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

УТВЕРЖДАЮ
Директор Юридического института
Смирнов Д.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Правовое регулирование информационной безопасности в цифровой среде

Направление подготовки	40.03.01 Юриспруденция
Направленность (профиль)	Технологическая юриспруденция в цифровую эпоху
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	7

Предисловие

1. Назначение. Фонд оценочных средств обеспечивает объективный контроль достижения запланированных результатов обучения по дисциплине «Правовое регулирование информационной безопасности в цифровой среде» студентов, обучающихся по направлению подготовки 40.03.01 «Юриспруденция».

2. Фонд оценочных средств текущего контроля успеваемости и промежуточной аттестации разработан на основе рабочей программы дисциплины «Правовое регулирование информационной безопасности в цифровой среде» и в соответствии с образовательной программой высшего образования по направлению подготовки 40.03.01 «Юриспруденция». ФОС прошел процедуру экспертизы.

3. Разработчик Боташева Л.Э. – к.ю.н., доцент, доцент кафедры Административного и финансового права юридического института СКФУ

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: Смирнов Д.А., зав. кафедрой АФП, д.ю.н., профессор

Члены комиссии:

Мельникова В.А., к.ю.н., доцент

Заикин В.В., к.ю.н., доцент

Представитель организации-работодателя:

Представитель организации-работодателя

Андреев Н.Н., адвокат. МКА ВМ-Право

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 40.03.01 Юриспруденция, направленности (профиля) «Технологическая юриспруденция в цифровую эпоху».

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-4 Способен выявлять, раскрывать, расследовать и квалифицировать преступления и иные правонарушения	**ИД-1 ПК-4** С соблюдением норм материального и процессуального права осуществляет мероприятия/совершает действия по получению юридически значимой информации, анализу, проверке, оценке и использованию ее в целях выявления, раскрытия и расследования преступлений и иных правонарушений	Определяет юридически значимую информацию для выявления, раскрытия и расследования преступлений и правонарушений в цифровой среде с целью обеспечения информационной безопасности.
	ИД-2 ПК-4 Юридически правильно квалифицирует правонарушение	Показывает навыки профессионально верной квалификации правонарушений, совершающихся в цифровой среде и посягающих на информационную безопасность
	ИД-3 ПК-4 С соблюдением норм процессуального права и правил делопроизводства оформляет результаты профессиональной деятельности в юридических документах	Показывает способность оформления результатов юридической деятельности с соблюдением норм материального и процессуального права

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
		Форма обучения очная Семестр__ 7	
1.	Б	Какая категория информации, согласно ФЗ-149, требует обязательного принятия мер по её защите? А) Любая информация, размещенная в сети Интернет. Б) Информация, составляющая государственную тайну, и иная информация ограниченного доступа, установленная федеральными законами. М) Только информация о частной жизни граждан. Г) Информация, передаваемая исключительно по государственным каналам связи.	**ПК-4**
2.	Б	Что понимается под «критической информационной инфраструктурой» (КИИ) согласно ФЗ-187? А) Совокупность всех серверов и дата-центров на территории РФ. Б) Информационные системы, сети и автоматизированные системы управления, функционирующие в стратегически важных сферах (здравоохранение, транспорт, связь, энергетика и др.). В) Только государственные информационные системы (ГИС). Г) Совокупность компьютеров в ведении Министерства обороны РФ.	**ПК-4**
3.	Б	В какой срок оператор персональных данных обязан уведомить Роскомнадзор о произошедшем инциденте (утечке данных) с момента его обнаружения? А) В течение 12 часов. Б) В течение 24 часов. В) В течение 72 часов. Г) В течение 30 календарных дней.	**ПК-4**
4.	Б	Какое техническое средство защиты информации (СЗИ) подлежит обязательной сертификации при использовании в государственных информационных системах (ГИС)? А) Любое антивирусное ПО, купленное в магазине.	**ПК-4**

