменение или уничтожение информации, содержащейся на каком-либо

материальном носителе<sup>364</sup>. К.К. Groшиков выделил 32 нормы Особенной части

УК РФ, охраняющие общественные отношения, связанные с оборотом информации (сведений, сообщений, тайны, заявлений)<sup>365</sup>. При этом

наблюдается тенденция к расширению перечня преступлений, признаком которых является информация. Так, в 2012–2017 гг. УК РФ был дополнен ст. 205.6, 274.1, 280.1,

283.1 и другими, в которых информация имеет кримиобразующее значение.

362 Шульга А.В. Объект и предмет преступлений против собственности в условиях рыночных

— отношений и информационного общества: автореф. дис. ... д-ра юрид. наук.

363 Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография.

М.: Юрлитинформ, 2018. С. 3.

364 Бикмурзин М. П. Предмет преступления: теоретико-правовой анализ: автореф. дис. ...

канд. юрид. наук.С. 17; Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ, 2006. С. 51.

365 Грошиков К.К. Социально значимая информация и ее уголовно-правовая охрана: монография. М.: Юрлитинформ, 2011. С. 17.

255

Информация представляет собой «явление жизни и человека, и общества, важнейший фактор их существования»

366. Как признак состава преступления

информация — это «...сведения (сообщения, данные) независимо от формы их

представления»

367. А.А. Фатьянов характеризует информацию как воспринимаемую живым организмом через органы чувств окружающую действительность

в виде распределения материи и энергии во времени и в пространстве, подчеркивает то, что она не материальна, хотя ее носителем является материя<sup>368</sup>

.

А.А. Стрельцов уточняет, что формами существования информации являются сведения и сообщения. При этом сведения представляют собой результат отражения окружающей действительности в организме, сообщение — набор знаков,

с помощью которых сведения, накопленные одним организмом, могут быть переданы другому организму и восприняты им, а понятие «данные» выступает

как разновидность сообщений, предназначенных для автоматизированной обработки с использованием средств вычислительной техники<sup>369</sup>. Сведения

—

нематериальны, сообщения обладают лишь свойством материальности, определяемым как их «способность воздействовать на органы чувств»

370

.

Информация как признак состава различных преступлений большинством ученых, исследующих вопросы Особенной части уголовного права,

признается

... именно предметом преступления<sup>371</sup>. В связи с этим М.П. Бикмурзин,  
разраба-

366 Организационно-правовое обеспечение информационной безопасности:  
учеб. пособие

для студ. высш. учеб. заведений / А.А. Стрельцов и др.; под ред. А.А.  
Стрельцова. М.: Академия, 2008. С. 18.

367 Об информации, информационных технологиях и о защите информации:  
Федеральный

закон от 27.07.2006 № 149-ФЗ (ст. 5) // КонсультантПлюс. URL:  
<http://www.consultant.ru>

368 Фатьянов А.А. Правовое обеспечение безопасности информации в  
Российской Федерации: учеб. пособие. М.: Юрист, 2001. С. 10–11.

369 Организационно-правовое обеспечение информационной безопасности:  
учеб. пособие для

студ. высш. учеб. заведений / А.А. Стрельцов и др.; под ред. А.А. Стрельцова.  
С. 16–18.

370 Стрельцов А.А. Теоретические и методологические основы правового  
обеспечения информационной безопасности России: автореф. дис. ... д-ра  
юрид. наук. М., 2004. С. 18.

371 См., например: Мазуров В.А. Уголовно-правовая защита тайны: автореф.  
дис. ... канд.

юрид. наук. Томск, 2001. С. 23; Мазуров В.А. Тайна: государственная,  
коммерческая, банковская, частной жизни: учеб. пособие / под ред. С.В.  
Землюкова. М.: Дашков и К, 2003.

С. 65; Шульга А.В. Объект и предмет преступлений против собственности в  
условиях рыночных отношений и информационного общества: автореф. дис.  
... д-ра юрид. наук. С. 11–

12; Сулопаров А.В. Компьютерные преступления как разновидность  
преступлений информационного характера: автореф. дис. ... канд. юрид.  
наук. Владивосток, 2010. С. 8–9; Грошиков К.К. Социально значимая  
информация и ее уголовно-правовая охрана. С. 19; Клима-  
256

тывая общее учение о предмете преступления, обоснованно констатирует, что  
«традиционное понимание предмета преступления как вещи пережило свое  
время». Он предлагает включать в предмет преступления различные объекты  
материального мира (вещи, природные объекты, энергию) и информацию,  
не опосредованную какими-либо объектами материального мира<sup>372</sup>. Такой  
подход к пониманию предмета преступления в целом разделяется и другими  
авторами<sup>373</sup>. Поддержан он в учебной литературе, где предметом  
— преступления

предлагается считать «вещи или иные предметы внешнего мира, а также интеллектуальные ценности»,

374 «материальное или нематериальное благо»,

375 «материальные или нематериальные блага»

376

, «материальные или нематериальные блага (ценности)»

377. Полагаем, что более обобщенно предмет преступления

можно определить как материальные или нематериальные явления.

Развитие цифровых отношений перед учением о предмете преступления

ставит достаточно сложные задачи. Они касаются выработки согласованной терминологии, единообразного понимания природы тех предметов, которые

нов А.М., Пешков Д.В., Розовская Т.И. Преступления против конституционных прав и свобод человека и гражданина: науч.-практич. пособие / под общ. ред. З.И. Брижак. М.: Юрлитинформ, 2015. С. 12.

372 Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ: автореф. дис. ...

канд. юрид. наук. С. 8–9, 17; Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ, 2006. С. 55.

373 Кузнецов И.В. Понятие и виды предметов преступлений в уголовном праве России: автореф. дис. ... канд. юрид. наук. С. 10–11; Винокуров В.Н.

Предмет преступления: отличие от смежных понятий // Журнал российского права. 2011. № 12. С. 58–59;

Спиридонова О.Е.

Содержательный аспект предмета преступления (современный взгляд на проблему) // Актуальные проблемы уголовного права на современном этапе (вопросы дифференциации ответственности и законодательной техники).

2012. № 1 (1). С. 81; Маслакова Е.А. Предмет преступления как форма выражения общественных отношений // Ученые записки Орловского государственного университета. Серия: Гуманитарные и социальные науки. 2015. № 1 (64).

С. 258; Хилота В.В. Предмет преступления в науке уголовного права: проблемы и противоречия // Журнал российского права. 2016. № 7. С. 75, 78.

374 Уголовное право Российской Федерации. Общая часть: учебник. Изд. 2-е, перераб. и доп. /

под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. М.: Контракт: ИНФРА-М, 2010.

С. 115 (автор главы Д.А. Семенов).

— 375 Российское уголовное право. Общая часть / под ред. В.С. Комиссарова.

376 Уголовное право. Общая часть: учеб. пособие / под общ. ред. В.А. Уткина, А.В. Шеслера.

Томск: Изд. Дом Томск. гос. ун-та, 2016. С. 158 (автор главы А.В. Шеслер).

377 Полный курс уголовного права: в 5 т. / под ред. А.И. Коробеева. Т. I: Преступление

и наказание. СПб.: Юридический центр Пресс, 2008. С. 345 (автор главы Г.П. Новоселов).

257

не вписываются в привычную среду правового регулирования, и рекомендаций

по квалификации посягательств на них. Так, до недавнего времени дискуссионным был вопрос о безналичных денежных средствах как предмете хищений

и иных преступлений против собственности. В настоящее время он в основном

решен в постановлениях Пленума Верховного Суда РФ от 17 декабря 2015 г.

№ 56378 и от 30 ноября 2017 г. № 48379. Однако возникла проблема

уголовноправовой оценки общественно опасных деяний, направленных на

такие предметы, как «цифровые права», включенные в ст. 128 ГК РФ

Федеральным законом

от 18 марта 2019 г. № 34-ФЗ380

, и «цифровые деньги» (криптовалюту). С развитием киберспорта не менее

значимым становится вопрос о признании предметом имущественных преступлений «атрибутов виртуальной игры», «виртуальных активов».

Теория и практика уголовного права пока не могут выработать

единых подходов по квалификации подобных деяний<sup>381</sup>. Так, в одном случае

завладение виртуальными внутриигровыми предметами у участника турнира

по компьютерным играм, совершенное с угрозой применения к нему насилия,

опасного для жизни, было квалифицировано как разбой по ч. 2 ст. 162 УК

РФ<sup>382</sup>. В другом — по факту хищения атрибутов компьютерной игры

потерпевшей в возбуждении уголовного дела было отказано<sup>383</sup>. Есть

прецедент квалификации незаконного корыстного изъятия и распоряжения

чужими вирту-

378 О судебной практике по делам о вымогательстве (статья 163 Уголовного

кодекса Российской Федерации): постановление Пленума Верховного Суда

РФ от 17.12.2015 № 56 // Сайт

Верховного Суда РФ. URL: <https://vsrf.ru/documents/own/?year=2015>

379 О судебной практике по делам о мошенничестве, присвоении и растрате:

постановление

РФ. URL:

<https://vsrf.ru/documents/own/?year=2017>

380 О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского

кодекса Российской Федерации: Федеральный закон от 18.03.2019 № 34-ФЗ // КонсультантПлюс. URL: <http://www.consultant.ru>

381 Похитители танков. За кражу аксессуаров компьютерных игр будет грозить уголовное

наказание // Интернет-портал «Российской газеты». URL:

<https://rg.ru/2019/09/16/v-rf-vvedutugolovnoe-nakazanie-za-krazhu-predmetov-v-kompiuternyh-igrah.html> (дата обращения: 06.01.2020).

382 В Красноярске полицейские задержали злоумышленников, напавших на участника компьютерного турнира // Официальный сайт Министерства внутренних дел Российской Федерации. URL:

<https://24.mvd.rf/news/item/9145006/> (дата обращения 06.01.2020).

