

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Дмитрий Александрович
Должность: директор Юридического института
Дата подписания: 18.06.2026 13:44:09
Уникальный программный ключ:
9b20b9de2b80ed5232cec32f2c1771c09e23b783

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Директор юридического института
д.ю.н., профессор
Д.А. Смирнов

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Цифровой суверенитет и кибербезопасность:
правоприменительные аспекты»

Направление подготовки	40.04.01 Юриспруденция
Направленность (Профиль)	Юрист в сфере правоприменительной и экспертно-аналитической деятельности
Год начала обучения	2026
Форма обучения	заочная
Реализуется в семестре	4

Введение

1. Фонд оценочных средств обеспечивает объективный контроль достижения запланированных результатов обучения по дисциплине «Цифровой суверенитет и кибербезопасность: правоприменительные аспекты» студентов, обучающихся по направлению 40.04.01 «Юриспруденция», профиль «Юрист в сфере правоприменительной и экспертно-аналитической деятельности».
2. ФОС является приложением к программе дисциплины (модуля) «Цифровой суверенитет и кибербезопасность: правоприменительные аспекты»
3. Разработчики: Зав. кафедрой теории и истории государства и права, к.ю.н. доцент Мельникова В.А, старший преподаватель Тер-Аванесова И.Н.
4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Мельникова Виктория Анатольевна, к.ю.н., доцент, зав. кафедрой теории и истории государства и права.

Члены комиссии:

Лаута Олег Николаевич, к.и.н., доцент кафедры теории и истории государства и права Тер-Аванесова Ирина Николаевна, старший преподаватель кафедры теории и истории государства и права

Представитель организации-работодателя:

Диреганова А.В. Первый заместитель главы администрации города Ставрополя, канд. юрид. наук.

Экспертное заключение: представленные в данном ФОС оценочные средства позволяют определить уровень сформированности компетенций и соответствия результатов обучения задачам будущей профессиональной деятельности у обучающихся по ОП ВО направления подготовки 40.04.01 Юриспруденция, направленности (профиля) «Юрист в сфере правоприменительной и экспертно-аналитической деятельности», разработанной на основе ФГОС ВО по направлению подготовки 40.04.01 Юриспруденция.

- 5.Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание показателей и критериев оценивания на различных этапах их формирования, описание шкал оценивания

Уровни сформированности компетенции(й), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>ПК-3 Способен участвовать в проведении юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции</i>				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-1 ПК 3 Определяет правовые основы и принципы обеспечения цифрового суверенитета Российской Федерации; характеризует международные стандарты и лучшие практики в области кибербезопасности; анализирует теоретические и практические проблемы регулирования критической информационной инфраструктуры (КИИ).	Не владеет информацией о правовых основах цифрового суверенитета РФ; не может охарактеризовать международные стандарты безопасности.	Демонстрирует общее представление о суверенитете; допускает ошибки при анализе проблем регулирования КИИ.	Верно характеризует стандарты и лучшие практики; допускает незначительные неточности в анализе теоретических проблем.	Глубоко анализирует практические аспекты регулирования КИИ; свободно оперирует международными стандартами.
Результаты обучения по дисциплине (модулю): Индикатор: ИД-2 ПК-3 Осуществляет классификацию цифровых рисков; выявляет особенности правоприменения в зависимости от уровня угроз и режимов обработки персональных данных; анализирует коррупционные факторы в нормативных актах, регулирующих государственные информационные системы.	Не способен классифицировать цифровые риски; не идентифицирует коррупционные факторы в ГИС.	Проводит классификацию рисков по шаблону; допускает неточности при определении режимов обработки данных.	Успешно выявляет особенности правоприменения ; испытывает затруднения при глубоком анализе факторов в актах ГИС.	Безошибочно анализирует коррупционные факторы; учитывает все уровни угроз при оценке правоприменения.
Результаты обучения по дисциплине	Не владеет навыками	Формулирует обоснование	Грамотно определяет	Демонстрирует высокий уровень