		Б) СЗИ, прошедшее процедуру оценки соответствия в формах сертификации или декларирования (ФСТЭК или ФСБ России). В) Программное обеспечение с открытым исходным кодом (Open Source). Г) Только зарубежное ПО, локализованное в РФ.	
5.	В	Какая статья Уголовного кодекса РФ предусматривает ответственность за создание, использование и распространение вредоносных компьютерных программ? А) ст. 159.6 УК РФ. Б) ст. 272 УК РФ. В) ст. 273 УК РФ. Г) ст. 274.1 УК РФ.	**ПК-4**
6.	В	Что является правовым основанием для признания информации «коммерческой тайной» организации? А) Устное распоряжение руководителя компании. Б) Факт того, что информация приносит прибыль. В) Введение режима коммерческой тайны (принятие локального акта, нанесение грифа, ограничение доступа). Г) Регистрация информации в реестре налоговой службы.	**ПК-4**
7.	В	Какую ответственность несет оператор КИИ за нарушение правил эксплуатации объектов КИИ, повлекшее причинение вреда, согласно УК РФ? А) Только дисциплинарную. Б) Административную (штраф до 50 тысяч рублей). В) Уголовную по ст. 274.1 УК РФ. Г) Материальную в размере 10-кратного оклада.	**ПК-4**
8.	Б	Обязан ли оператор персональных данных осуществлять первичный сбор и хранение данных граждан РФ на серверах, находящихся внутри страны (требование локализации)? А) Нет, это носит рекомендательный характер. Б) Да, это обязательное требование ч. 5 ст. 18 ФЗ-152. В) Только если данные относятся к государственной тайне. Г) Только для государственных органов.	**ПК-4**
9.	В	Кто является уполномоченным федеральным органом по контролю и надзору в сфере защиты персональных данных?	**ПК-4**

		А) ФСБ России. Б) ФСТЭК России. В) Роскомнадзор. Г) Министерство цифрового развития.	
10.	Б	В чем заключается правовой принцип «минимизации данных» при обеспечении информационной безопасности? А) В удалении всех данных после завершения рабочего дня. Б) В обработке только тех персональных данных, которые необходимы для достижения конкретных, заранее определенных целей. В) В хранении данных в сжатом (архивированном) виде для экономии места. Г) В ограничении доступа сотрудников к сети Интернет.	**ПК-4**
11.		Каков правовой алгоритм присвоения категории значимости объекту критической информационной инфраструктуры и какие юридические последствия наступают для субъекта КИИ после завершения этой процедуры?	**ПК-4**
12.		Какие пять обязательных мер, согласно ФЗ «О коммерческой тайне», должен предпринять обладатель информации, чтобы получить право на судебную защиту своих секретов?	**ПК-4**
13.		Раскройте содержание обязанности оператора по обеспечению записи, систематизации и хранения персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ. Существуют ли исключения из этого правила?	**ПК-4**
14.		Проведите сравнительный анализ компетенций ФСТЭК России и ФСБ России в сфере защиты информации. В каких случаях организации необходимо обращаться в каждое из этих ведомств?	**ПК-4**
15.		Проанализируйте законопроекты (или действующие нормы) о введении оборотных штрафов для компаний за утечки персональных данных. Какие правовые аргументы существуют «за» и «против» такой меры?	**ПК-4**
16.		Каковы требования российского законодательства к использованию средств криптографической защиты информации (СКЗИ) в частном бизнесе и государственном секторе? Когда требуется лицензирование?	**ПК-4**

17.		Каков правовой регламент взаимодействия частной компании с государственным центром ГосСОПКА при обнаружении компьютерной атаки?	**ПК-4**
18.		Опишите процедуру уведомления Роскомнадзора о намерении осуществлять трансграничную передачу данных после вступления в силу изменений в ФЗ-152 в 2023 году.	**ПК-4**
19.		В чем заключается различие в квалификации деяний по ст. 272 УК РФ (неправомерный доступ) и ст. 274.1 УК РФ (преступления против безопасности КИИ)?	**ПК-4**
20.		Как соотносятся нормы об информационной безопасности с институтами адвокатской, банковской и врачебной тайны в условиях цифровизации архивов?	**ПК-4**