383 Лукашев Я. Потерявшая виртуальные вещи ростовчанка добивается справедливости в реальном мире // Радиостанция Вести ФМ. URL:

<https://radiovesti.ru/brand/61178/episode/2227853/> (дата обращения: 06.01.2020).

258

альными игровыми предметами только по ч. 2 ст. 272 УК РФ как неправомерного доступа к компьютерной информации, совершенного из корыстных побуждений<sup>384</sup>

В целях единого понимания и формирования общих подходов к квалификации общественно опасных деяний, совершаемых в киберпространстве, в литературе предлагается ввести в научный оборот термин «виртуальный предмет преступления». В частности, Н.А. Розенфельд пишет: «...Направленность указанных преступлений определяется переносом определенных категорий общественных отношений в виртуальное пространство и избранием преступниками целью своих посягательств предметов виртуального мира». В связи с этим целесообразно выделять в теории уголовного права в качестве разновидности предмета преступления виртуальный предмет — «...такой предмет объективного мира, который создан при помощи специальных методов и (или) способов, не имеет внешнего представления, однако может его приобрести при помощи специальных методов и способов воздействия»

т... плодотворной. Она учитывает особенности виртуальных предметов,

закрывающиеся в том, что они существуют только в цифровой материи, созданной

в информационных системах, являются идеальными по природе, выражаются в форме цифровых знаков, символов и обозначений, их цифровых комбинаций

и кодов. Эти отличительные черты предметов цифрового пространства требуют

специальных знаний и умений при квалификации и расследовании посягательств на них.

Вторая тенденция, характеризующая современную концепцию предмета преступления, направлена на расширение этого понятия за счет включения в его объем опасных и вредных для общества и государства вещей, веществ,

384 В Раменском за неправомерный доступ к компьютерной информации третьих лиц осужден местный житель // Прокуратура Московской области. URL: <https://mosoblproc.ru/news/vramenskom-za-nepravomerniy-dostup-k-kompyuternoy-informatsii-tretih-lits-osuzhdyonmestnyi-zhitel/> (дата обращения: 06.01.2020).

385 Розенфельд Н.А. Некоторые аспекты необходимости введения понятия «виртуальный предмет преступления» в теорию уголовного права // Известия Саратовского университета.

Новая серия. Серия: Экономика. Управление. Право. 2007. Т. 7, № 2. С. 63. 259

и явлений. Реальностью является то, что уголовный закон закрепляет в качестве

признака состава преступлений предметы и продукты преступной деятельности: поддельные денежные средства, ценные бумаги, платежные карты (ст. 186,

187), оружие, взрывчатые вещества, взрывные устройства (ст. 222, 222.1), наркотические средства, психотропные вещества, их аналоги (ст. 228, 228.1), субстанции и методы, запрещенные в спорте (ст. 230.1, 230.2),

порнографические материалы и предметы (ст. 242, 242.1), предметы взятки (ст. 290, 291,

291.1, 291.2), поддельные официальные документы (ст. 327 УК РФ) и другие.

В литературе по Общей и Особенной частям уголовного права, в судебной практике они определяются как предмет преступления<sup>386</sup>

.  
Вышеизложенное можно отнести и к информации. По выводу С.В.

— Землюкова, «...по своему содержанию вредные продукты преступного

т... быть материальными или нематериальными», они «...не обязательно

выступают только в форме предметов или вещей. Это могут быть явления и события»

387. Формирование и распространение антиценностей в информационной среде не менее опасно для общества и государства, чем незаконный оборот запрещенных материальных предметов. В работах по информационной безопасности в зависимости от значения информации ее делят на два вида: на защищаемую и на «негативную информацию», то есть информацию, «...от которой

необходимо защищать психику субъектов информационных отношений»

388

Негативную информацию, созданную и распространенную в обществе, необходимо признавать предметом преступления. К примеру, в этом качестве она за-

386 См., например: Кузнецов И.В. Понятие и виды предметов преступлений в уголовном праве России: автореф. дис. ... канд. юрид. наук. С. 11, 22–24; О судебной практике по делам

о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами: постановление Пленума Верховного Суда РФ

от 15.06.2006 № 14 (ред. от 16.05.2017) // Сайт Верховного Суда РФ. URL: <https://vsrf.ru/documents/own/?year=2006>; О судебной практике по делам о взяточничестве

и об иных коррупционных преступлениях: постановление Пленума Верховного Суда РФ от

09.07.2013 № 24(ред. от 24.12.2019) // Сайт Верховного Суда РФ. URL: <https://vsrf.ru/documents/own/?year=2013>

387 Землюков С.В. Уголовно-правовые проблемы преступного вреда.

Новосибирск: Изд-во

Новосибирск. ун-та, 1991. С. 31.

388 Ефремова М.А. Уголовно-правовая охрана информационной безопасности: монография.

М.: Юрлитинформ, 2018. С. 17.

260

креплена в следующих составах преступлений: «Заведомо ложное сообщение об акте терроризма» (ст. 207), «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда

экстремистской деятельности» (ст. 280), «Возбуждение ненависти либо вражды, а равно

унижение человеческого достоинства» (ст. 282 УК РФ) и других.

Трактовка предмета преступления, охватывающая предметы ценности и антиценности, не могла не возродить в науке уголовного права дискуссию о соотношении объекта и предмета преступления и месте предмета в составе преступления. Предметы, характеризующиеся вредными свойствами, не входят

в структуру общественных отношений как объекта уголовно-правовой охраны,

а потому встает вопрос о допустимости отнесения таких предметов к подсистеме объекта. Разрешить возникшее противоречие между объектом и предметом

современные авторы предлагают путем пересмотра классических представлений о составе преступления. Ряд ученых считают, что предмет должен быть

признаком объективной стороны состава преступления (М.П. Бикмурзин, В.В. Мальцев)<sup>389</sup>. Другие — высказывают идею о разделении предмета преступления на два самостоятельных признака: собственно предмет преступления, относящийся к объекту, и «предмет совершения преступления», входящий

в объективную сторону состава преступления (В.И. Винокуров, Е.А. Маслакова, В.В. Воробьев)<sup>390</sup>. Такие взгляды на предмет преступления не новы, впервые

были высказаны в советском уголовном праве. Их обоснованная критика содержится в работах В.В. Тацян. Полагаем, что она актуальна и сегодня. Аргументы В.В. Тацян связаны с оценкой практической значимости предлагаемых

389 Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ: автореф. дис. ...

канд. юрид. наук. С. 8; Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ,

2006. С. 60–84; Мальцев В.В. Объект охраны (преступления) в уголовном праве: монография. М.: Юрлитинформ, 2012. С. 263–264.

390 Винокуров В.Н. Объект преступления: история развития и проблемы понимания: монография. Красноярск: Сибирск. ин-т МВД России, 2009. С. 44–46; Винокуров В.Н. Предмет

преступления: отличие от смежных понятий // Журнал российского права. — 2011. № 12.

общественных отношений. С. 258–261; Воробьев В. В. О предмете преступления, его месте в составе преступления и особенностях в компьютерных преступлениях // Символ науки. 2015. № 6. С. 222–223.

261

изменений. Он отмечает, что включение предмета в объективную сторону состава преступления не учитывает правового значения этого признака.

Нельзя

отрывать от объекта предмет преступления, входящий в структуру общественного отношения и выступающий элементом этого отношения.

Нецелесообразно

исключать из объекта также предмет, который не входит в структуру охраняемого законом общественного отношения. И тот и другой предмет необходим

для установления характера преступления, уточнения его объекта и конкретизации содержания объекта<sup>391</sup>. Кроме того, представляется неоправданным

включение в состав преступления дополнительных признаков. Состав преступления имеет сложившуюся классическую структуру. Введение новых признаков состава преступления неизбежно вызовет дополнительные сложности в разграничении всех смежных признаков («предмета», «предмета, совершения преступления», «способа», «средств совершения преступления», «орудий преступления» и «преступного вреда»), что вряд ли будет способствовать достижению

задачи правильной уголовно-правовой квалификации содеянного.

Приходим к выводу, что предмет преступления следует рассматривать в качестве факультативного признака элемента (подсистемы) объекта преступления. Предмет преступления можно определить как предусмотренное уголовным законом материальное или нематериальное явление, путем воздействия

на которое причиняется вред или создается угроза его причинения объекту.

Подчеркнем, что термин «воздействие» в дефиниции использован для обобщенного описания различных форм уголовно наказуемого обращения с предметами преступлений<sup>392</sup>

.

391 Таций В. Я. Предмет преступления // Правоведение. 1984. № 4. С. 54, 56–57; Таций В. Я.

Объект и предмет преступления в советском уголовном праве. Харьков: Выща шк., Изд-во

— при Харьков. гос. ун-те, 1988. С. 39–41, 55–56.

дис. ... канд. юрид.

наук. Барнаул. С. 108–109; Землюков С.В. Уголовно-правовые проблемы преступного вреда.

С. 29–35; Землюков С.В. Преступный вред: теория, законодательство, практика: автореф.

дис. ... д-ра юрид. наук. М., 1993. С. 16–17

**Учебно-методический комплекс КазНУ им. Аль-Фараби**

**ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ КАЗНУ им. АЛЬ-ФАРАБИ**

**КАФЕДРА ТАМОЖЕННОГО, ФИНАНСОВОГО И  
ЭКОЛОГИЧЕСКОГО ПРАВА**

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**  
**для проведения семинарских занятий и самостоятельной работы**  
**студентов по дисциплине**  
**НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ ФИНАНСОВО-ЦИФРОВОЙ**  
**СРЕДЫ.**

**АЛМАТЫ 2023 г.**

## Общие положения

Одним из форм обучения студентов, обучающихся по образовательной программе «БВ04109 Цифровая экономика» признаются семинарские занятия. Предлагаемые общие положения носят исключительно рекомендательный характер.