(модулю): Индикатор: ИД-3 ПК-3 Логически обосновывает необходимость принятия или изменения нормативного решения в сфере цифровизации, определяет последствия его реализации с учетом возможных коррупционных рисков; разрабатывает и оформляет проекты экспертных заключений с учетом правил юридической техники.	оформления экспертных заключений; не может логически обосновать нормативное решение.	поверхностно; нарушает правила юридической техники при оформлении проектов.	последствия реализации НПА; допускает отдельные огрехи в логике обоснования рисков.	владения юридической техникой; готовит безупречные экспертные заключения.
<i>ПК-4 Способен выявлять и устранять признаки нарушений требований антимонопольного законодательства Российской Федерации</i>				
Результаты обучения по дисциплине (модулю): Индикатор: ИД-1 ПК-4 Формулирует основания, принципы и особенности антимонопольного регулирования цифровых рынков; определяет юридическую природу доминирующего положения цифровых платформ; анализирует теоретические и практические проблемы конкурентного права в условиях сетевых эффектов.	Не понимает специфику сетевых эффектов; не может определить природу доминирования платформ.	Описывает принципы регулирования в общих чертах; допускает неточности в определении статуса цифровых платформ.	Хорошо анализирует проблемы конкурентного права; допускает несущественные ошибки в оценке оснований регулирования.	Глубоко формулирует особенности антимонопольного права в цифре; свободно анализирует сетевые эффекты.
Результаты обучения по дисциплине (модулю): Индикатор: ИД-2 ПК-4 Классифицирует виды нарушений антимонопольного	Не владеет методикой квалификации нарушений (алгоритмическое ценообразование, блокировка API).	Классифицирует базовые нарушения; ошибается при оценке влияния цифровой зрелости рынка на	Верно выявляет особенности действий субъектов; допускает неточности при анализе сложных	Точно квалифицирует любые акты недобросовестной конкуренции с учетом всех рыночных

законодательства в цифровой среде; выявляет особенности квалификации действий (например, алгоритмического ценообразования, блокировки доступа к API) в зависимости от уровня цифровой зрелости рынка.		квалификацию.	алгоритмических схем.	факторов.
Результаты обучения по дисциплине (модулю): Индикатор: ИД-3 ПК-4 Аргументирует необходимость принятия мер реагирования ФАС России; прогнозирует последствия реализации антимонопольных предписаний; участвует в составлении и оформлении проектов исковых заявлений и представлении интересов в антимонопольных органах по вопросам кибербезопасности и доступа к инфраструктуре.	Не способен аргументировать меры реагирования; не владеет навыками составления исковых заявлений.	Прогнозирует последствия с ошибками; допускает значительные неточности при оформлении документов для ФАС.	Убедительно аргументирует необходимость мер ФАС; испытывает затруднения при защите интересов по вопросам КИИ.	Профессионально готовит исковые проекты; дает точный прогноз реализации антимонопольных предписаний.

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Семестр 4	
1.	Ж. Боден	Кто ввел в научный оборот термин «суверенитет»? А) Т. Гоббс Б) Ж. Боден В) Н. Макиавелли Г) Аристотель	ПК-3, ПК-4
2.	Вестфальский мир	Какое событие закрепило принцип территориального суверенитета в Европе? А) Великая французская революция Б) Венский конгресс В) Вестфальский мир Г) Подписание Устава ООН	ПК-3, ПК-4
3.	Верховенство	Какой признак суверенитета означает, что на территории государства не может существовать другой власти, равной или стоящей над властью государства? А) Неотчуждаемость Б) Постоянство В) Верховенство Г) Делимость	ПК-3, ПК-4
4.	Ж.-Ж. Руссо	В чьих трудах наиболее полно развита идея «народного суверенитета»? А) Дж. Локка Б) Ж.-Ж. Руссо В) Г. Гегеля Г) И. Канта	ПК-3, ПК-4
5.	Концепция делегированного суверенитета	Какая концепция суверенитета утверждает, что государство может добровольно ограничивать свои права в пользу международных организаций? А) Концепция делегированного суверенитета Б) Концепция абсолютного суверенитета В) Концепция изоляционизма Г) Теория общественного договора	ПК-3, ПК-4
6.	Инфраструктурный	Какой уровень цифрового суверенитета отвечает за контроль над серверами и кабелями связи? А) Информационный	ПК-3, ПК-4

		Б) Технологический В) Инфраструктурный Г) Контентный	
7.	Локализация	Как называется требование закона хранить персональные данные граждан РФ на серверах внутри страны? А) Глобализация Б) Локализация В) Индексация Г) Трансграничность	ПК-3, ПК-4
8.	Китай	Какая страна реализует модель «цифрового суверенитета» через жесткую систему фильтрации контента на национальном шлюзе? А) США Б) Германия В) Китай Г) Бразилия	ПК-3, ПК-4
9.	Технологическая зависимость	Какое понятие описывает ситуацию полной зависимости государства от иностранного программного обеспечения? А) Цифровая зрелость Б) Технологическая зависимость В) Сетевой эффект Г) Юрисдикционный иммунитет	ПК-3, ПК-4
10.	Требование открыть официальное представительство в РФ	В чем заключается суть «Закона о приземлении» ИТ-гигантов? А) Требование открыть официальное представительство в РФ Б) Запрет на использование иностранных поисковиков В) Обязательная передача исходных кодов программ государству Г) Требование снизить цены на рекламу для госорганов	ПК-3, ПК-4
11.	ФСТЭК	Какой орган в РФ осуществляет лицензирование деятельности по технической защите конфиденциальной информации? А) МВД Б) Минцифры В) ФСТЭК Г) Роскомнадзор	ПК-3, ПК-4
12.	Роскомнадзор	Согласно ФЗ о «суверенном интернете», кто осуществляет централизованное управление сетью общего пользования в случае угрозы?	ПК-3, ПК-4

