Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Тлисов Азамат Борисович
Должность: Директор Северо-Кавказского института - филиала РАНХиГС
Дата подписания: 25.12.2025 20:14:56
Уникальный программный ключ:
ac2df3a37f30cf89983b8fac4daa7e874c1d10ed

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Северо-Кавказский институт-филиал

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00D6F63EBCD061699092680962737E91ED
Владелец: Тлисов Азамат Борисович
Действителен: с 28.04.2025 до 22.07.2026

Директор института-филиала
А..Б. Тлисов
«28» февраля 2025 г.

УТВЕРЖДЕНА
ученым советом института-филиала
Протокол от «28» февраля 2025г. № 06

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

повышения квалификации

«Цифровая грамотность работника»

Пятигорск, 2025

Разработчики:

Кандидат экономических наук, доцент,
доцент кафедры экономики и финансового
права _____ Е.А. Акопян

Старший преподаватель кафедры правового
обеспечения деятельности органов власти _____ С.Р. Решетняк

Руководитель программы: _____ Е.А. Акопян

Руководитель структурного подразделения: _____ В.В. Браткова

_____ А.В. Манкиева

Дополнительная профессиональная программа рекомендована к утверждению и реализации на заседании ученого совета института-филиала «28» февраля 2025 г., протокол № 6.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ 4
1.1. Цель реализации 4
1.2. Нормативная правовая база 4
1.3. Планируемые результаты обучения....5
1.4. Категория слушателей....6
1.5. Формы обучения и сроки освоения 7
1.6. Период обучения и режим занятий....7
1.7. Документ о квалификации....7
2. СОДЕРЖАНИЕ ПРОГРАММЫ....7
2.1. Календарный учебный график 7
2.2. Учебный план....9
2.3. Содержание программы по модулям, разделам, дисциплинам или темам. 11
3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ....12
3.1. Кадровое обеспечение....12
3.2. Материально-техническое и программное обеспечение реализации программы 16
3.3. Учебно-методическое и информационное обеспечение программы 16
4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЕ ПРОГРАММЫ…….30

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации

Повышение квалификации для лиц, которым необходимо профессиональное развитие в части формирования цифровых компетенций, необходимых человеку для активного участия во всех сферах жизни цифрового общества и экономики, позволяющих использовать цифровые технологии безопасно и творчески для достижения целей, связанных с работой, учебой, досугом, социальной интеграцией и адаптацией к меняющимся условиям на рынке труда.

1.2. Нормативная правовая база

Дополнительная профессиональная программа повышения квалификации разрабатывалась на основании следующих нормативных документов:

1. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»// Собрание законодательства Российской Федерации от 31 декабря 2012 г. № 53 (часть I) ст. 7598
2. Приказ Минобрнауки России от 01 июля 2013 №499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (ред. от 15 ноября 2013) // Гарант: справочно-правовая система [Офиц. сайт]. URL: https://www.garant.ru/ (дата обращения: 15.12.2024).
3. Приказ Минтруда России от 14.09.2022 № 533н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей»» (Зарегистрировано в Минюсте России 14.10.2022 № 70515)» // [Электронный ресурс]. - Гарант: справочно-правовая система [Офиц. сайт]. URL: https://www.garant.ru/ (дата обращения: 15.12.2024).
4. «Общероссийский классификатор видов экономической деятельности» (утв. Приказом Росстандарта от 31.01.2014 (14-ст) (ред. от 07 ноября 2023) // Гарант: справочно-правовая система [Офиц. сайт]. URL: https://www.garant.ru/ (дата обращения: 15.12.2024).
5. Приказ Минздравсоцразвития РФ от 26.08.2010 №761н (ред. от 31 мая 2011) «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей работников образования» (ред. от 31 мая 2011) // Гарант: справочно-правовая система [Офиц. сайт]. URL: https://www.garant.ru/ (дата обращения: 15.12.2024).
6. Постановление Минтруда России от 21 августа 1998 №37 (ред. от 27 марта 2018) «Квалификационный справочник должностей руководителей, специалистов и других служащих» (ред. от 27 марта 2018) // Гарант: справочно-правовая система [Офиц. сайт]. URL: https://www.garant.ru/ (дата обращения: 15.12.2024).
7. Постановление Правительства РФ от 11 октября 2023 г. N 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».
8. Методические рекомендации по использованию электронного обучения, дистанционных образовательных технологий при реализации дополнительных профессиональных образовательных программ Министерства образования и науки Российской Федерации от 10 апреля 2014 №06–381 // Гарант: справочно-правовая система [Офиц. сайт]. URL: https://www.garant.ru/ (дата обращения: 15.12.2024).
9. Методические рекомендации по разработке основных профессиональных образовательных программ дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (утв. Минобрнауки России 22 января 2015 №ДЛ-1/05вн) // Гарант: справочно-правовая система [Офиц. сайт]. URL: https://www.garant.ru/ (дата обращения: 15.12.2024).
10. Приказ РАНХиГС от 22 сентября 2017 №01–6230 «Об утверждении положения о

применении в Академии электронного обучения. Дистанционных образовательных технологий при реализации образовательных программ».

11. Приказ РАНХиГС от 19 апреля 2019 №02–461 «Об утверждении локальных нормативных активов РАНХиГС по дополнительному профессионального образованию».

12. Приказ РАНХиГС от 13 августа 2021 г. №02–835 «Порядок разработки и утверждения в РАНХиГС дополнительных профессиональных программ профессиональной переподготовки, программ повышения квалификации» с изм. от 9 декабря 2024 г., утв. Приказом Ректора Академии № 02-2499.

1.3. Планируемые результаты обучения

Таблица 1

Планируемые результаты освоения программы повышения квалификации, качественное изменение которых осуществляется в результате обучения

Виды деятельности	Общепрофессиональные /профессиональные компетенции или трудовые функции (формируются и (или) совершенствуются) ПСК и ПК	Знания	Умения	Практический опыт
Информационно-аналитическая деятельность	ПК-1 способен осознано и ответственно использовать цифровые технологии в профессиональной, общественной и личной жизни.	Знает основные принципы цифровой экономики; знает основы этики и норм общения в цифровой среде; знаете основ информационной безопасности и способов защиты информации.	Умеет искать, анализировать и создавать информацию в цифровой среде; умеет создавать цифровой профиль.	Имеет навыки пользования интернетом и его сервисами, включая средства поиска информации, облачные хранилища и другие инструменты.
	ПК-2 Способен к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства	Знает основные принципы сбора информации по кибербезопасности и методы анализа разнородных данных для анализа проблем и принятия решений по кибербезопасности	Умеет решать задачи по отбору актуальной информации по кибербезопасности	Имеет навыки применения процедур анализа и принятия решений при решении задач по кибербезопасности
	ПКС-1 (С/02.7) - Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	Знает нормативные правовые акты в области защиты информации	Умеет анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия.	Имеет навыки Принятия решения о необходимости защиты информации, содержащейся в информационной системе; классификация информационной системы по требованиям защиты информации; определение угроз безопасности

Виды деятельности	Общепрофессиональные /профессиональные компетенции или трудовые функции (формируются и (или) совершенствуются) ПСК и ПК	Знания	Умения	Практический опыт
				информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; разработка модели угроз безопасности информации; разработка руководящих документов по защите информации в организации