**Практические занятия** являются необходимым элементом учебного процесса. Цель практических занятий-углубление знаний, полученных лекцией, формирование профессионально важных знаний и умений. Практические занятия помогают студентам освоить юридическую терминологию, развивать культуру речи и профессиональное мышление, являются средством оперативного двухстороннего общения.

Студенты приобретают на практических занятиях навыки применения правовых норм к конкретным условиям, разъяснения нормативных документов, отбора соответствующих норм из множества правовых актов, способности придерживаться своей индивидуальности, самостоятельности мышления, своего мнения до конца.

Структура практических занятий включает следующие элементы: организационный этап (преподаватель приветствует студентов и определяет студентов, не посещающих занятия в журнале, определяет подготовку студентов к занятиям, публикует темы и планы занятий); заслушивает ответы студентов на вопросы по материалу; основная часть (анализ теоретических вопросов и решение задач); подведение итогов урока (преподаватель оценивает работу всей группы, оглашает и объясняет оценки, показывает результаты и допущенные недостатки в ответах конкретного студента, дает задание на следующее занятие). Основная часть практических занятий должна быть направлена на оперативную координацию теоретических вопросов с решением задач, значительная часть времени направляется на решение задач, в течение 50-минутного занятия рекомендуется потратить 10-15 минут на анализ теоретических вопросов. Анализ теоретических вопросов разнообразен: доклады студентов, решение задач, теоретический семинар.

Преподаватель должен объяснить студентам, каким требованиям должен соответствовать доклад. Отмечая тему доклада, следует отметить авторов, использованных в работе, подробно излагать план доклада и соответствующие вопросы по докладу на источники с указанием ссылок на источники, мнения авторов, по возможности, выражая свое мнение.

Решение задач должно содержаться в тетрадях студентов в письменной форме в виде полного ответа на поставленные вопросы. Каждое событие, изложенное в задаче, требует юридической оценки связанных с ними вопросов. На каждый вопрос необходимо дать четкий ответ (Да, нет) со ссылкой на нормы закона. Студент должен указать, как применялась

соответствующая норма, в соответствующих случаях со ссылкой на нормативные постановления Верховного Суда РК (иные правовые акты), научные разъяснения. Студент, освоивший данную методологию, приобретает практические навыки, связанные с эффективным решением профессиональных задач.

**Семинар** (лат. *seminarium*-рассадник) - форма учебного процесса, основанная на самостоятельном изучении студентов в виде отдельных вопросов, докладов или совместного обсуждения проблем по поручению руководителя. По сравнению с практическими занятиями семинар носит теоретический характер и глубоко направлен на определенную дисциплину. Семинарские занятия способствуют укреплению знаний, направляя учащихся на самостоятельность в учебно-познавательной деятельности. В ходе семинара систематизируются, углубляются и отслеживаются знания, полученные в результате работы с источниками, дополнительной литературой, документами. Главная цель семинарских занятий-обеспечить студентов возможностью приобретения навыков использования теоретических знаний, исходя из особенностей изучаемых областей.

Различают три типа семинара в зависимости от основных целевых направлений:

- семинар, посвященный углубленному изучению определенного курса обучения, тематически связанный с материалом данного курса;
- семинар по методологически значимому курсу или обоснованной подготовке определенной темы;
- семинар по исследовательскому типу, предназначенному для научной обработки отдельных актуальных проблем, который может быть перенесен на специальный семинар

Специальный семинар представляет собой школу общения молодых исследователей с определенной проблемой под руководством известного ученого. Опытный руководитель создает атмосферу научного творчества, ориентирует студентов на коллективную мыслительную деятельность, использует эффективные методы исследовательской работы. На итоговом занятии преподаватель проводит полный обзор и обобщает научные работы, раскрывает возможности дальнейшего изучения рассматриваемых проблем, объясняет возможности заинтересованных студентов участвовать в исследовании этих проблем.

Семинарские занятия тесно связаны с лекционными занятиями, однако учебный материал семинара не дублирует лекционный материал. Руководящая роль преподавателя заключается в тщательном планировании учебной работы, выделении важных вопросов на анализ семинара, выборе литературы для самостоятельной подготовки, руководстве процессом обсуждения.

В зависимости от способа проведения семинар подразделяется на следующие виды:

**Семинар-интервью** означает вовлечение значительной части студентов к активному обсуждению темы, выразив готовность всех студентов к занятиям по всем вопросам в плане семинара. После краткого доклада преподавателя, заслушиваются подробные заявления нескольких студентов по конкретным вопросам плана, дополняются ответами других студентов, в конце преподаватель делает выводы.

**Семинар-дискуссия**, или семинар-диспут представляют собой возможность диалога участников семинара для коллективного обсуждения и решения какой-либо проблемы. Для обсуждения выбираются наиболее актуальные проблемы изучаемой дисциплины. Участники дискуссии учатся четко сформулировать свои мысли, поддерживать свое мнение, уважать критические мнения. Наиболее эффективной формой семинарских занятий является «круглый стол» в правилах соответствия участников. В связи с этим необходимо обучить студентов культуре общения и взаимодействия, чтобы обсудить тему дискуссии через диалог.

**Смешанная форма семинара** проводится в виде обсуждения докладов, свободных выступлений участников, запланированных дискуссий.

Педагогическое руководство подготовкой студентов к семинару заключается в помощи преподавателя в составлении плана докладов, обучении конспектированию литературных источников, правильном оформлении текстов рефератов и докладов, консультировании по вопросам, возникающим в процессе самостоятельной работы.

- **Самостоятельная работа студентов**
- **Виды работ. Их общая характеристика. Требования к написанию**
- **Цели написания самостоятельной работы**

Самостоятельная работа-запланированная работа студентов, направленная на развитие познавательных способностей студентов и повышение самостоятельного непрерывного образования, под руководством и заданием преподавателя.

В связи с резким ростом учебного и научного материала, нехваткой аудиторных часов для изучения дисциплины, СРС играет важную роль в рамках учебного процесса. Любой выпускник вуза должен обладать фундаментальными знаниями, навыками, навыками профессиональной деятельности, опытом творческой и исследовательской деятельности, социальными и коммуникативными навыками, формируемыми в процессе самостоятельной работы студентов.

Дидактические задачи СРС: закрепление, углубление, расширение, систематизация знаний, полученных в ходе аудиторных занятий; самостоятельное освоение нового учебного материала; развитие

профессиональных навыков, а также навыков самостоятельной мыслительной деятельности; совершенствование самостоятельного мышления, интереса к юридической литературе, практической юридической деятельности, правотворческому процессу.

Основными формами СРС являются: домашняя работа; подготовка рефератов по отдельным темам; учебно-исследовательская и научно-исследовательская работа студентов, представляющая собой участие в работе научных кружков и научных конференций (учебно-исследовательская работа студентов - УИРС и научно-исследовательская работа студентов - НИРС); организация и проведение деловых игр во внеаудиторное время.

**Домашняя работа** проявляется в самостоятельной подготовке к практическим и семинарским занятиям, в виде любой самостоятельной учебной деятельности, являющейся частью учебного процесса. Основная деятельность-развитие навыков самостоятельного обучения, определение методов и средств работы, планирование обучения. Домашняя работа помогает закрепить полученные на аудиторных занятиях знания и навыки, сформировать навыки, овладеть новым материалом.

Дидактические условия, обеспечивающие успешное выполнение самостоятельной работы: четкое представление задач и рекомендаций, касающихся выполнения заданий; обоснованность учебного задания (для чего, почему помогает); эффективный объем домашних заданий; форма отчета через преподавателя, сроки сдачи; определение видов консультаций; критерии оценки, виды и формы контроля.

Содержание самостоятельной учебной работы студентов составляет: изучение и конспектирование литературы, представленной преподавателем; решение задач по конкретным разделам, разделам курса в сочетании с обсуждением на практических занятиях; обзор судебных дел с обсуждением на семинаре или заседании научного кружка; участие в судебных заседаниях по поручению преподавателя, ознакомление с работой юридических отделов различных организаций, нотариальных контор; подготовка отзывов на законопроекты в виде домашнего задания. ; подготовка проектов правовых документов в рамках изучаемой темы в сочетании с практическими занятиями.

Подготовка рефератов-одна из форм организации и контроля СРС. Реферат (лат. *referre*-изложение, сообщение) – это краткое изложение содержания источника путем рациональной оценки или раскрытие состояния какой-либо проблемы на основе сравнения и анализа нескольких источников. В зависимости от содержания и деятельности в учебном процессе рефераты подразделяются на научно-проблемные и обзорно-информационные.

Цель написания реферата - совершенствование у студентов навыков самостоятельной работы с литературными и нормативными источниками,

опубликованной судебно-следственной практикой. Студенты могут сделать выводы теоретического и практического характера путем самостоятельного обоснования на основе их анализа и обобщения. Тематика рефератов, список рекомендуемой литературы определяется преподавателем. Рефераты, связанные с кратким изложением содержания какой-либо книги или статьи, могут быть рассмотрены первым этапом подготовки дипломной работы по соответствующей теме. Объем реферата может быть как 15-20 страниц машинного текста. Типичная структура реферата: план; введение с указанием основ темы и задач; основная часть, состоящая из нескольких параграфов; заключение, содержащее выводы по теме; библиографический список.

- **Общие требования к работе**

При выборе темы самостоятельной работы студентов должны учитываться следующие правила:

- работа должна отвечать интересам, конкретной воле студентов,
- работа должна быть полезной для специальности юриспруденции (в частности, тема должна быть пригодна для публикации в качестве статьи с учетом современного состояния науки). Сказанное не должно повторяться таким образом, чтобы они отвечали требованиям студентов, которые в связи с продвижением науки вперед. Еще одна возможность в дальнейшем не дает четких тем самостоятельной работы с целью недопущения копирования.