		А) Роскомнадзор Б) ФСБ В) Правительство РФ Г) ПАО «Ростелеком»	
13.	Всеобъемлющая международная конвенция о противодействии использованию ИКТ в преступных целях	Какое международное соглашение Россия считает приоритетным для разработки под эгидой ООН? А) Будапештская конвенция Б) Парижский призыв к доверию в киберпространстве В) Всеобъемлющая международная конвенция о противодействии использованию ИКТ в преступных целях Г) Таллиннское руководство	ПК-3, ПК-4
14.	Государственные органы и организации, работающие в стратегически важных отраслях (здравоохранение, транспорт, связь и др.)	К субъектам КИИ относятся: А) Только государственные органы Б) Только компании с госучастием В) Государственные органы и организации, работающие в стратегически важных отраслях (здравоохранение, транспорт, связь и др.) Г) Все юридические лица РФ	ПК-3, ПК-4
15.	Национальная система доменных имен (НСДИ)	Какая информационная система, согласно законодательству о «суверенном интернете», обязательна для использования операторами связи и обеспечивает работу Рунета при невозможности подключения к зарубежным корневым серверам? А) Единая система идентификации и аутентификации (ЕСИА) Б) Национальная система доменных имен (НСДИ) В) Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) Г) Единый реестр запрещенных сайтов	ПК-3, ПК-4
16.	Установление юридической основы дела (выбор нормы)	Какая стадия правоприменения предшествует принятию решения по делу о киберпреступлении? А) Издание акта Б) Установление юридической основы дела (выбор нормы) В) Исполнение решения Г) Оглашение приговора	ПК-3, ПК-4
17.	ФСТЭК России	Какой орган исполнительной власти отвечает за выработку государственной политики в области технической защиты информации?	

		А) МВД РФ Б) Минцифры РФ В) ФСТЭК России Г) Роскомнадзор	
18.	Постановление суда о назначении штрафа за нарушение правил защиты КИИ	Что из перечисленного является актом правоприменения? А) Уголовный кодекс РФ Б) Постановление суда о назначении штрафа за нарушение правил защиты КИИ В) Должностная инструкция специалиста по ИБ Г) Статья в научном журнале о киберугрозах	
19.	Управление «К»	Какое подразделение МВД РФ специализируется на борьбе с преступлениями в сфере ИТ? А) ГИБДД Б) Главное управление по вопросам миграции В) Управление «К» Г) Управление по контролю за оборотом наркотиков	
20.	Обоснованность и соблюдение установленной процедуры	Какое требование является обязательным для законности правоприменительного акта в цифровой сфере? А) Опубликование в социальных сетях Б) Обоснованность и соблюдение установленной процедуры В) Написание кода программы в приложении к акту Г) Согласование с международными ИТ-корпорациями	
21.	Статья 273	Какая статья УК РФ устанавливает ответственность за создание вредоносных компьютерных программ? А) Статья 272 Б) Статья 273 В) Статья 159.6 Г) Статья 274.1	
22.	Дисциплинарная	К какому виду ответственности относится выговор за использование рабочего компьютера в личных целях в нарушение ЛНА? А) Административная Б) Гражданско-правовая В) Дисциплинарная Г) Уголовная	