1.4. Категория слушателей

а) граждане в возрасте 50 лет и старше, граждане предпенсионного возраста;

б) граждане, фактически осуществляющие уход за ребенком и находящиеся в отпуске по уходу за ребенком до достижения им возраста 3 лет;

в) женщины, не состоящие в трудовых отношениях и имеющие детей дошкольного возраста в возрасте от 0 до 7 лет включительно;

г) инвалиды;

д) граждане, обратившиеся в органы службы занятости в целях поиска работы;

е) безработные граждане, зарегистрированные в органах службы занятости;

ж) работники, находящиеся под риском увольнения, включая введение режима неполного рабочего времени, простой, временную приостановку работ, предоставление отпусков без сохранения заработной платы, проведение мероприятий по высвобождению работников;

з) граждане Украины и лица без гражданства, постоянно проживающие на территории Украины, которые получили удостоверение беженца или свидетельство о предоставлении временного убежища на территории Российской Федерации;

и) ветераны боевых действий, принимавшие участие (содействовавшие выполнению задач) в специальной военной операции на территориях Донецкой Народной Республики, Луганской Народной Республики и Украины с 24 февраля 2022 г., на территориях Запорожской области и Херсонской области с 30 сентября 2022 г., уволенные с военной службы (службы, работы);

к) лица, принимавшие в соответствии с решениями органов публичной власти Донецкой Народной Республики, Луганской Народной Республики участие в боевых действиях в составе Вооруженных Сил Донецкой Народной Республики, Народной милиции Луганской Народной Республики, воинских формирований и органов Донецкой Народной Республики и Луганской Народной Республики начиная с 11 мая 2014 г.;

л) члены семей лиц, указанных в подпунктах "и" и "к" настоящего пункта, погибших (умерших) при выполнении задач в ходе специальной военной операции (боевых действий), члены семей лиц, указанных в подпунктах "и" и "к" настоящего пункта, умерших после увольнения с военной службы (службы, работы), если смерть таких лиц наступила вследствие увечья (ранения, травмы, контузии) или заболевания, полученного ими при выполнении задач в ходе специальной военной операции (боевых действий);

м) молодежь в возрасте до 35 лет включительно, относящаяся к категориям:

граждан, которые со дня окончания военной службы по призыву не являются занятыми в соответствии с законодательством о занятости населения в течение 4 месяцев и более;

граждан, которые со дня выдачи им документа об образовании и (или) о квалификации не являются занятыми в соответствии с законодательством о занятости населения в течение 4 месяцев и более;

граждан, находящихся под риском увольнения (планируемых к увольнению в связи с ликвидацией организации либо прекращением деятельности индивидуальным предпринимателем, сокращением численности или штата работников организации, индивидуального предпринимателя и возможным расторжением трудовых договоров);

граждан, завершающих обучение по образовательным программам среднего профессионального или высшего образования в текущем календарном году (за исключением получивших грант на обучение или обучающихся по договорам о целевом обучении), обратившихся в органы службы занятости, для которых отсутствует подходящая работа по получаемой профессии (специальности) с уровнем образования СПО, бакалавр, специалист, магистр.

1.5. Формы обучения и сроки освоения

Форма обучения очно-заочная с применением ЭО и ДОТ. Общая трудоемкость дисциплин (модулей) – 72 ак. часа (с применением ЭО и ДОТ); количество академических часов, выделенных на лекционную часть – 16 ак. часов; на практическую работу слушателей – 18 ак. часа (с применением ДОТ); самостоятельную работу – 36 ак. часов, Итоговая аттестация проводится в форме итогового экзамена (эссе), в соответствии с учебным планом – 2 ак. часа с применением ЭО.

1.6. Период обучения и режим занятий

Продолжительность обучения составляет 9 дней очно по 8 часов в день (по утвержденному графику).

1.7. Документ о квалификации

Удостоверение о повышении квалификации федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», установленного образца.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Календарный учебный график

Таблица 2

Период обучения – 9 дней				
1 день	2 день	3 день	4 день	5 день
УЗ ДОТ, СР	УЗ ДОТ, СР	УЗ ДОТ, СР	УЗ ДОТ, СР	УЗ ДОТ, СР
6 день	7 день	8 день	9 день	
УЗ ДОТ, СР	УЗ ДОТ, СР	УЗ ДОТ, СР	УЗ ДОТ, ИА ЭО	

Условные обозначения: УЗ ДОТ– учебные занятия с применением дистанционных образовательных технологий; СР – самостоятельная работа; ИА ЭО – итоговая аттестация с применением электронного обучения.

2.2. Учебный план

Таблица 3

Учебный план

№п/п[1]	Наименование (модуля/раздела/дисциплины/темы), практики (стажировки)[2]	Общая трудоемкость, час.[3]	Контактная работа, час.[4]					Самостоятельная работа, час[7]	Контактная работа (с применением дистанционных образовательных технологий, электронного обучения), час.[6]					Самостоятельная работа, час[7]	Текущий контроль успеваемости[8]	Промежуточная аттестация (форма/час)[9]	Итоговая аттестация (вид /час.)[10]	Код компетенции[11]
			Всего[4]	В том числе					Всего[4]	В том числе								
				Лекции / в интерактивной форме[5]	Лабораторные занятия (практикум) /в интерактивной форме[5]	Практические (семинарские) занятия /в интерактивной форме[5]	Контактная самостоятельная работа, час[7]			Лекции/ в интерактивной форме[5]	Лабораторные занятия (практикум) /в интерактивной форме[5]	Практические (семинарские) занятия /в интерактивной форме[5]	Контактная самостоятельная работа, час7					
1.	2	3	4	5	6	7	8	9	10	11	12	13	14	16	17	18	19	20
1	Цифровая грамотность как конкурентное преимущество в условиях становления цифровой экономики	**8**							**4**	2		2		4				ПК-1
2	Технология больших данных								**4**	2		2		4				ПК-1
3	Управление данными в государственном секторе	**10**							**6**	2		4		4				ПК-1
4	Этика и цифра	**8**							**4**	2		2		4				ПК-1
5	Управление цифровой репутацией	**10**							**6**	2		4		4				ПК-1
6	Приоритетная роль правового обеспечения информационной безопасности при построении глобального информационного общества	**6**							**2**	2				4				ПК-2
7	Нормативно-правовая основа обеспечения информационной безопасности	**6**							**2**			2		4				ПК-2
8	Современные проблемы в сфере информационной безопасности в Российской Федерации	**8**							**4**	2		2		4				ПК-2
9	Правовые основы защиты персональных данных	**6**							**2**	2				4				ПК-2

	Итого:	**70**							**34**	16		18		36				
	Итоговая аттестация	**2**							2									
	Всего:	72							36	16		18		36			2	ПК-1, ПК-2

2.3. Содержание программы по модулям, разделам, дисциплинам или темам.