- **Основные направления самостоятельной работы**

- **Рефераты (доклады)**

По основному учебному курсу дается тематический обзор (сравнительный анализ) и дается тематика, связанная с проблемами предмета, не охваченной основной программой в зависимости от времени. В частности, в зависимости от основного курса их можно разделить на три группы: а) с целью более глубокого раскрытия темы, кратко охватываемой основным курсом; б) темы, вообще не охваченные обязательным курсом; в) темы, рассматриваемые на обязательном курсе, не относящиеся к самостоятельной работе студентов.

- **Требования к оформлению самостоятельной работы**

Работа должна быть набрана на компьютере. В тексте должны быть указаны курс, предмет, ФИО автора, название работы. Если работа имеет перевод, то должна быть представлена библиографическая точная информация того же материала. Кроме того, к переводу должен быть приложен словарь профессиональных терминов. Если работа не переводится, то дается его содержание. На последней странице работы обязательно указывается пронумерованный список использованной литературы. В тексте номера работ в данном списке обязательно должны быть указаны в прямых скобках с указанием соответствующих мест.

- **Подготовка к самостоятельной работе и ее написание**

Выбор темы. Предварительный выбор темы по вышеуказанным направлениям осуществляется самостоятельно студентом. Уточняется тема, консультации с преподавателем, составление плана, список используемой литературы. По любым возникшим вопросам студент может получить ответы от преподавателя. В необходимых случаях назначаются консультации. Работа поручается преподавателю не позднее, чем за две недели до сессии. Защита самостоятельной работы допускается во время сессии.

- **Критерии оценки самостоятельной работы**

Преподаватель ставит устные вопросы при приеме работы от каждого студента. Студент должен ответить на вопрос преподавателя в зависимости от текста работы. При ответе необходимо указать усвоение материала в тексте (написание, перевод, копирование). При оценке работы должен учитывать письменный вариант текста и оригинальность написания самостоятельной работы студентов, обоснованность данных выводов и указаний.

График выполнения и сдачи заданий СРС

Тема №	Содержание задания	Время и форма сдачи (прием и защита)	Количество баллов
1	<p><b>1 СРС Тема:</b> Исключительные права в цифровой среде: охрана и защита. (презентация).</p>	<p>Получение задания на 2 недели; 3 неделя сдача СРС форма-защита презентации. При раскрытии темы необходимо : анализировать, сравнивая законодательство, регулирующее данное отношение, сравнивать с законодательством одного из стран ближнего и дальнего зарубежья, показать особенности.</p>	<p>20 баллов. Основы оценки работы: Верность идеи, глубокое изучение материалов, полнота решения, художественное оформление, ораторское искусство.</p>
2	<p><b>2 СРС тема:</b> Ответственность за неправомерные действия при разработке и использовании технологии искусственного интеллекта.</p>	<p>Получение задания на 6 неделе; Сдача и защита на 7 неделе; Форма сдачи-защита дебат. При раскрытии темы необходимо : анализировать, сравнивая законодательство, регулирующее данное отношение, сравнивать с законодательством одного из стран ближнего и дальнего зарубежья, показать особенности.</p>	<p>23 баллов. Основы оценки работы: Верность идеи, глубокое изучение материалов, полнота решения, художественное оформление, ораторское искусство.</p>
3	<p><b>3 СРС. Тема:</b> Обсуждение актуальных вопросов дальнейших тенденций развития финансово-цифровой среды по Посланию Президента РК народу Казахстана</p>	<p>Получение задания на 9 неделе; Сдача и защита на 11 неделе; Форма сдачи-защита презентации.</p>	<p>15 баллов. Основы оценки работы: Верность идеи, глубокое изучение материалов, полнота решения,</p>

		При раскрытии темы необходимо : анализировать, сравнивая законодательство, регулирующее данное отношение, сравнивать с законодательством одного из стран ближнего и дальнего зарубежья, показать особенности.	художественное оформление, ораторское искусство.
4	<b>4 СРС. Тема:</b> Вопросы правового регулирования налоговой службы Республики Казахстан. Виды налогов. Анализ налогового законодательства	Получение задания на 10 неделе; Сдача и защита на 11 неделе; Форма сдачи-защита реферат. При раскрытии темы необходимо : анализировать, сравнивая законодательство, регулирующее данное отношение, сравнивать с законодательством одного из стран ближнего и дальнего зарубежья, показать особенности.	12 баллов. Основы оценки работы: Верность идеи, глубокое изучение материалов, полнота решения, художественное оформление, ораторское искусство.
5	<b>5 СРС. Тема:</b> Развитие Open API, Open Banking и экосистемы цифровых финансовых сервисов в Республике Казахстан.	Получение задания на 12 неделе; Сдача и защита на 13 неделе; Форма сдачи-защита презентации. При раскрытии темы необходимо : анализировать, сравнивая законодательство, регулирующее данное отношение, сравнивать с законодательством одного из стран ближнего и дальнего зарубежья, показать особенности.	15 баллов. Основы оценки работы: Верность идеи, глубокое изучение материалов, полнота решения, художественное оформление, ораторское искусство.

## НПА и литература:

### Литература:

#### Основная:

1. Цифровая экономика. Учебное пособие/ М.М. Ковалев, Г.Г. Головенчик. – Минск: Изд. центр БГУ, 2018. – 328 с.
2. Кулумбетова Д.Б., Маулина Н.Х., Асанова А.Б. Цифровая трансформация казахстанского банковского сектора на современном этапе развития //Научный вестник: Финансы, банки, инвестиции № 3. 2021.
3. Касенова Г.Е Современные финансовые услуги банков: учебное пособие /Қазақ Университеті- Алматы, 2021, 264с.
4. Глоссарий по цифровым финансовым услугам. Совместная публикация Всемирного почтового союза и Международного союза электросвязи. 2017 // <https://creativecommons.org/licenses/by-nc-sa/4.0/>
5. Цифровая трансформация финансовых услуг: модели развития и стратегии для участников отрасли. SKOLKOVO Business School – Ernst & YoungInstitute for Emerging Market Studies (IEMS) // <https://www.skolkovo.ru>.
6. Новикова Е.А Цифровизация финансового сектора: новые инструменты и перспективы их использования: Материалы конференции «Право, экономика и управление: от теории к практике». Чебоксары, 2020г.
7. Касенова Г.Е Финансовые риски: учебное пособие /Қазақ Университеті- Алматы, 2020, 264с.
8. Государственная программа "Цифровой Казахстан" от 12 декабря 2017 года // <https://adilet.zan.kz/rus/docs/P1700000827>

#### Дополнительная:

1. Закон Республики Казахстан «О введении национальной валюты Республики Казахстан» от 12 ноября 1993г. // <https://online.zakon.kz>
2. Закон Республики Казахстан «О Национальном Банке Республики Казахстан». от 30 марта 1995 № 2155 (с доп.и изм. 03.03.2023г.) // <https://online.zakon.kz>
3. Закон Республики Казахстан «О банках и банковской деятельности в Республики Казахстан» от 31августа 1995. № 2444 (с доп.и изм. 03.03.2023г.). // <https://online.zakon.kz>
4. Закон Республики Казахстан от 4 июля 2003 года № 474-ІІ «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» (с доп.и изм. по состоянию на 12.09.2022 г.)
5. Закон РК от 24 мая 2021 года № 43-VІІ «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам регулирования банковской, микрофинансовой и коллекторской деятельности в РК», (с изм. и доп. по состоянию на 03.03.2023 г.) // <https://online.zakon.kz>
6. Концепция развития Open API и Open Banking в Республике Казахстан на 2023–2025 годы // <https://www.nationalbank.kz/>
7. Бюро национальной статистики. Информационный бюллетень. Проект Kazstat // <https://new.stat.gov.kz/ru/>.
8. Концепции развития Open API и Open Banking// <https://www.nationalbank.kz/>
9. Исследования Международного финансового центра «Астана» // <https://aifc.kz/ru/>
- 10.Краткий отчет Mobile banking rank Казахстан 2022 // <https://markswebb.ru/report/mobile-banking-rank-kz-2022/>
11. Концепция развития финансового сектора Республики Казахстан до 2030 года от 26 сентября 2022 года // <https://adilet.zan.kz/rus/docs/U2200001021>

#### Интернет-ресурсы:

1. Официальный сайт НБРК // <http://www.nationalbank.kz>

2. Официальный сайт Агентства РК по регулированию и развитию финансового рынка // <https://www.gov.kz>
3. Официальный сайт Казахстанской фондовой биржи KASE // <http://www.kase.kz>
4. Аналитические дэшборды // [Ranking.kz](http://Ranking.kz)
5. Аналитический портал // <https://kapital.kz/finance>

## Практические занятия

### Тема 1. Понятие и сущность финансово-цифровой среды

#### Вопросы

1. Какова роль финансово-цифровой среды в современном мире?
2. Назовите причины и условия возникновения финансово-цифровой среды?
3. Какова сущность информационно-коммуникационных технологий?
4. Перечислите новые феномены в постиндустриальной экономике?
5. Дайте понятие цифровой экономики, какова ее институциональная структура?

### Тема 2. Финансово-цифровая среда как новая стадия глобализации

#### Вопросы

1. Назовите технологические уклады и промышленные революции?
2. Какова периодизация финансово-цифровой среды?
3. Финансово-цифровой среды как новая стадия глобализации.
4. Какова инфраструктура цифрового финансового рынка, его объекты и субъекты?
5. В чем заключается регулирование финансово-цифровой среды?
6. Определите взаимосвязь финансово-цифровой среды и экономического роста?