23.	Лишение свободы на срок до 10 лет	Какое максимальное наказание предусмотрено ст. 274.1 УК РФ (ч. 5), если деяние повлекло тяжкие последствия? А) Штраф до 500 тыс. рублей Б) Обязательные работы В) Лишение свободы на срок до 10 лет Г) Лишение права занимать определенные должности на 1 год	
24.	Роскомнадзор	Какой орган уполномочен составлять протоколы по ст. 13.11 КоАП РФ (нарушение законодательства о персональных данных)? А) ФСБ России Б) Роскомнадзор В) ФСТЭК России Г) Налоговая служба	
25.	Своевременное принятие мер по удалению контента после уведомления правообладателя	Что является основанием для освобождения владельца сайта от ответственности за нарушение авторских прав пользователем (согласно ГК РФ)? А) Отсутствие прибыли от сайта Б) Своевременное принятие мер по удалению контента после уведомления правообладателя В) Наличие дисклеймера «Администрация не несет ответственности» Г) Использование зарубежного хостинга	
26.	10 рабочих дней	В течение какого срока субъект КИИ обязан направить сведения о результатах категорирования во ФСТЭК России? А) 3 рабочих дня Б) 5 календарных дней В) 10 рабочих дней Г) 30 календарных дней	
27.	ФСТЭК России	Какой федеральный орган исполнительной власти ведет Реестр значимых объектов КИИ? А) ФСБ России Б) Роскомнадзор В) ФСТЭК России Г) Минцифры России	
28.	Да, если она владеет информационной системой в сфере	Является ли частная клиника, имеющая лицензию на медицинскую деятельность, субъектом КИИ? А) Нет, КИИ — это только госсектор	

	здравоохранения	Б) Да, если она владеет информационной системой в сфере здравоохранения В) Только если в ней более 500 сотрудников Г) Только по решению губернатора региона	
29.	Нарушение условий международного договора РФ	Какое из перечисленного является показателем политической значимости объекта КИИ? А) Прямой экономический ущерб Б) Нарушение условий международного договора РФ В) Гибель людей Г) Прекращение подачи электроэнергии	
30.	Не реже одного раза в пять лет (или при изменении показателей)	С какой периодичностью субъекты КИИ должны проводить перекатегорирование объектов? А) Каждый год Б) Раз в 10 лет В) Не реже одного раза в пять лет (или при изменении показателей) Г) По требованию прокуратуры	
31.	Повышение уровня правовой и технической грамотности кадров	Что является приоритетным в стратегии формирования цифровой зрелости в РФ? А) Закупка самого дорогого оборудования Б) Полный отказ от интернета В) Повышение уровня правовой и технической грамотности кадров Г) Использование только бумажных носителей	
32.	Технологический нигилизм	Деформация правосознания, проявляющаяся в пренебрежении к отечественным ИТ-разработкам, называется: А) Кибертерроризм Б) Технологический нигилизм В) Цифровой суверенитет Г) Информационная гигиена	
33.	Доктрина информационной безопасности РФ	Какой документ является основой для формирования правовой культуры в сфере информационной безопасности в РФ? А) Уголовный кодекс (только он) Б) Устав ООН В) Доктрина информационной безопасности РФ Г) Лицензионное соглашение Windows	
34.	Обязательное использование	Цифровой суверенитет в правоприменении обеспечивается через: А) Случайный выбор ПО	

	программного обеспечения из Реестра отечественного ПО	Б) Обязательное использование программного обеспечения из Реестра отечественного ПО В) Использование любых бесплатных программ Г) Передачу данных на зарубежные серверы	
35.	Способность распознавать противоправный контент и действовать в рамках закона	«Цифровой иммунитет» личности в правовом контексте — это: А) Наличие антивируса на телефоне Б) Отсутствие аккаунтов в соцсетях В) Способность распознавать противоправный контент и действовать в рамках закона Г) Использование дипломатического паспорта в сети	
36.		Дайте определение суверенитета и назовите его основные признаки по Ж. Бодену.	
37.		В чем заключается суть принципа народного суверенитета по Ж.-Ж. Руссо?	ПК-3, ПК-4
38.		Охарактеризуйте основные принципы Вестфальской системы международных отношений.	ПК-3, ПК-4
39.		Какие этапы развития идеи суверенитета можно выделить в российской политико-правовой мысли?	ПК-3, ПК-4
40.		Как соотносятся понятия «суверенитет» и «независимость» в современной правовой доктрине?	ПК-3, ПК-4
41.		Сформулируйте определение цифрового суверенитета. Перечислите и кратко охарактеризуйте основные уровни цифрового суверенитета.	ПК-3, ПК-4
42.		В чем заключаются основные риски «технологического колониализма» для современных государств?	ПК-3, ПК-4
43.		Какие нормативные акты РФ составляют правовую основу цифрового суверенитета?	ПК-3, ПК-4
44.		Объясните суть принципа локализации персональных данных.	ПК-3, ПК-4
45.		Как цифровой суверенитет соотносится с концепцией «свободного интернета»?	ПК-3, ПК-4
46.		Назовите основные нормативно-правовые акты, составляющие основу кибербезопасности РФ.	ПК-3, ПК-4
47.		Каковы полномочия ФСБ и ФСТЭК в сфере обеспечения цифрового суверенитета?	ПК-3, ПК-4
48.		Опишите правовой режим объектов критической информационной инфраструктуры	ПК-3, ПК-4