Таблица 4

Содержание дисциплин (модулей)

Номер темы (раздела)	Содержание темы (раздела)
Цифровая грамотность как конкурентное преимущество в условиях становления цифровой экономики	Понятие цифровой грамотности. Цифровые компетенции. Цифровая экономика: обзор базовых понятий, концепций, ключевые составляющие цифровой экономики. Реализация национального проекта «Цифровая экономика РФ», национальная программа «Экономика данных». Цифровая трансформация в отраслях экономики. Цифровые платформы. Технология 5G: особенности и преимущества использования.
Технология больших данных	Что такое Big Data. Как работает технология Big Data: сбор, хранение, обработка. Преимущества технологии Big Data. Где применяется аналитика больших данных. Использование Big Data в России и мире
Управление данными в государственном секторе	Данные как актив. Особенности государственных данных. Трудности в работе с государственными данными. Проблема качества данных. Безопасность и риски при работе с данными. Цифровые сервисы. Большие данные в государственном управлении. Основные типы и технологии искусственного интеллекта. Программа поддержки внедрений искусственного интеллекта. Применение искусственного интеллекта в государственном управлении. Системы распределенного реестра. Интернет вещей и цифровая прослеживаемость. Системы цифровой прослеживаемости и управления рисками. Цифровой двойник и цифровой профиль.
Этика и цифра	Дата-этика. Этика искусственного интеллекта. Этика интернета вещей. Приватность человека и защита его персональных данных. Отраслевая этика в контексте цифровых технологий: этика цифровых технологий в образовании, медицине, полиции. Цифровизация социальной сферы.
Управление цифровой репутацией	Понятие цифровой репутации, управление цифровой репутацией. Правила создания цифровой репутации. Цифровой профиль. Понятие «репутация». Репутация человека и репутация объекта или профессии. Кем создается цифровая репутация. Сетевой этикет.
Приоритетная роль правового обеспечения информационной безопасности при построении глобального информационного общества	Понятие кибербезопасности. Цели, задачи, функции кибербезопасности. Кибербезопасность в системе национальной и общественной безопасности. Приоритетная роль правового обеспечения информационной безопасности при построении глобального информационного общества.
Нормативно-правовая основа обеспечения информационной безопасности	Национально-правовые и международно-правовые основы обеспечения кибербезопасности. Система кибербезопасности. Субъекты и объекты кибербезопасности: правовые, организационные и информационно-технологические ресурсы. Основные направления обеспечения кибербезопасности. Государственные органы, обеспечивающие информационную безопасность. Стандарты информационной безопасности.
Современные проблемы в сфере информационной безопасности в Российской Федерации	Понятие и правовая оценка угроз кибербезопасности. Угрозы кибербезопасности в системе угроз национальной и общественной безопасности. Организация взаимодействия государственных и негосударственных структур в системе обеспечения кибербезопасности. Состояние и перспективы международного сотрудничества в обеспечении кибербезопасности. Обеспечение безопасности личности, общества и государства в условиях цифровой реальности.
Правовые основы защиты персональных данных	Нормативные правовые акты в области персональных данных. Некоторые особенности обработки персональных данных. Ответственность за нарушение закона о персональных данных.

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Кадровое обеспечение

Таблица 7

Сведения о профессорско-преподавательском составе и ведущих специалистах

Ф.И.О. преподавателя / ведущего специалиста	Специальность, присвоенная квалификация по диплому	Дополнительные квалификации	Место работы, должность, основное / дополнительное место работы	Ученая степень, ученое (почетное) звание	Стаж работы в области профессиональной деятельности / по дополнительной квалификации	Стаж научно-педагогической работы		Наименование преподаваемой дисциплины / темы (модуля), практики / стажировки (при наличии) по данной программе
						Всего	В том числе по преподаваемой дисциплине (модулю)	
1	2	3	4	5	6	7	8	9
Акопян Елена Александровна	Южно-Российский государственный технический университет (Новочеркасский политехнический институт), специальность - математические методы и исследование операций в экономике, квалификация - экономист-математик, 2000 г.	Организация электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ) в системе дистанционного обучения (СДО) № 08139-2023-У-КУ УМУ 22.03.2023	Северо-Кавказский институт-филиал РАНХиГС, доцент кафедры экономики и финансового права, кандидат экономических наук, доцент	Кандидат экономических наук, доцент	24 г.	24 л.	5 л.	Цифровая экономика. Управление данными в государственном секторе. Технология больших данных. Этика и цифра. Управление цифровой репутацией.
Решетняк Сергей Романович	ГОУ ВПО «Российский университет Дружбы народов» (филиал г. Ессентуки), специальность «Юриспруденция»,	Реформа гражданского законодательства. Особенности контрактной системы размещения заказов. Авторские и смежные права (№ 001693 УПК-РАНХиГС-27,	Северо-Кавказский институт-филиал РАНХиГС, старший преподаватель кафедры		15 л. 10 мес.	12 л. 6 мес.	2 г.	Приоритетная роль правового обеспечения информационной безопасности при построении глобального информационного

	квалификация «Юрист», 2008г.	01.06.2018) Основы методов проверки качества материалов онлайн-курсов для преподавателей, отвечающих за подготовку материалов онлайн-курсов (№ 001102 УПК-РАНХиГС-5626; 12.2018) Управление государственными и муниципальными закупками (№ 000051 УО-РАНХиГС-150. 26.04.2019) Использование СДО в образовательном процессе с применением электронного обучения и дистанционных образовательных технологий (ЭО и ДОТ) (№ 003529 УПК-РАНХиГС-27; 27.03.2020) Взаимодействие куратора практики с обучающимся инвалидом, в том числе с применением дистанционных технологий (№ 56158;	правового обеспечения деятельности органов власти					общества. Нормативно-правовая основа обеспечения информационной безопасности. Современные проблемы в сфере информационной безопасности в Российской Федерации. Правовые основы защиты персональных данных.

		30.04.2021) Актуальные технологии работы с молодежью в современном пространстве (№ 00741-2021-У-ЦКУ 30.06.2021) Инклюзивная политика и инклюзивная практика в вузе (№ 59566; 15.12.2021) Противодействие распространению экстремистской идеологии в образовательных организациях (№ И-450/21; 24.12.2021) Технологии адаптации и сопровождения обучающихся с инвалидностью и ОВЗ в вузе Управление государственными и муниципальными закупками (для преподавателей) (00244н-2024-У-ВШГУ, 19.07.2024) Электронная информационно-						

		образовательная среда образовательной организации (ЭИОС) Защита прав человека в современных условиях						

3.2. Материально-техническое и программное обеспечение реализации программы

Институт располагает специальными помещениями, представляющие собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения должны быть укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Института. В процессе обучения используются корпоративные аккаунты на платформе видеоконференцсвязи (Яндекс Телемост, МТС-Линк и др.).

3.3. Учебно-методическое и информационное обеспечение программы

Методические разработки по проведению текущего контроля успеваемости

Тема 1. Цифровая экономика (2 часа)

Практическая работа №1

Охарактеризуйте содержание следующего определения.

1. «Цифровая экономика — это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом формате, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг». Дайте свои предложения по трактовке данного понятия.