Задание: Подготовить презентацию по теме: «Анализ регулирования цифровой экономики в странах мира» (Выбрать страну)

### Тема 3. Big Data в принятии решений в экономике и финансах

1. Что собой представляют облачные вычисления и хранилища данных?
2. Облачные вычисления и хранилища данных.
3. Отличительные характеристики облачных вычислений.
4. Облака сообществ, публичные, частные и гибридные.
5. Модели облачных услуг.
6. Мировой рынок облачных сервисов.
7. Какова концепция больших данных (Big Data)?
8. Какова роль Big Data в экономике и в финансах государства?
9. Характеристика технологий больших данных.
10. Ограничения и сдерживающие факторы использования больших данных.

Задание: Подготовить презентацию по теме: «Роль Big Data в экономике и в финансах стран мира» (Выбрать страну)

## **Тема 4. Международные подходы регулирования Open API и Open Banking**

### Вопросы

1. Концепция развития финансового сектора Республики Казахстан до 2030 года.
2. Основные цели финансовых регуляторов, стимулирующие развитие Open API и Open Banking
3. Директивы PSD (Payment Services Directive) и PSD2.

Задание: Подготовить презентацию по теме: «Особенности регулирования Open API и Open Banking в мире»

## **Тема 5. Развитие Open API, Open Banking и экосистемы цифровых финансовых сервисов в Республике Казахстан**

### Вопросы

1. Определить основные направления Концепция развития Open API и Open Banking
2. Тенденции развития Open API и Open Banking
3. Участник развития и внедрения Open API и Open Banking
4. Нормативно-правовое регулирование Open API и Open Banking
5. Проект Закона Республики Казахстан по вопросам регулирования цифровых технологий
6. Каковы области регулирования и предлагаемые нормы НПА?

Задание: Подготовить презентацию по теме: «Новации в регулировании цифровых технологий в Казахстане»

## **Тема 6. Развитие устойчивой инфраструктуры Open API и Open Banking**

### Вопросы

1. Развитие экосистемы Open API и Open Banking
2. Монетизация данных
3. Меры развития Open API и Open Banking
4. Дорожная карта на 2023-2025 годы

Задание: Подготовить презентацию по теме: «Лучшие кейсы внедрения Open API и Open Banking»

## **Тема 7. Цифровизация налогообложения**

### Вопросы для самоконтроля

1. Каково влияние цифровых технологий на развитие налоговой системы?
2. Назовите направления цифровизация органов государственных доходов?
3. Определите электронные услуги (прием налоговой отчетности, выдача

выписок из лицевого счета о состоянии расчетов с бюджетом, а также по социальным платежам, представление сведений об отсутствии (наличии) задолженности, учет по которым ведется в органах государственных доходов)?

4. Каковы направления «Цифровизации налогового администрирования»?
5. Горизонтальный мониторинг крупных налогоплательщиков.

Задание: Подготовить презентацию по теме: «Цифровизация налогообложения в развитых странах» (Выбрать страну)

## **Тема 8. Цифровой банкинг**

Вопросы

1. Цифровая трансформация банковских услуг
2. Зарубежные бизнес-модели банка в условиях цифровизации
3. Трансформация банковских бизнес-моделей в условиях цифровых технологий
4. Рейтинг мобильных приложений БВУ
5. Экосистемы банков: понятие и виды экосистем
6. Цифровые банки и их рейтинг
7. Цифровая трансформация казахстанских банков

Задание: Подготовить презентацию по теме: «Анализ цифровых продуктов в БВУ» (Выбрать БВУ)

## **Тема 9. Цифровизация на рынке ценных бумаг**

Вопросы

1. Какой уровень цифровизации технологий фондового рынка?
2. Каковы особенности цифровизации деятельности фондовой и валютной биржи?
3. Каковы перспективы и проблемы развития современного рынка ценных бумаг в условиях цифровизации?
4. Торгово-клиринговой системы ASTS+ (дает возможность участникам рынка торговать в режиме реального времени с участием и без участия центрального контрагента).

Задание: Подготовить презентацию по теме: «Мобильные приложения по инвестициям и управлению портфелем ЦБ» (Выбрать БВУ или управляющую компанию)

## **Тема 10. Цифровизация в страховании**

Вопросы

1. Дайте характеристику понятия «цифровое страхование»?
2. Дайте анализ текущего состояния страхового рынка в условиях цифровизации страхования.
3. Характеристика основных направлений цифровизации страхового

рынка.

4. Использование цифровых технологий в бизнес-процессах страховщика.

Задание: Подготовить презентацию по теме: «Мобильные приложения по страховым продуктам» (Выбрать СК)

### **Тема 11. Цифровой тенге**

Вопросы

1. Определение и особенности технологии блокчейн.
2. Экономические основы технологии распределенных реестров хранения информации (блокчейн).
3. Блокчейн в государственных услугах.
4. Результаты исследования о необходимости внедрения цифрового тенге
5. Модель принятия решения о внедрении Цифрового тенге

Задание: Подготовить презентацию по теме: «Цифровые валюты Центральных банков (CBDC) стран мира» (Выбрать страну)

### **Тема 12. Цифровизация платежей и переводов**

Вопросы

1. Осуществить анализ развития систем электронных платежей.
2. Система электронных платежей.
3. Преимущества электронных платежных систем.
4. Риски электронных платежных систем.

Задание: Подготовить презентацию по теме: «Цифровые платежные системы Казахстана»

### **Тема 13. Криптовалюты: история возникновения и классификация**

Вопросы

1. Сущность и определение криптовалюты.
2. Сходства и различия криптовалют с фиатными валютами.
3. Классификация криптовалют.
4. Криптовалютные биржи.
5. ICO и лейдинг.
6. Правовое регулирование криптовалют в различных странах.
7. Перспективы и риски применения криптовалют в финансовой системе государства.

Задание: Подготовить презентацию по теме: «Анализ и особенности обращения криптовалюты» (Выбрать криптовалюту)

### **Тема 14. Киберпреступность и стратегии кибербезопасности**

## Вопросы

1. Понятие киберпреступности и киберпреступления.
2. Характеристики глобальной киберпреступности.
3. Национальные стратегии кибербезопасности и информационной безопасности.
4. Расходы на кибербезопасность.

Задание: Подготовить презентацию по теме: «Международные стратегии кибербезопасности»

## **Тема 15. Оценка киберрисков банков Казахстана**

### Вопросы

1. Киберстратегия, трансформация и оценка
2. Управление киберрисками и соответствие нормативным требованиям
3. Обучение, образование и повышение осведомленности в области кибербезопасности
4. Аналитика киберрисков
5. Операционный центр безопасности
6. Киберразведка и анализ угроз
7. Реагирование на кибер-инциденты
8. Кибербоевые учения

Задание: Подготовить презентацию по теме: «Анализ киберугроз современных банков» (Выбрать банк)

### **Требования к оформлению презентаций:**

1. 7-10 информативных слайда, шрифт Arial (Основной текст)
2. не более 3-5 предложений в одном слайде
3. не более трех цветов в одном слайде
4. В презентации рассмотреть 3-4 вопроса
5. В шапке каждого слайда – номер и название рассматриваемого вопроса
6. В слайдах желательно использовать инфографику (графический метод подачи информации - схемы, рисунки, диаграммы, таблицы)
7. Все презентации должны быть сделаны по единому образцу
8. В последнем слайде указать источники литературы или официальные сайты, используемые при подготовке данной презентации

## СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

### Основная:

1. Цифровая экономика. Учебное пособие/ М.М. Ковалев, Г.Г. Головенчик. – Минск: Изд. центр БГУ, 2018. – 328 с.
2. Кулумбетова Д.Б., Маулина Н.Х., Асанова А.Б. Цифровая трансформация казахстанского банковского сектора на современном этапе развития //Научный вестник: Финансы, банки, инвестиции № 3. 2021.
3. Касенова Г.Е Современные финансовые услуги банков: учебное пособие /Қазақ Университеті- Алматы, 2021, 264с.
4. Глоссарий по цифровым финансовым услугам. Совместная публикация Всемирного почтового союза и Международного союза электросвязи. 2017 // <https://creativecommons.org/licenses/by-nc-sa/4.0/>
5. Цифровая трансформация финансовых услуг: модели развития и стратегии для участников отрасли. SKOLKOVO Business School – Ernst & YoungInstitute for Emerging Market Studies (IEMS) // <https://www.skolkovo.ru>.
6. Новикова Е.А Цифровизация финансового сектора: новые инструменты и перспективы их использования: Материалы конференции «Право, экономика и управление: от теории к практике». Чебоксары, 2020г.
7. Касенова Г.Е Финансовые риски: учебное пособие /Қазақ Университеті- Алматы, 2020, 264с.