		(КИИ)	
49.		В чем заключаются основные отличия позиции РФ по международному киберправу от позиции стран ЕС?	ПК-3, ПК-4
50.		Какие требования предъявляются к обработке персональных данных в контексте обеспечения национальной безопасности?	ПК-3, ПК-4
51.		Дайте определение акта правоприменения в сфере кибербезопасности и назовите его основные признаки.	ПК-3, ПК-4
52.		Перечислите основные стадии правоприменительного процесса при совершении компьютерного преступления.	ПК-3, ПК-4
53.		Какова структура системы органов исполнительной власти, осуществляющих правоприменение в цифровой сфере?	ПК-3, ПК-4
54.		В чем заключаются особенности установления фактических обстоятельств дела при совершении правонарушений в сети Интернет?	ПК-3, ПК-4
55.		Охарактеризуйте правовой статус ГосСОПКА как элемента механизма обеспечения кибербезопасности.	ПК-3, ПК-4
56.		Каковы обязательные элементы состава преступления, предусмотренного статьей 273 УК РФ?	ПК-3, ПК-4
57.		В каких случаях наступает административная ответственность по статье 13.12 КоАП РФ?	ПК-3, ПК-4
58.		Охарактеризуйте особенности дисциплинарной ответственности работника за нарушение требований информационной безопасности.	ПК-3, ПК-4
59.		Какие виды наказаний предусмотрены за неправомерное воздействие на объекты КИИ РФ?	ПК-3, ПК-4
60.		Каков порядок и сроки привлечения к ответственности за нарушение законодательства о локализации персональных данных россиян?	ПК-3, ПК-4
61.		Какие три категории значимости объектов КИИ выделяет законодательство?	ПК-3, ПК-4
62.		Перечислите основные показатели социальной значимости объектов КИИ.	ПК-3, ПК-4
63.		Каковы сроки уведомления ФСБ России о компьютерном инциденте на значимом объекте КИИ?	ПК-3, ПК-4
64.		В чем заключается процедура ведения реестра значимых объектов КИИ ФСТЭК России?	ПК-3, ПК-4

65.		Назовите основные нормативные акты, устанавливающие требования к системам безопасности значимых объектов КИИ.	ПК-3, ПК-4
66.		Дайте определение «цифровой зрелости» в контексте нормативных актов РФ 2024–2026 гг.	ПК-3, ПК-4
67.		Каковы основные элементы правовой культуры субъекта критической информационной инфраструктуры?	ПК-3, ПК-4
68.		В чем заключается роль правового воспитания в профилактике киберугроз?	ПК-3, ПК-4
69.		Опишите взаимосвязь между правовым нигилизмом и уязвимостью цифрового суверенитета.	ПК-3, ПК-4
70.		Какие этические нормы регулируют деятельность юриста-эксперта в сфере ИТ?	ПК-3, ПК-4

2. Описание шкалы оценивания

Рейтинговая система оценки не предусмотрена для студентов, обучающихся на образовательных программах уровня высшего образования - магистратуры.

3. Критерии оценивания

Оценка «зачтено» выставляется студенту, если он раскрыл вопрос в полной мере на основе учебной, методической, дополнительной литературы, а также необходимых нормативно-правовых актов, а также если студент демонстрирует (ПК-3, ПК-4):

- Полноту знаний: свободное оперирование понятиями «цифровой суверенитет», «критическая информационная инфраструктура (КИИ)», «цифровая зрелость» и «правоприменительный акт в ИТ-сфере»
- Аналитические навыки: способность провести юридическую экспертизу нормативного акта на предмет выявления коррупциогенных факторов и угроз кибербезопасности
- Практическую подготовку: успешное выполнение **всех** индивидуальных творческих заданий и прохождение тестирования (не менее 60% правильных ответов)
- Владение методологией: умение классифицировать цифровые риски и определять компетенцию органов власти (ФСБ, ФСТЭК, Роскомнадзор) в конкретных кейсах правоприменения
- Самостоятельность: обоснованная защита докладов и презентаций, подготовленных с использованием отечественного ПО

Оценка «не зачтено» выставляется студенту, если ответ по существу отсутствует, несмотря на наводящие вопросы преподавателя, а также если студент не раскрыл содержание вопросов, не знает базовых определений (ПК-3, ПК-4)