2. Некоторые ученые считают, что феномен стоимости как экономической категории в условиях цифровой экономики вообще перестанет существовать. «Стоимость потеряет свой социально-хаосный характер — и превратится в нестоимостной технологический счет-расчет, вполне и упорядоченный, которому как раз и предшествуют мошеннические игрища в те же криптовалюты». Такое категоричное суждение, на наш взгляд, не имеет пока теоретической посылки обоснования исключения данной категории из теоретико-прикладной формы обобщения экономики, хозяйственной и социальной деятельности.

Каково ваше отношение к данным суждениям?

3. «На наш взгляд, природа данного явления (цифровой экономики) зиждется на действии объективного экономического закона экономии общественно необходимых затрат труда и общественного времени, суть которого заключается в сокращении затрат труда и времени на производство товаров, работ и услуг по мере развития общественных формаций» (Сергеев Л. Экономическая природа содержательных положений цифровых платформ // Общество и экономика. 2020. № 3.).

Каково ваше отношение к данному утверждению?

Тема 2. Технология больших данных (2 часа)

Практическая работа №2

Контрольные вопросы:

1 Является-ли Big Data сквозной технологией цифровой экономики РФ?
2 Как изменили Big Data структуру и администрирование информационных систем?
3 Есть-ли Big Data в банковских информационных системах?
4 Источники Big Data?
5 Как формируются большие данные?

Тема 3. Управление данными в государственном секторе (4 часа)

Практическая работа №3

1 Рассмотрите модель государства, ориентированного на данные:



Раскройте содержание каждого аспекта, представленного в модели. При подготовке используйте примеры, представленные в источнике.

2. Каковы цели использования данных разными группами потребителей? Заполните таблицу.

Таблица 8

Цели использования данных

Потребителя данных	Представители группы	Цели использования государственных данных
Государство	Федеральные и региональные Органы исполнительной власти, муниципалитеты, органы законодательной власти, суды, правительство, президент, государственные институты развития, территориальные органы управления и др.	
Бизнес	Технологические компании, ИТ-стартапы, малый бизнес, ритейл, производство и др.	

Наука и образование	НИИ, вузы, аналитические агентства, частные лица, занимающиеся наукой и исследованиями, и др.	
Общество, СМИ, НКО	Общественные организации, СМИ и НКО как представители гражданского общества, специализирующиеся на обеспечении гражданского контроля деятельности государства, граждане (физические лица) и др.	

3. Каковы на Ваш взгляд проблемы низкого качества данных?

4. Ознакомьтесь со статьей и выполните задание: оцените уровень клиентоцентричности официального сайта органа МСУ в части удобства использования правовой базы, ответьте на вопросы из перечня ниже:

1. Вы сразу нашли раздел с правовыми актами на официальном сайте или для этого понадобились дополнительные клики и поиск во всех вкладках? Сколько секунд вам потребовалось?
2. Как выглядят тексты муниципальных правовых актов внутри раздела? Есть ли там актуализированные версии актов, то есть тексты МПА со всеми внесенными в них действующими изменениями?
3. Есть ли в разделе возможность создать поисковый запрос по ситуации?
4. Есть ли рубрикатор, который помогает найти акт по ситуации без его точных реквизитов и названия?
5. Адаптирован ли рубрикатор для обычного человека?
6. Содержание актов объясняется простым языком? Есть ли в рубриках разъяснительные материалы в виде схем, видеороликов, презентаций?

Практическая работа №4

Клиентоцентричный подход: как сделать муниципальный правовой акт понятным, удобным и доступным

Автор статьи - Светлана Гуркова, генеральный директор центра повышения квалификации муниципальных служащих «Компетенции и технологии», к. ю. н.

Федеральные чиновники поставили задачу внедрить клиентоцентричный подход в системе государственного и муниципального управления. Например, в июне 2021 года на Петербургском международном экономическом форуме была организована секция «Клиентоцентричное государство».

Муниципальные правовые акты — один из основных каналов коммуникации с населением. Они содержат правила поведения, которые людям приходится соблюдать. Правовые нормы, которые трудно понять и невозможно найти, раздражают граждан. Люди начинают сомневаться в профессионализме тех, кто написал МПА. Поэтому рекомендуем внедрить клиентоцентричный подход в деятельность разработчиков этих актов. Читайте в статье, как это сделать.

Зачем органу МСУ внедрять клиентоцентричный подход

Термин «клиентоцентричность» пришел в госуправление из маркетинга. Речь идет о способе коммуникации, при котором главное — это эффективное взаимодействие с человеком, уважение и понимание его нужд и интересов.

Клиентоцентричный подход предполагает, что служащие органа местной власти при взаимодействии с населением смотрят его глазами на все процессы в муниципалитете.

Противоположный подход, ставший уже привычным для органов местного

самоуправления, называют функциональным.

Пример 1. Гражданин прислал на электронную почту местной администрации обращение с одним коротким вопросом: планируется ли благоустройство дворовой площадки по его адресу?

Чиновники прислали ответ на трех листах с цитатами из законодательства и муниципальных правовых актов без четкого вывода в конце. Ответ содержит предложения длиной в полстраницы с причастными и деепричастными оборотами. Этот язык непонятен обычному человеку. Гражданин называет ответ отпиской и остается недоволен работой органов власти. Это типичный пример функционального подхода к взаимодействию с населением.

Внедрение клиентоцентричного подхода в работу органа МСУ поможет существенно повысить его авторитет, а также уровень доверия между обществом и властью.

Если вы решили внедрять клиентоцентричный подход в органе местного самоуправления, то функциональный придется исключить. Не стремитесь сделать это сразу везде. Рекомендуем для начала внедрить клиентоцентричный подход в какую-то одну сферу деятельности, потом — в другую. Когда придет первый опыт, распространять его на другие рабочие процессы или сферы будет легче.

Изучите целевую аудиторию и особенности ее восприятия

Важно не только изучить целевую аудиторию, но и сегментировать ее

Муниципальный правовой акт устанавливает правила поведения, которые всегда адресованы кому-либо. Если МПА нормативный, то он адресован неограниченному кругу лиц. При клиентоцентричном подходе лица, которые должны исполнять МПА, — это его целевая аудитория. Они будут клиентами для разработчиков проекта акта.

Разработчику важно определить целевую аудиторию МПА уже на стадии подготовки его проекта, продумать, как клиенты будут выполнять новые правила. При этом важно не только изучить целевую аудиторию, но и сегментировать ее, то есть разделить на группы по определенным критериям. У каждой группы свои особенности, которые нужно учесть при работе над проектом МПА.

Пример 2. Для порядка предоставления субсидий на озеленение дворов частью целевой аудитории будут получатели субсидии — лица, которые занимаются управлением МКД. Разработчику МПА нужно изучить этот сегмент и ответить на три вопроса.

1. Каковы особенности восприятия текста муниципального правового акта этой группой?

2. Будет ли им понятен МПА, написанный в бюрократическом стиле, с длинными предложениями и большим количеством причастных и деепричастных оборотов?

3. Будет ли данному сегменту удобно исполнять положения этого акта?

Другой частью целевой аудитории порядка субсидирования станут муниципальные служащие, которые предоставляют субсидию. У них будут иные особенности восприятия. Их тоже нужно выявить и учесть при подготовке проекта порядка.