### Дополнительная:

1. Закон Республики Казахстан «О введении национальной валюты Республики Казахстан» от 12 ноября 1993г. // <https://online.zakon.kz>
2. Закон Республики Казахстан «О Национальном Банке Республики Казахстан». от 30 марта 1995 № 2155 (с доп.и изм. 03.03.2023г.) // <https://online.zakon.kz>
3. Закон Республики Казахстан «О банках и банковской деятельности в Республике Казахстан» от 3 августа 1995. № 2444 (с доп.и изм. 03.03.2023г.). // <https://online.zakon.kz>
4. Закон Республики Казахстан от 4 июля 2003 года № 474-ІІ «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» (с доп.и изм. по состоянию на 12.09.2022 г.)
5. Закон РК от 24 мая 2021 года № 43-VІІ «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам регулирования банковской, микрофинансовой и коллекторской деятельности в РК», (с изм. и доп. по состоянию на 03.03.2023 г.) // <https://online.zakon.kz>
6. Концепция развития Open API и Open Banking в Республике Казахстан на 2023–2025 годы // <https://www.nationalbank.kz/>
7. Бюро национальной статистики. Информационный бюллетень. Проект Kazstat // <https://new.stat.gov.kz/ru/>.
8. Концепции развития Open API и Open Banking// <https://www.nationalbank.kz/>
9. Исследования Международного финансового центра «Астана» // <https://aifc.kz/ru/>
10. Краткий отчет Mobile banking rank Казахстан 2022 // <https://markswebb.ru/report/mobile-banking-rank-kz-2022/>

Интернет-ресурсы:

1. Официальный сайт НБРК // <http://www.nationalbank.kz>
2. Официальный сайт Агентства РК по регулированию и развитию финансового рынка // <https://www.gov.kz>
3. Официальный сайт Казахстанской фондовой биржи KASE  
//<http://www.kase.kz>
4. Аналитические дэшборды // [Ranking.kz](http://Ranking.kz)
5. Аналитический портал // <https://kapital.kz/finance>

### Карта обеспечения учебниками и учебно-методическими пособиями

№	Ф. И. О. автора / составителя	Наименование	издательство, год выпуска	Количество экземпляров		Общее количество студентов	%
				В библиотеке	на кафедре		
<b>Учебная литература</b> (только учебники или учебные пособия, а также в формате электронного издания)							
1.	Спанкулова, Л. С.	Защита банковской информации	КазНУ, 2002. - 82 с. - URL: <a href="http://elib.kaznu.kz/order-book">http://elib.kaznu.kz/order-book</a> .	18	0	3	
	О. В. Китова (науч.ред.), С. Н. Брускин, Л. П. Дьяконова и др	Цифровой бизнес : учебник	<a href="http://elib.kaznu.kz/order-book">http://elib.kaznu.kz/order-book</a> . - Библиогр.: с. 410-412. - 500 (тираж) экз. - ISBN 978-5-16-013017-	1	0	3	
	М. В. Ларин, В. Ф. Янковая, Н. Г. Суровцева, Е. В. Трентьева ;	Управление документами в цифровой экономике : организация, регламентация, реализация	РГГУ. - Москва : РГГУ, 2021. - 241	1	0	3	
<b>Дополнительная литература</b>							
1.	Товма, Наталья Александровна.	Цифровая экономика: зарубежный опыт и Казахстанская практика	КазНУ им. аль-Фараби. - Алматы	9	0	3	
2.	Жатканбаев, Ержан Байгужаевич.	Интеллектуализация техники и технологии - содержание четвертой промышленной	Е. Б. Жатканбаев ; КазНУ им. аль-Фараби. - Алматы : Қазақ ун-ті, <a href="http://elib.kaznu.kz/book/15863">http://elib.kaznu.kz/book/15863</a> .	1	0	3	

		революции					
3.	Султанбаева, Гульмира Серикбаевна.	Формирование интеллектуального капитала в цифровых СМИ :	КазНУ им. аль-Фараби. - Алматы : Қазақ ун-ті, 2015. <a href="http://elib.kaznu.kz/order-book">http://elib.kaznu.kz/order-book</a>	1	0	3	
1.	Материалы Международного круглого стола на интерактивной площадке "G- GLOBAL" "Интеллектуальное обеспечение...".	"Интеллектуальное обеспечение перехода Казахстана к цифровой экономике: изменение парадигмы образования и трудовых отношений".	междунар. круглый стол (2017 ; Алматы). 27 сент. 2017 г. : сборник / М-во образования и науки РК, КазНУ им. аль- Фараби ; [под общ. ред. М. С. Тулегеновой]. - Алматы : Қазақ ун-ті, 2017. - 69 с. : ил. - URL: <a href="https://elib.kaznu.kz/book/19726">https://elib.kaznu.kz/book/19726</a> .	1	0	3	

**Рассмотрено на заседании кафедры таможенного, финансового и экологического права  
протокол № \_\_\_ «\_\_\_» \_\_\_\_\_ 2023 г.**

**Заведующий кафедрой  
доктор юридических наук,  
профессор**

**Г. А. Куаналиева**

**Лектор  
кандидат юридических наук,  
доцент**

**Ж. М. Аманжолов**

**КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ**  
**Юридический факультет**  
**Кафедра таможенного, финансового и экологического права**

**ПРОГРАММА ИТОГОВОГО ЭКЗАМЕНА**

**Предмет: 98454 Нормативное регулирование финансово-цифровой среды.**

**Образовательная программа «6В04109 Цифровая экономика»**

Курс – 3

Семестр – 6

Кол-во кредитов – 5

Форма обучения: дневная

**Алматы 2024 г.**



## Введение

Освоение образовательной программы бакалавра по специальности «БВ04109 Цифровая экономика» в соответствии с государственным общеобязательным стандартом образования РК и академической политикой, изучение дисциплины завершается итоговым контролем, заключающимся в сдаче экзамена. К экзаменационно-итоговому контролю допускаются только студенты, набравшие соответствующие баллы по завершению образовательного процесса по дисциплине в соответствии с учебными программами и рабочими учебными планами бакалавриата. Экзамен проводится в сроки, указанные в Академическом календаре и рабочем учебном плане.

Студентам, получившим неудовлетворительную оценку, сдача итогового контроля за этот период разрешается только с оплатой кредита и повторным обучением. Предусмотрена подача апелляции. Студент, получивший по результатам экзамена неудовлетворительную оценку 25 баллов приказом университета регистрируется на повторное обучение, ФХ сдается повторно. Документы по состоянию здоровья, выданные после получения неудовлетворительной оценки, не рассматриваются.

Пересдача экзамена в целях поощрения оценки не допускается.

Экзаменационные вопросы проходят проверку и утверждаются.

Правила проведения экзамена

Форма экзамена-стандартная устная офлайн. Устный экзамен: традиционный-ответы на вопросы. Устный экзамен-по графику экзамена обучающийся принимается преподавателем или представителями экзаменационной комиссии. Комиссия обеспечивает соблюдение требований экзамена с начала и до окончания экзамена.

Формат экзамена-офлайн устный.

Прием экзаменов осуществляется в соответствии с графиком, утвержденным факультетом.

Процесс сдачи устного экзамена студентом осуществляется в форме выбора экзаменационного билета, на который магистрант должен дать устный ответ экзаменационной комиссии. При проведении устного экзамена в обязательном порядке осуществляется комиссией.

Проводится устный экзамен:

\* в закрепленной аудитории;

\* в составе комиссии.

Контроль проведения экзамена

Преподаватель или экзаменационная комиссия:

\* объясняет требование экзамена,

\* проверяет, не повторяются ли вопросы билета.

Продолжительность

Время подготовки-решает экзаменатор или экзаменационная комиссия. Время ответа-экзаменатор или экзаменационная комиссия решает. Для ответа на все вопросы билета предоставляется 15-20 минут.

График проведения экзамена должен быть заранее известен экзаменуемым магистрантам и преподавателям, т.е. проводится в соответствии с утвержденным графиком в утвержденной аудитории. Это ответственность кафедр и факультетов.

Формат экзамена-офлайн устный. Обучающийся сдает экзамен в режиме реального времени «здесь и сейчас».

Продолжительность экзамена-указывается дата и время в утвержденном расписании.

Билеты создаются автоматически для магистрантов.

Преподаватель

1. в системе Univer размещается «программа итогового экзамена " и итоговый экзамен по дисциплине должен быть представлен в формате pdf, в котором:

- \* правила проведения экзамена;
- \* Оценочная политика;
- \* график проведения;
- \* платформа для проведения экзаменов

Важно. Оглашение экзаменационных вопросов запрещено. Только в программе итогового экзамена записываются вопросы, охватываемые по дисциплине.

2. преподаватель в обязательном порядке после установления даты экзамена в расписании сообщает магистрантам, где находятся правила итогового экзамена.

Оглашает регламент экзамена:

- \* порядок сдачи экзаменов,
- \* время подготовки,
- \* время отклика;
- \* разрешает при необходимости составлять тезисы ответов на бумаге;
- \* ручкой;
- \* экзаменатор предупреждает, что он должен показать лист.

Преподаватель:

1. объявляет фамилию, имя и отчество экзаменуемого;

2. экзаменуемого просят предъявить документ, удостоверяющий личность (удостоверение личности или паспорт. Прием экзамена по ID-карте запрещен);

3. предупреждает о запрете использования дополнительных источников информации;

4. председатель экзаменационной комиссии называет ФИО магистранта, читает вопросы экзаменационного билета и билета;

6. комиссия записывает вопросы, озвученные студентом, для последующего опроса;

7. дает время для подготовки ответа:

\* время подготовки определяется преподавателем и / или членами комиссии;

\* члены комиссии и преподаватель контролируют процесс подготовки магистранта;

\* при необходимости делать замечания или останавливать ответ студента (грубое нарушение правил поведения на экзамене с составлением акта нарушения в случае наличия);

\* студентам разрешается использовать проект для составления конспекта ответа;

8. студента спрашивают по вопросам билетов;

9. после завершения ответа экзаменатор дает разрешение студенту выйти из аудитории;

10. далее процедуру повторяют с каждым выпускником группы.

Студенты

**ВНИМАНИЕ. СТУДЕНТ НЕ ВПРАВЕ ОТКРЫВАТЬ БИЛЕТ ДО ЛИЧНОГО ВЫЗОВА КОМИССИИ ДЛЯ СДАЧИ ЭКЗАМЕНА. ТОЛЬКО ПО РАЗРЕШЕНИЮ КОМИССИИ СТУДЕНТ ОТКРЫВАЕТ СВОЙ БИЛЕТ.**

При начале экзамена студент, приглашенный комиссией, предъявляет свое удостоверение личности.

Важно. Запрещается публиковать и отправлять обучающимся любые экзаменационные билеты перед началом экзамена.