При разработке проектов ориентируйтесь на три основные ценности МПА для целевой аудитории: его понятность, доступность и удобство исполнения. Расскажем об этом подробнее.

Сделайте муниципальные правовые акты понятными

Невнятно изложенные и запутанные правовые нормы невозможно исполнить. Поэтому понятность актов, которые устанавливают правила поведения, напрямую связана с их исполнением.

Непонятность муниципальных правовых актов бывает преодолимой и непреодолимой.

Преодолимая непонятность возникает, когда разработчики нарушают правила техники изложения правовых норм.

Пример 3. Муниципальный правовой акт содержит длинные предложения на полстраницы. Их можно понять, только если пару часов или даже дней потратить на их толкование. Например, нарисовать схемы, разбить правовые нормы на признаки, поискать судебную практику, проконсультироваться с юристом, посоветоваться с коллегой, изучить опыт других муниципалитетов. Но зачастую у правоприменителей на все это нет времени. В результате они просто не исполняют правовую норму, которую не поняли. Проблема всплывает только при проверке, проведенной контрольно-надзорным органом. Негативные последствия возникают не только у правоприменителей, но и у органов местного самоуправления.

Чтобы этого избежать, обучите своих сотрудников. Тех, кто пишет проекты МПА, — приемам их эффективной разработки. Тех, кто занимается исполнением этих актов, — технике толкования правовых норм. Также преодолимую непонятность можно устранить, если проводить разъяснительную работу. Перечислим инструменты, которые можно при этом использовать.

Видеоролики очень эффективны. Их использует, в частности, Центризбирком

1. Схемы. Хорошо составленные схемы облегчают задачу понимания текста большинству людей.

Например, блок-схемы хороши для различных процедурных муниципальных правовых актов — порядков, регламентов.

2. Иллюстрированные схемы.

3. Видеоролики, в том числе мультипликационные.

4. Текстовые разъяснения понятным языком.

5. Презентации в PowerPoint. Их цель — визуальное сопровождение информации. Основной принцип здесь: минимум текста, больше схем и иных иллюстраций. Презентацию, в которую скопирован текст мелким шрифтом, никто не будет смотреть.

Если целевая аудитория муниципального правового акта — сотрудники органа местного самоуправления, разместите схемы, разъяснения, презентации в локальной сети. Можно использовать их для подготовки раздаточных материалов к методическим семинарам. Текстовые и другие разъяснения оформите как методические рекомендации по применению МПА. Чтобы проверить результаты этой работы, включите вопросы на знание МПА в материалы для аттестации. А саму разъяснительную работу проводите в рамках подготовки к аттестации.

Если целевая аудитория МПА — население, то размещайте схемы, видеоролики и другие материалы в соцсетях и в СМИ, на официальном сайте муниципального образования, информационных досках.

Непреодолимая непонятность выражается в скрытых противоречиях между правовыми нормами, которые трудно выявить без должного уровня квалификации. О такой непонятности можно говорить, если нарушены четыре правила. Посмотрите их в таблице 9.

Таблица 9

Правила, нарушение которых приводит к непреодолимой непонятности МПА

Правило	Пример ошибки
Единообразное понимание юридических терминов	Вместо юридических понятий используются их синонимы
Единообразное использование юридических понятий	Одно и то же понятие используется несколько раз, но в разных значениях
Непротиворечивость	Явные коллизии, которые создают риск коррупции. Скрытые логические ошибки: например, не выверены соотношения юридических понятий
Ясность значения слов	Юридическое понятие введено, а его значение не раскрыто либо раскрыто через размытые признаки с неясным смыслом

Привлеките к разработке проекта МПА правоприменителей

Устранить такие дефекты правовой нормы можно только посредством внесения изменений в правовой акт или принятия нового правового акта.

Чтобы избежать непреодолимой непонятности МПА, обучите сотрудников, участвующих в разработке их проектов, правилам клиентоцентричного подхода.

Сделайте муниципальные правовые акты удобными для исполнения

Правило исполнимости МПА — главное среди всех правил клиентоцентричного подхода. На практике встречаются нормативные правовые акты, неисполнимые по своей природе в любых условиях. Зачастую так получается, когда правовые акты пишут далекие от практики люди. Например, юристы без участия правоприменителей или разработчики, которые не изучили целевую аудиторию МПА.

Пример 4. В муниципальном образовании приняли новый правовой акт. Он распространялся на ресурсоснабжающие организации. При этом разработчики не изучили целевую аудиторию и специфику ее работы. Когда ресурсоснабжающие организации столкнулись с этим МПА, выяснилось, что они не могут его исполнить из-за уже утвержденных планов-графиков и других нюансов работы. Пришлось срочно вносить в акт изменения. Поскольку он нормативный, быстро это сделать не удалось. Возникло множество неудобств для большого количества людей.

Чтобы избежать этих сложностей, тщательно изучайте целевую аудиторию МПА. Привлеките к разработке проекта правоприменителей. Совместно с ними спрогнозируйте все возможные нюансы исполнения акта еще до его принятия.

Сделайте доступными тексты муниципальных правовых актов в актуальной редакции

Если адресаты муниципального правового акта не знают о его существовании, они не смогут его исполнить. Та же проблема возникает, когда акт слишком сложно найти. В большинстве случаев документ приходится искать в газетной подшивке в библиотеке или на официальном сайте органа местного самоуправления.

С поиском на сайте, как правило, возникают проблемы. Все документы находятся в разделе вперемешку, без какого-либо рубрикатора. Функции поиска нет, а если даже она есть, то использовать ее неудобно. Чтобы найти МПА, не зная его точных реквизитов, необходимо последовательно открывать сотни документов за все годы работы органа МСУ. Даже гражданские юристы не в состоянии это сделать, не говоря об обычных людях.

Пример 5. Филиал крупной нефтяной компании срубил перед своим офисом две сухие елки, которые когда-то сам высадил. Оказалось, что эти деревья находились на территории общего пользования. Согласно муниципальным правилам благоустройства и административному регламенту, нужно было получать порубочный билет. Но эти два муниципальных правовых акта невозможно было найти на официальном сайте органа МСУ без их точных реквизитов. У компании не было намерения нарушить установленные правила. Ее юристы просто не знали о существовании этих норм, потому что не смогли их найти. Результатом стал судебный процесс, на который компания и чиновники потратили время.

Разместите на официальном сайте органа местного самоуправления ссылку на раздел с муниципальными правовыми актами так, чтобы его можно было легко найти. Обратите внимание на то, как часто информация в этом разделе обновляется.

Во многих муниципалитетах раздел с нормативными документами ведется формально. Даже если юрист знает реквизиты МПА, пользы это не приносит, поскольку на сайте висит неактуальная версия акта. Действующие и недействующие МПА на сайтах органов МСУ обычно не разделены. Это также неудобно для адресатов МПА.

Определите, кто в вашем органе местного самоуправления отвечает за наполнение информацией раздела с муниципальными правовыми актами. Предусмотрите в разделе функцию поиска. Она должна быть устроена так, чтобы документ можно было найти не только по его реквизитам, но и по ситуации.

Предусмотрите возможность поиска МПА не только по реквизитам, но и по ситуации

Пример 6. Человеку нужно снести аварийное дерево у себя во дворе. На официальном сайте в разделе с правовыми актами он находит рубрику «Типовые запросы». В ней есть подрубрика «Хочу снести дерево». Внутри подрубрики — информация о том, как надо действовать. Сначала выяснить, относится ли земля к территории МКД. Объясняется, где и как это можно сделать. Если земля не относится к территории дома, то какие правовые акты регулируют этот вопрос. Здесь же можно посмотреть:

- актуальные тексты этих актов;
- информацию о том, нужен ли порубочный билет;
- предупреждение о санкциях за нарушение правил.

Чтобы оценить уровень клиентоцентричности официального сайта органа МСУ в части удобства использования правовой базы, ответьте на вопросы из перечня.

Тема 4. Этика и цифра (2 часа)

Практическая работа №5

Таблица 10

Рассмотрите ситуации использования данных и определите, с какими недостатками они могут быть связаны.

Преимущества и недостатки использования данных

Преимущество	Ситуация с использованием данных	Недостаток
• Развитие прикладных наук (в частности, в сфере здравоохранения); • крупные и международные научные проекты (сейсмология, метеорология, добыча полезных ископаемых, космонавтика, исследования климатических изменений и т. п.)	Сбор и обработка больших данных	
• Персонифицированные сервисы; • новые продукты и услуги; • цифровые платформы	Аккумулирование данных у компаний	
• Безопасность общества; национальная безопасность; • сокращение времени на получение госуслуг; • открытые данные; • актуальная статистика для принятия государственных решений	Аккумулирование данных у государства, включая видеонаблюдение ›	
• Быстрое оказание услуг; • персонализация услуг и продуктов; • масштабное развитие прикладных наук (в частности, в сфере здравоохранения)	Передача данных для искусственного интеллекта	
• Общение и самовыражение в социальных сетях и других онлайн-ресурсах; › свобода слова; • новые виды СМИ	Пользовательские данные, размещенные в открытом доступе	

Контрольные вопросы:

1. Этика цифровых технологий в образовании.
2. Этика цифровых технологий в медицине.
3. Цифровизация социальной сферы: преимущества и этические риски.
4. Этика цифровых технологий в полиции.
5. «Умный» город: этические проблемы.
6. Права человека и цифровые технологии.
7. Приватность человека и защита его персональных данных.
8. Дискриминация и цифровое неравенство.
9. Рынок труда и риски безработицы в условиях перехода к цифровой экономике.
10. Этика Интернет-вещей.

Тема 5. Управление цифровой репутацией (2 часа)

Практическая работа №6

Практическая работа №7

Тема 6. Приоритетная роль правового обеспечения информационной безопасности при построении глобального информационного общества (2 часа)

Практическая работа №8

Контрольные вопросы

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
4. Дайте характеристику Федерального закона от 27 июля 2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации».

Задание: выбрать страну и изучить ее основные правовые документы об информационной безопасности, собрать материал о взаимном влиянии законодательства данной страны и мирового сообщества в сфере информационной безопасности.

Тема 7. Нормативно-правовая основа обеспечения информационной безопасности (2 часа)

Практическая работа №9

1. Изучить следующие нормативно-правовые документы (список не является окончательным):

- Конституция Российской Федерации
- Доктрина информационной безопасности (2016) стратегия национальной безопасности Российской Федерации (2015)
- Федеральные законы:
  - ФЗ «О безопасности» (2010)
  - ФЗ «О государственной тайне» (1993)
  - ФЗ «Об информации, информационных технологиях и о защите информации» (2006)
  - ФЗ «О персональных данных» (2006)
  - ФЗ «О техническом регулировании» (2002)
  - ФЗ «О коммерческой тайне» (2004)
  - ФЗ «Об электронной подписи» (2011)

Выделить понятия, относящиеся к сфере информационной безопасности, составить словарь важных терминов.

Подготовленный словарь должен содержать определения ключевых терминов с обязательным указанием источника.

Практическая ситуация 1

Используя основные положения части 4, главы 70 Гражданского кодекса РФ, решить ситуационную задачу.

Гражданин Смирнов А.В. создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием

«Albert 3D» и зарегистрировал на него свои права. 15.09.2019 этот гражданин заключил договор с компанией «MosTechnology» и передал свои имущественные права на

распространение своего программного продукта сроком на один год. После заключения договора компания «MosTechnology» распространила версию программы «Albert 3D» с предварительной модификацией данного программного продукта без ведома автора.

Вопрос: Имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова?

Ответ: согласно статьи №….

Тема 7. Современные проблемы в сфере информационной безопасности в Российской Федерации (2 часа)

Практическая работа №9

Практическое задание 1

Дано пять информационных объектов:

- компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия (отдел кадров);
- компьютер бухгалтера (бухгалтерия);
- личная банковская карта;
- школьный компьютер (компьютерный класс);
- компьютер – рабочая станция оператора (ТЭЦ).

Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами.

Обозначить источник каждой из приведенных угроз. Работу рекомендуется выполнять в таблице вида:

Таблица 1

Рекомендуемый вид таблицы

№ п/п	Наименование угрозы	Источник	Метод защиты от угрозы
Компьютер с конфиденциальной информацией о сотрудниках предприятия			
1.	…	…	…
Банковская карта			
1.	…	…	…
Компьютер бухгалтера			
1.	…	…	…
Компьютер в классе			
1.			
Рабочая станция оператора			
1.			

Практическое задание 2

Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников.

Цель: уведомление новых сотрудников о строгом выполнении требований по

обеспечению информационной безопасности и ответственности за их нарушение.

Контрольные вопросы

1. Что понимается под угрозой информации?
2. Перечислите основные виды угроз.
3. Какова классификация угроз информационной безопасности?
4. Что понимается под термином информационный объект?
5. Назовите источники угроз информационной безопасности.

Практическая ситуация 1

Используя статьи УК РФ, ответьте на вопросы после ознакомления с ситуацией.

Ситуация: А.Н. Иванов, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 780000 рублей.

Вопросы:

Какая статья УК РФ была нарушена?

Что послужило предметом преступления?

Какие неправомерные информационные действия были совершены А.Н. Ивановым?

Практическая ситуация 2: Фишинговая атака

Фишинговая атака — одна из самых распространенных угроз. Фишинговые атаки могут привести к утечке конфиденциальных данных и значительным финансовым потерям. Допустите реальный инцидент, когда сотрудники компании стали жертвами фишинговой атаки. Рассмотрите методы социальной инженерии, используемые злоумышленниками, и способы защиты от таких атак.

Для анализа этого кейса вам потребуется изучить, какие методы социальной инженерии использовали злоумышленники и как они смогли обмануть сотрудников компании. Укажите какие меры могли бы предотвратить инцидент и как можно улучшить защиту от фишинговых атак. Предложите защитные меры противодействия таким атакам.

Задания к практическому занятию по теме «Правовые основы защиты персональных данных»

Практическая ситуация 1: Утечка данных

Утечка данных может иметь серьезные последствия для компании. Утечка данных — это серьезная угроза, которая может привести к значительным финансовым потерям и ущербу для репутации компании. Допустите реальный инцидент, когда конфиденциальные данные были украдены из-за слабой защиты базы данных. Разбор включает анализ причин утечки и рекомендации по усилению безопасности.