Время выставления аттестационных баллов за устный экзамен-48 часов.

Итак:

1. Экзамен проводится по расписанию.

2. Студенты и преподаватель должны заранее знать дату и время экзамена.

3. Разместить в системе Univer итоговый экзаменационный документ по дисциплине.

4. До начала экзамена студентам проводится предварительная консультация.

5. Председатель экзаменационной комиссии разъясняет требования экзамена.

6. Баллы, набранные студентами в течение 48 часов, выставляются в аттестационной ведомости.

Политика оценки. Критериальное оценивание: оценка результатов обучения в соответствии с дескрипторами (проверка формирования компетенций на экзаменах с промежуточным контролем).

#### **Политика оценивания:**

**Критериальное оценивание:** оценка результатов обучения в соответствии с дескрипторами, проверка сформированности компетенций (результатов обучения) на промежуточном контроле и экзаменах.

Оценка экзаменационных ответов производится по 100-балльной шкале, с учетом степени полноты ответа обучающегося:

Оценка	Критерии
Отлично	1.Даны правильные и полные ответы на все теоретические вопросы; 2.Полностью решено практическое задание; 3.Материал изложен грамотно с соблюдением логической последовательности; 4.Продемонстрированы творческие способности.
Хорошо	1. Даны правильные, но неполные ответы на все теоретические вопросы, допущены несущественные погрешности или неточности; 2.Практическое задание выполнено,однако Допущен незначительная ошибка; 3.Материал изложен грамотно с соблюдением логической последовательности.
Удовлетворительно	1.Ответы на теоретические вопросы в принципе правильные, но неполные, допущены неточности в формулировках и логические погрешности; 2.Практическое задание выполнено неполностью;
	3.Материал изложен грамотно,однако нарушена логическая последовательность.
Неудовлетворительно	1. Ответы на теоретические вопросы содержат грубые ошибки; 2. Практическое задание не выполнено; 3. В изложении ответа допущены грамматические, терминологические ошибки, нарушена логическая последовательность.

Оценка по квенной системе	Цифровой эквивалент	Баллы(%-ный показатель)	Оценка по Традиционной системе
A	4	95-100	Отлично
A-	3,67	94-90	
B+	3,33	85-89	Хорошо
B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	Удовлетворительно
C	2,0	65-69	
C-	1,67	60-64	
D+	1,33	55-59	
D-	1,0	50-54	
FX	0,5	25-49	Неудовлетворительно
F	0	0-24	

### Основные темы для подготовки к экзамену:

#### Тема 1. Введение в дисциплину. Понятие, цель, задачи финансово-цифровой среды

Юридические аспекты формирования и развития финансово-цифровой среды. Концепция комплексного правового регулирования цифровой

экономики. Международные соглашения в сфере регулирования финансово-цифровой среды.

## **Тема 2. Тенденции развития права и правовое регулирование отношений в финансово-цифровой среде.**

Объекты интеллектуальной собственности, используемые в цифровой экономике. Виды интеллектуальных прав, используемых в отношении по созданию и распространению информации в цифровой среде. Объекты интеллектуальных прав, охраняемые свидетельствами. Правовое регулирование отношений в цифровой среде.

## **Тема 3. Гражданско-правовое регулирование отношений при создании и распространении информации в Интернете. Исключительные права в цифровой сфере: объекты, границы, пределы осуществления.**

Государственная программа «Цифровой Казахстан». Виды информации, распространяемые в Интернете. Информация, которая запрещена для распространения в Интернете. Документы, регулирующие распространение информации в цифровой среде. Понятие и виды исключительных прав.

## **Тема 4. Основы нормативно-правового регулирования в сфере информационных технологий: технологии искусственного интеллекта, правовой режим нейросетей.**

Документы, регулирующие использование технологии искусственного Интеллекта. Виды искусственного интеллекта и основные проблемы правового регулирования некоторых направлений. Риски при использовании технологии искусственного интеллекта. Нейросети: понятие, классификация и правовое регулирование.

## **Тема 5. Правовое регулирование в сфере сбора, передачи, хранения, обработки, доступа к информации и обработки персональных данных.**

Персональные данные: определение, виды, правовые основания обработки персональных данных. Конфиденциальность информации: понятие, особенности регулирования, правила работы. Основные направления развития законодательства в сфере сбора, передачи, хранения, обработки и доступа к информации. Законодательство в сфере регулирования общественных отношений, связанных с обработкой персональных данных. Организации, регулирующие деятельность в сфере сбора, передачи, хранения, обработки и доступа к информации. Обезличивание персональных данных. Законодательство, устанавливающее режимы различных видов тайн ответственность за неправомерные действия в сфере сбора, передачи, хранения, обработки, доступа к информации и обработки персональных данных.

#### **Тема 6. Понятие и основные направления государственного регулирования цифровой экономики. Правовые условия для формирования единой финансово-цифровой среды доверия.**

Методы противодействия коррупции в условиях цифровой среды. Инструменты государственного регулирования. Формы государственной поддержки научной и инновационной деятельности. Структура механизма государственного регулирования процессов цифровизации в РК

#### **Тема 7. Информационная инфраструктура и безопасность.**

Создание глобальной конкурентоспособной инфраструктуры передачи, обработки и хранения данных. Внедрение цифровых технологий в строительстве и управлении городским хозяйством «Умный город». Риски в сфере информационной безопасности и пути их преодоления (повышение уровня защищенности личности, информационной безопасности и устойчивости сетей связи общего пользования; создание новых сервисов (услуг) для граждан, гарантирующих защиту их персональных данных; профилактика и выявление правонарушений с использованием информационных технологий, разработка новых механизмов поддержки отечественных разработчиков программного обеспечения и компьютерного оборудования в сфере информационной безопасности).

## **Тема 8. Цифровые технологии и право.**

Понятие и свойства сквозных цифровых технологий. Правовые предпосылки для развития приоритетных сквозных цифровых технологий (большие данные, технологии распределенного реестра, квантовые технологии, новые производственные технологии, промышленный интернет, робототехника и сенсорика, технологии беспроводной связи, виртуальная и дополненная реальность). Создание сквозных цифровых технологий (преимущественно на основе отечественных разработок) как одна из стратегических задач развития РК на период до 2025 года. Отраслевое регулирование правоотношений в сфере робототехники.

## **Тема 9. Электронный бюджет. Понятие, правовой статус и порядок функционирования.**

Электронный и цифровой бюджет, особенности формирования. Проектное бюджетирование как метод повышения эффективности государственных и местных расходов. Анализ процессов планирования и исполнения бюджета, процессы управления закупками, процессы сбора и анализа показателей социально-экономического развития региона.

## **Тема 10. Организация финансового контроля в условиях цифровизации финансовых правоотношений.**

Особенности организации финансового контроля с использованием современных информационно-коммуникационных средств. Налоговый мониторинг как одна из форм финансового контроля. Понятие цифровых правоотношений, контроль за соблюдением прав и законных интересов их субъектов. Контроль в сфере закупок для государственных и местных нужд с использованием единой информационной системы в сфере закупок.

## **Тема 11. Цифровая форма платежных средств и государственный финансовый контроль в цифровой среде. Особенности использования криптовалют.**

Денежные элементы цифровой экономики. Цифровые валюты в альтернативных платежных системах. Основные направления регулирования в сфере обращения цифровых финансовых активов и цифровой валюты. Цифровая форма законных платежных средств. Понятие и особенности использования криптовалют. Ответственность за неправомерные действия в сфере обращения цифровых финансовых активов и цифровой валюты.

### **Тема 12. Особенности договорного регулирования в условиях цифровой экономики.**

Понятие и система договоров в сфере цифровой экономики. Трансформация договорного права в условиях цифровой экономики. Технология блокчейн. Особенности заключения и исполнения договоров в цифровой среде. Договоры по созданию объекта инновации. Договоры по передаче в пользования объектов инновационной деятельности. Организационные договор.

### **Тема 13. Трудовые отношения в финансово-цифровой среде. Особенности использования смарт-контрактов. Проблемы ведения электронного документооборота.**

Особенности правового режима электронной цифровой подписи. Правовые основы введения электронных трудовых книжек. Применение смарт-контрактов и возможности правового регулирования их применения в финансово-цифровой среде. Право на забвение.

### **Тема 14. Правовые основы обеспечения и защиты прав в финансово-цифровой среде. "Цифровая" криминалистика.**

Трансформация судебной защиты прав в условиях цифровизации. Правовые условия судопроизводства и нотариата в цифровой среде. Создание и функционирование единой информационной системы нотариата. Основные направления развития законодательства об альтернативных механизмах онлайн урегулирования споров в цифровой среде. Правовые условия процедуры медиации. Применение «цифровой» криминалистики.

## **Тема 15. Уголовно-правовая охрана отношений, возникающих в связи с развитием финансово-цифровой среды.**

Классификация преступлений с использованием цифровых технологий. Способы защиты от уголовно-правовых рисков для граждан и организаций. Основные угрозы в цифровой сфере. Ответственность за правонарушения, связанные с использованием цифровых технологий. Превентивные меры в борьбе с уголовными преступлениями.