Укажите какие уязвимости могли быть использованы злоумышленниками и какие методы они применяли для кражи данных. Какие меры могли бы предотвратить инцидент и как можно улучшить защиту базы данных.

Промежуточная аттестация по модулю 2

Тест:

Вопрос 1. Безопасность критической инфраструктуры – это:

А) безопасность государства от критики оппозиционных структур.

Б) защита информационных ресурсов, похищение которых может негативно отразиться на деятельности органов государственной власти.

В) защита компьютерных систем, сетей и других активов, о которой зависит экономическое благополучие, национальная и общественная безопасность государства.

Г) обеспечение информационной безопасности технико-технологической инфраструктуры предприятия.

Д) защита приоритетных ресурсов субъекта хозяйственной деятельности от информационных атак.

Вопрос 2. Фишинг – это:

А) хитрый прием ловли на удочку крупной рыбы с использованием интернета. Б) похищение крупных денежных средств со счетов высокооплачиваемых сотрудников частных компаний.

В) мошеннические манипуляции со счетами финансовых компаний.

Г) вид интернет-мошенничества, направленного на получение доступа к конфиденциальным данным пользователей – логинам и паролям.

Д) обман покупателей и заказчиков.

Вопрос 3. Кибербуллинг – это

А) мошенническая киберигра с шарами на основе правил игры в боуллинг для вымогательства денег.

Б) издевательство над человеком, психологическая травля с использованием интернет-технологий.

В) использование интернета для организации мошеннических действий.

Г) мошеннический прием в социальных сетях, направленный на знакомство с человеком для выманивания у него денежных средств.

Д) вид интернет-мошенничества, направленного на получение доступа к конфиденциальным данным

Вопрос 4. Форензика – это:

А) основанная на искусственном интеллекте методика исследования цифровых источников информации о киберугрозах.

Б) поиск и фиксация угроз кибербезопасности.

В) методика изобличения киберпреступников в совершении ими мошеннических манипуляций с финансовыми средствами.

Г) наука о раскрытии и расследовании преступлений, связанных с компьютерной информацией.

Д) криминалистическая теория о кибербезопасности.

Вопрос 5. Какой федеральный закон содержит правовую регламентацию устранения из интернет- пространства сюжетов, содержащих признаки киберпреступления:

А) Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

Б) Закон РФ от 11 марта 1992 г. № 2487-I «О частной детективной и охранной деятельности в Российской Федерации».

В) Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Г) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Д) Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Нормативные правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (с изменениями на 4 октября 2022 года) // Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.); Официальный интернет-портал правовой информации www.pravo.gov.ru, 06.10.2022, № 0001202210060013.
2. Кодекс РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 27.01.2023). // СЗ РФ. 2002. № 1 (ч. 1) Ст. 1 **(перв. текст)**
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.
4. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // Российская газета. 1993, 21 сентября.
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // [Электронный ресурс]. - Режим доступа: СПС КонсультантПлюс.
6. Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции» // [Электронный ресурс]. - Режим доступа: СПС КонсультантПлюс.
7. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // [Электронный ресурс]. - Режим доступа: СПС КонсультантПлюс.
8. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» // [Электронный ресурс]. - Режим доступа: СПС КонсультантПлюс.
9. Закон РФ от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» // Российская газета. 1992, 30 апреля.
10. Федеральный закон от 06.04.2011 № 64-ФЗ «Об административном надзоре за лицами, освобожденными из мест лишения свободы» // [Электронный ресурс]. - Режим доступа: СПС КонсультантПлюс.
11. Приказ Минтруда России от 14.09.2022 № 533н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей»» (Зарегистрировано в Минюсте России 14.10.2022 № 70515)» // [Электронный ресурс]. - Режим доступа: СПС КонсультантПлюс.

Основная литература

1. Горелов, Н. А. Развитие информационного общества: цифровая экономика : учебное пособие для вузов / Н. А. Горелов, О. Н. Кораблева. — Москва : Издательство Юрайт, 2023. — 241 с. — (Высшее образование). — ISBN 978-5-534-10039-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515661 (дата обращения: 23.06.2023).
2. Государство как платформа: Люди и технологии/ под ред. Шклярук М.С., — М: РАНХиГС, 2019 — с.111. [сайт].— URL: https://urait.ru/bcode/472188.
3. Декларация ценностей клиентоцентричности. Стандарт «Государство для людей». – Текст. Электронный ресурс. Официальный сайт Министерства экономического развития РФ. // https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/vnedrenie_novyh_principov_predostavleniya_uslug/ocenka_kachestva_gosuslug/
4. Доступность государственных цифровых сервисов. Исследование / под ред. О. В. Линник, К. А. Ткачевой, М. В. Тумановой. – М. : РАНХиГС, 2022. – 108 стр. [сайт]. — URL: https://cdto.ranepa.ru/sum-of-tech/materials/53
5. Калмыкова, С. В. Работа с таблицами в Microsoft Excel: учебно-методическое пособие для вузов / С. В. Калмыкова, Е. Ю. Ярошевская, И. А. Иванова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2022. — 136 с. — ISBN 978-5-507-44447-2. — Текст: электронный // Лань: электронно-библиотечная система. [сайт].— URL: https://e.lanbook.com/book/226487

6. Камолов, С. Г. Цифровое государственное управление : учебник для вузов / С. Г. Камолов. — Москва : Издательство Юрайт, 2023. — 336 с. — (Высшее образование). — ISBN 978-5-534-14992-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520044
7. Клиентоцентричный подход в государственном управлении: Навигатор цифровой трансформации / под ред. О. В. Линник, А. В. Ожаровского, М. С. Шклярук. — Москва: РАНХиГС при Президенте РФ, 2020. — 180 с. [сайт]. — URL: https://cx.cdto.ranepa.ru/CX_navigator_CDTO_RANEPA.pdf
8. Коршунов, М. К. Экономика и управление: применение информационных технологий: учебное пособие для вузов / М. К. Коршунов ; под научной редакцией Э. П. Макарова. — 2-е изд. — Москва: Издательство Юрайт, 2021. — 110 с. — (Высшее образование). — ISBN 978-5-534-07724-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/472188.
9. Лапина М. А. Информационное право: учебное пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция» / М. А. Лапина, А. Г. Ревин, В. И. Лапин; под редакцией И. Ш. Килясханов. — Москва: ЮНИТИ-ДАНА, 2017. — 335 с. — ISBN 5-238-00798-1. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/74890.html — Режим доступа: для авторизир. пользователей.

10. Обеспечение законности в сфере цифровой экономики : учебное пособие для вузов / А. О. Баукин [и др.] ; под редакцией Н. Д. Бут, Ю. А. Тихомирова. — Москва : Издательство Юрайт, 2023. — 250 с. — (Высшее образование). — ISBN 978-5-534-13931-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519761
11. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва: ЮНИТИ-ДАНА, 2017. — 287 с. — ISBN 978-5-238-02857-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/72444.html— Режим доступа: для авторизир. пользователей.

12. Основы цифровой экономики : учебник и практикум для вузов / М. Н. Конягина [и др.] ; ответственный редактор М. Н. Конягина. — Москва : Издательство Юрайт, 2023. — 235 с. — (Высшее образование). — ISBN 978-5-534-13476-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519464
13. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7) [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_328854/
14. Рогозин В. Ю. Информационное право: учебное пособие для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / В. Ю. Рогозин, С. Б. Вепрев, А. В. Остроушко. — Москва: ЮНИТИ-ДАНА, 2017. — 191 с. — ISBN 978-5- 238-02858-3. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/72440.html — Режим доступа: для авторизир. пользователей.
15. Сергеев, Л. И. Цифровая экономика : учебник для вузов / Л. И. Сергеев, Д. Л. Сергеев, А. Л. Юданова ; под редакцией Л. И. Сергеева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 437 с. — (Высшее образование). — ISBN 978-5-534-15797-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/509767.
16. Сергеев, Л. И. Цифровая экономика : учебник для вузов / Л. И. Сергеев, Д. Л. Сергеев, А. Л. Юданова ; под редакцией Л. И. Сергеева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 437 с. — (Высшее образование). — ISBN 978-5-534-15797-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543648

17. Управление данными в госсекторе. Навигатор для начинающих / под ред. О. М. Гиацинтова, В. А. Сазонова, М. С. Шклярук. – М. : РАНХиГС, 2022. – 198 стр. [сайт]. — URL: https://cdto.ranepa.ru/media/reports/pdfs/Data_1_CDTO_RANEPA_.pdf
18. Этика и «цифра»: от проблемк решениям/ подред. Е. Г.Потаповой, М. С. Шклярук. — М.: РАНХиГС, 2021. — 184 с. [сайт]. — URL: https://cdto.ranepa.ru/reports/ethics/2021/

Дополнительная литература

1. Кармановский Н. С. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — Санкт-Петербург : Университет ИТМО, 2016. — 169 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/67452.html— Режим доступа: для авторизир. пользователей.
2. Качество цифрового образования 2022-2030. Материалы вебинаров, бесед и исследований Юрайт. Академии. Выпуск 6. Летняя школа преподавателя 2022 / О. А. Серова [и др.] ; под общей редакцией Н. В. Рыбкиной ; под редакцией А. О. Стрельниковой, А. А. Сафонова, Э. Т. Кокой. — Москва : Издательство Юрайт, 2023. — 129 с. — (Юрайт.Академия). — ISBN 978-5-534-15752-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520585.
3. Кубанков, А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект : учебное пособие / А. Н. Кубанков, Н. Н. Куняев ; под редакцией А. В. Морозов. — Москва : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. — 78 с. — ISBN 978-5-89172-850-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/47262.html Режим доступа: для авторизир. пользователей.
4. Прохоров А., Коник Л. Цифровая трансформация. Анализ, тренды, мировой опыт. Издание второе, исправленное и дополненное./А. Прохоров, Л. Конник — М.: ООО «КомНьюс Груп», 2019 — 368 стр., ил.
5. Сибел, Т. Цифровая трансформация: как выжить и преуспеть в новую эпоху. Пер. с англ. Ю. Гиматовой; под науч. ред. М. Савицкого и др.; предисл. Г. Грефа./ Т. Сибел. – М.: Манн, Иванов и Фербер, 2021. – 253 с.
6. Сологубова, Г. С. Составляющие цифровой трансформации : монография / Г. С. Сологубова. — Москва : Издательство Юрайт, 2023. — 147 с. — (Актуальные монографии). — ISBN 978-5-534-11335-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/517151 (дата обращения: 23.06.2023).
7. Цифровая экономика: 2022 : краткий статистический сборник / Г. И. Абдрахманова, С.А. Васильковский, К.О. Вишневский и др.; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2022. – 124 с. – 300 экз. – ISBN 978-5-7598-2599-9 (в обл.). Текст: электронный // URL: file:///C:/Users/User/Downloads/552091260.pdf.
8. Шибаев Д. В. Информационное право: практикум по курсу / Д. В. Шибаев. — Саратов: Ай Пи Эр Медиа, 2017. — 277 с. — ISBN 978-5-4486-0016-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/67340.html — Режим доступа: для авторизир. пользователе

Интернет – ресурсы

1. Официальный сайт Министерства экономического развития РФ: https://www.economy.gov.ru/
2. Официальный сайт Государственной думы Российской Федерации [Электронный ресурс]. – Режим доступа: http://wbase.duma.gov.ru
3. Официальный сайт Министерства финансов Российской Федерации [Электронный ресурс]. – Режим доступа: http:// www.mi№fi№.ru
4. Официальный сайт Федеральной службы государственной статистики Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.gks.ru

5. Электронно-библиотечная система «IPRbooks» [Электронный ресурс]. – Режим доступа: http://www.iprbookshop.ru/
6. Электронно-библиотечная система издательства «Лань» [Электронный ресурс]. – Режим доступа: https://e.la№book.com/
7. Электронно-библиотечная система издательства ЮРАЙТ [Электронный ресурс]. – Режим доступа: https://www.biblio-o№li№e.ru/

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Итоговая аттестация проводится в форме эссе на тему «Реалии и перспективы цифрового государственного управления».

«Значение информации, способов доступа к ней и защиты в условиях формирования цифрового государства»

Методические рекомендации по написанию эссе

Эссе - самостоятельная творческая письменная работа, по форме эссе обычно представляет собой рассуждение – размышление (реже рассуждение – объяснение), поэтому в нём используются вопросно-ответная форма изложения, вопросительные предложения, ряды однородных членов, вводные слова, параллельный способ связи предложений в тексте.

Цель эссе состоит в развитии навыков самостоятельного творческого мышления и письменного изложения собственных мыслей.

Особенности эссе:

- наличие конкретной темы или вопроса;
- личностный характер восприятия проблемы и её осмысления;
- небольшой объём;
- свободная композиция;
- непринуждённость повествования;
- внутреннее смысловое единство;
- афористичность, эмоциональность речи.

Требования к эссе:

1. Объем эссе не должен превышать 1–2 страниц (без учета списка использованных источников)
2. Эссе должно восприниматься как единое целое, идея должна быть ясной и понятной.
3. Необходимо писать коротко и ясно. Эссе не должно содержать ничего лишнего, должно включать только ту информацию, которая необходима для раскрытия вашей позиции, идеи.
4. Эссе должно иметь грамотное композиционное построение, быть логичным, четким по структуре.
5. Каждый абзац эссе должен содержать только одну основную мысль.
6. Эссе должно показывать, что его автор знает и осмысленно использует теоретические понятия, термины, обобщения, мировоззренческие идеи.
7. Эссе должно содержать убедительную аргументацию заявленной по проблеме позиции.

Список использованных источников указывается в конце текста.

Система оценки в ходе итоговой аттестации в форме эссе

Оценка	Требования к знаниям
зачтено	1. Материал изложен полно, даны правильные определения основных понятий 2. Слушатель обосновывает свои суждения, умозаключения и

	выводы, связывая с практикой 3. Материал изложен последовательно и грамотно с точки зрения стандартов в области оценки и норм литературного языка
не зачтено	Материал не подготовлен или подготовлен с существенными нарушениями.