**При подготовке к экзамену студенту рекомендуется изучить следующие НПА и литературу:**

1. Цифровая экономика. Учебное пособие/ М.М. Ковалев, Г.Г. Головенчик. – Минск: Изд. центр БГУ, 2018. – 328 с.
2. Кулумбетова Д.Б., Маулина Н.Х., Асанова А.Б. Цифровая трансформация казахстанского банковского сектора на современном этапе развития //Научный вестник: Финансы, банки, инвестиции № 3. 2021.
3. Касенова Г.Е. Современные финансовые услуги банков: учебное пособие /Қазақ Университеті- Алматы, 2021, 264с.
4. Глоссарий по цифровым финансовым услугам. Совместная публикация Всемирного почтового союза и Международного союза электросвязи. 2017 // <https://creativecommons.org/licenses/by-nc-sa/4.0/>
5. Цифровая трансформация финансовых услуг: модели развития и стратегии для участников отрасли. SKOLKOVO Business School – Ernst & Young Institute for Emerging Market Studies (IEMS) // <https://www.skolkovo.ru>.
6. Новикова Е.А. Цифровизация финансового сектора: новые инструменты и перспективы их использования: Материалы конференции «Право, экономика и управление: от теории к практике». Чебоксары, 2020г.
7. Касенова Г.Е. Финансовые риски: учебное пособие /Қазақ Университеті- Алматы, 2020, 264с.

8. Государственная программа "Цифровой Казахстан" от 12 декабря 2017 года // <https://adilet.zan.kz/rus/docs/P1700000827>

**Дополнительная:**

1. Закон Республики Казахстан «О введении национальной валюты Республики Казахстан» от 12 ноября 1993г. // <https://online.zakon.kz>
2. Закон Республики Казахстан «О Национальном Банке Республики Казахстан». от 30 марта 1995 № 2155 (с доп.и изм. 03.03.2023г.) // <https://online.zakon.kz>
3. Закон Республики Казахстан «О банках и банковской деятельности в Республики Казахстан» от 31августа 1995. № 2444 (с доп.и изм. 03.03.2023г.). // <https://online.zakon.kz>
4. Закон Республики Казахстан от 4 июля 2003 года № 474-ІІ «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» (с доп.и изм. по состоянию на 12.09.2022 г.)
5. Закон РК от 24 мая 2021 года № 43-VІІ «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам регулирования банковской, микрофинансовой и коллекторской деятельности в РК», (с изм. и доп. по состоянию на 03.03.2023 г.) // <https://online.zakon.kz>
6. Концепция развития Open API и Open Banking в Республике Казахстан на 2023–2025 годы // <https://www.nationalbank.kz/>
7. Бюро национальной статистики. Информационный бюллетень. Проект Kazstat // <https://new.stat.gov.kz/ru/>.
8. Концепции развития Open API и Open Banking// <https://www.nationalbank.kz/>
9. Исследования Международного финансового центра «Астана» // <https://aifc.kz/ru/>
- 10.Краткий отчет Mobile banking rank Казахстан 2022 // <https://markswebb.ru/report/mobile-banking-rank-kz-2022/>
11. Концепция развития финансового сектора Республики Казахстан до 2030 года от 26 сентября 2022 года // <https://adilet.zan.kz/rus/docs/U2200001021>

**Интернет-ресурсы:**

1. Официальный сайт НБРК // <http://www.nationalbank.kz>
2. Официальный сайт Агентства РК по регулированию и развитию финансового рынка // <https://www.gov.kz>
3. Официальный сайт Казахстанской фондовой биржи KASE // <http://www.kase.kz>
4. Аналитические дэшборды // [Ranking.kz](http://Ranking.kz)
5. Аналитический портал // <https://kapital.kz/finance>

## РУБРИКАТОР КРИТЕРИАЛЬНОГО ОЦЕНИВАНИЯ ИТОГОВОГО КОНТРОЛЯ

Дисциплина: Актуальные проблемы финансового права.

Форма: устный (оффлайн) . Платформа: ИС Univer .

№	Критерий	Балл	ДИСКРИПТОРЫ				
			«Отлично»	«Хорошо»	«Удовлетворительно»	«Неудовлетворительно»	
			90-100%	70-89%	50-69%	25-49%	0-24%
1	Понимание сущности и проблем финансово-цифровой среды  <b>11 балл</b>	Полное понимание тенденций формирования финансово-цифровой среды. Релевантные и уместные ссылки (цитаты) на первоисточники.	Понимает основные проблемы развития финансово-цифровой среды. Релевантные и уместные ссылки (цитаты) на первоисточники.	Среднее понятие проблем развития финансово-цифровой среды. Релевантные и уместные ссылки (цитаты) на первоисточники.	Ограниченное понимание проблем развития финансово-цифровой среды. Релевантные и уместные ссылки (цитаты) на первоисточники.	Поверхностное понимание/ непонимание развития проблем финансово-цифровой среды. Соответствующие и уместные ссылки (цитаты) на первоисточники не приводятся.	
	Понимание актуальных проблем развития финансово-цифровой среды  <b>11 балл</b>	Очень хорошо анализирует законодательство Республики Казахстан, регулирующего финансовые	Связывает проблемы финансово-цифровой среды с пробелами законодательства	Ограниченная связь между теоретическими и практическими проблемами финансово-цифровой среды и их ограниченное использование.	Слабое сравнение законодательства Республики Казахстан в сфере цифровых технологий с зарубежными	Очень плохое сравнение законодательства в сфере цифровых финансов Республики Казахстан с	

		отношения в сфере цифровой экономики. Идеальное обоснование аргументов фактами эмпирического исследования (например, на основе сравнительного правового или статистического анализа).	Республики Казахстан. Подкрепляет аргументы фактами эмпирического исследования.		нормативными правовыми актами. Ограниченное использование доказательств эмпирических исследований.	зарубежными нормативными правовыми актами. Мало или совсем не использует эмпирические исследования.
	Политическое предложение или практические рекомендации / предложения <b>11 балл</b>	Составление грамотных научных и/или практических рекомендаций и рекомендаций, связанных с решением проблем финансово-цифровой среды в Казахстане.	Предлагает некоторые соображения и/или практические рекомендации и предложения по решению проблем финансово-цифровой среды в Казахстане	Ограниченные практические рекомендации. Рекомендации поверхностны, не основаны на тщательном анализе и не критичны.	Практических рекомендаций мало или вообще нет, либо рекомендации очень низкого качества.	Соображений и практических рекомендаций, связанных с решением проблем финансово-цифровой среды в Казахстане, мало или совсем нет, или рекомендации очень низкого качества
2	понимать концепции с помощью теории <b>11 балл</b>	Дано общее понятие основных	Раскрыто содержание теоретические	Рекомендации поверхностны, не основаны на тщательном анализе	Предлагаемые рекомендации относительно	практических рекомендаций, связанных с

		концепций развития финансово-цифровой среды	концепций проблем финансово-цифровой среды		концепций очень низкого качества	теоретическими концепциями проблем финансово-цифровой среды в Казахстане очень мало
	понять основные вопросы <b>11 балл</b>	Предлагает некоторые рекомендации относительно постановки и актуализации проблем развития финансово-цифровой среды	Дано общее понятие существующих проблем развития финансово-цифровой среды	Раскрывает содержание актуальных практических проблем развития финансово-цифровой среды без учета их связи с постановлениями Верховного суда РК	Умеренно раскрыты основные теоретические вопросы	Плохо раскрыты основные вопросы проблем развития финансово-цифровой среды
	предложение или практические предложения/рекомендации <b>11 балл</b>	Очень хорошо сравнивает финансовое законодательство Республики Казахстан относительно его гармонизации с международно-правовыми нормами	Подкрепляет аргументы фактами эмпирического исследования	Хорошо демонстрирует ясность, точность и правильность в понимании проблем финансово-цифровой среды	Ограниченное использование доказательств эмпирических исследований	Мало или совсем не использует эмпирические исследования.
3	понимать концепции с помощью теории развития финансово-цифровой среды <b>11 балл</b>	Идеальное обоснование аргументов фактами	Очень хорошо обосновывает аргументы	Хорошо связывает проблемы развития финансово-цифровой среды с действительностью	Ограниченное использование доказательств теории развития	Совсем не использует практические данные

		эмпирического исследования			финансово-цифровой среды	
понять основные вопросы <b>11 балл</b>	Идеальное аргументирование основных вопросов	Хорошо связывает проблемы развития финансово-цифровой среды с научными достижениями.	Ограниченное использование доказательств	Данные ответы не соответствуют содержанию вопросов.	Основные ответы очень низкого качества.	
устно, стиль, грамотность речи <b>12 балл</b>	Устно демонстрирует ясность, точность и аккуратность в формулировании и раскрытии содержания вопросов. Строго придерживается APA style.	Устно демонстрирует ясность и точность раскрытия содержания вопросов. В основном придерживается APA style.	Имеются некоторые основные ошибки в формулировании ответов и необходимо улучшить качество ответов. Есть ошибки в следовании APA style.	Ответы являются не полными и не аргументированными	Ответы являются недостоверными. Есть много ошибок в следовании APA style.	

Формула расчета итоговой оценки:

+Итоговая оценка (КБ) = (B1+B2+B3+B4+B5+B6+B7+B8+B9+B10) / 6К, здесь Б — балльный критерий, К — общий критерий оценки.

**Пример подсчета итогового балла**

№	Критерий	Балл	«Отлично»	«Хорошо»	«Удовлетворительно»	«Неудовлетворительно»	
			90-100%	70-89%	50-69%	25-49%	0-24%
1.	1 Критерий	100					
2.	2 Критерий			75			
3.	3 Критерий				60		
4.	4 Критерий					45	
5.	5 Критерий	100					
6.	6 Критерий					49	
	<b>Итого %</b>	<b>200</b>	<b>75</b>	<b>60</b>	<b>94</b>	<b>200+ 75 + 60 + 94 = 429</b>  <b>429 / 6 критерий = 71,5</b>  <b>Итого балл в % = 72</b>	

На основе процента, полученного при расчете, мы можем сравнить цену со шкалой оценок.

72 балла от 70 до 89 баллов соответствует категории «Хорошо» по шкале оценок.

Таким образом, в данном расчете проект получит оценку «Хорошо», 72 балла по буквенно-рейтинговой системе оценки учебных достижений студентов, заменяющей традиционную рейтинговую шкалу и ECTS.