

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Крюков Вадим Николаевич

Должность: Проректор по образовательной деятельности и инновационной политике

Дата подписания: 17.06.2026 18:11:52

Уникальный программный ключ:

1b0adb7fd710f6a0705d90c58682bd0c5f2f25b2

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Заполярный государственный университет им. Н. М. Федоровского»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Организационно-правовое обеспечение информационных систем

Направление подготовки 09.03.02 «Информационные системы и технологии»

Профиль «Проектирование и реализация информационных систем и технологий»

Уровень образования: бакалавриат

Кафедра «Информационные системы и технологии»

Разработчик ФОС:

к.т.н., Доцент, Петров А.М. _____

Петров А.М.

Оценочные материалы по дисциплине рассмотрены и одобрены на заседании кафедры, протокол от 10.04.2026г. № 5.

Заведующий кафедрой _____ к.э.н., Беляев И.С.

Фонд оценочных средств по дисциплине Организационно-правовое обеспечение информационных систем для текущей/ промежуточной аттестации разработан в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности / направлению подготовки 09.03.02 Информационные системы и технологии на основе Рабочей программы дисциплины Организационно-правовое обеспечение информационных систем, утвержденной решением ученого совета от г., Положения о формировании Фонда оценочных средств по дисциплине (ФОС), Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся ЗГУ, Положения о государственной итоговой аттестации (ГИА) выпускников по образовательным программам высшего образования в ЗГУ им. Н.М. Федоровского.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1. Компетенции и индикаторы их достижения

Код и наименование компетенции	Индикаторы достижения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Определяет круг задач в рамках поставленной цели, определяет связи между ними
	УК-2.2 Предлагает способы решения поставленных задач и ожидаемые результаты; оценивает предложенные способы с точки зрения соответствия цели проекта
	УК-2.3 Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм

Таблица 2. Паспорт фонда оценочных средств

№п/п	Контролируемые разделы(темы) дисциплины	Кодрезультатаобучения по дисциплине/ модулю	Оценочные средства текущей		Оценочные средства промежуточной	
			Наименование	Форма	Наименование	Форма
3 семестр						

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы.

2.1. Задания для текущего контроля успеваемости

1. Обеспечение информационной безопасности в условиях
2. глобализации информационного пространства
3. Информационная безопасность в информационном обществе
4. Современное информационное противоборство и обеспечение информационной безопасности
5. Теоретические и методологические вопросы организационного и правового обеспечения информационной безопасности
6. Информационная безопасность в системе национальной безопасности Российской Федерации
7. Базовые принципы обеспечения информационной безопасности
8. Правовое регулирование информационной безопасности в системе российского информационного права
9. Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации
10. Правовые средства обеспечения безопасности информации
11. Организационное обеспечение информационной безопасности Российской Федерации
12. Организационно-правовые проблемы международной информационной безопасности
Международные правовые акты в области обеспечения информационной безопасности
13. Зарубежный опыт правового обеспечения информационной безопасности
14. Продвижение российских инициатив в области обеспечения международной информационной безопасности
15. Правовые режимы обеспечения безопасности информации ограниченного доступа
16. Ограничение доступа к информации в целях защиты интересов личности, общества и государства
17. Правовые режимы тайн в системе организационного и правового обеспечения безопасности информации ограниченного доступа
18. Правовой режим защиты государственной тайны
19. Правовой режим коммерческой тайны
20. Правовой режим обеспечения безопасности персональных данных
21. Актуальные вопросы режима служебной тайны
22. Актуальные проблемы правового и организационного обеспечения информационной безопасности
23. Противодействие экстремистской деятельности в информационной сфере .
24. Защита детей от информации, причиняющей вред их здоровью и развитию
25. Правовые проблемы обеспечения информационной безопасности в сети Интернет
26. Особенности организационно-правового обеспечения защиты информационных систем
27. Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении
28. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства
29. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем
30. Юридическая ответственность за правонарушения в информационной сфере
31. Понятие и виды юридической ответственности в области обеспечения информационной безопасности. Субъекты
32. Юридическая ответственность за правонарушения в информационной сфере

2.2 Темы письменных работ (эссе, рефераты, курсовые работы и др.)

Эссе

1. Роль правового регулирования в обеспечении безопасности информационных систем.
2. Этические аспекты использования персональных данных в информационных системах.
3. Влияние законодательства на развитие цифровых технологий.
4. Как правовые нормы защищают интеллектуальную собственность в IT-сфере?
5. Будущее правового регулирования искусственного интеллекта.
6. Правовые аспекты использования облачных технологий.
7. Ответственность за утечку данных: кто несет ответственность и как её избежать?
8. Как законодательство влияет на внедрение электронного документооборота?
9. Правовые риски при использовании открытого программного обеспечения.
10. Значение авторского права в разработке программного обеспечения.
11. Правовые основы защиты конфиденциальной информации в организациях.
12. Роль международного права в регулировании кибербезопасности.
13. Как правовые нормы влияют на развитие электронной коммерции?
14. Проблемы правового регулирования блокчейн-технологий.
15. Правовые аспекты использования биометрических данных.
16. Как законодательство защищает права пользователей интернета?
17. Роль государства в регулировании киберпреступности.
18. Правовые аспекты обработки больших данных (Big Data).
19. Ответственность за нарушение правил хранения персональных данных.
20. Этические и правовые вопросы использования ИИ в бизнесе.

Рефераты

21. Основные нормативные документы, регулирующие использование информационных систем в России.
22. Федеральный закон "О персональных данных": ключевые положения и их применение.
23. Международные стандарты защиты информации и их роль в правовом регулировании.
24. Правовые основы лицензирования программного обеспечения.
25. Защита авторских прав на программное обеспечение: российский и международный опыт.
26. Правовые аспекты использования облачных сервисов в бизнесе.
27. Правовые нормы, регулирующие электронный документооборот.
28. Ответственность за нарушение правил обработки персональных данных.
29. Правовые основы защиты информации в государственных учреждениях.
30. Роль законодательства в обеспечении кибербезопасности.
31. Правовые аспекты использования технологий распознавания лиц.
32. Международное сотрудничество в области правового регулирования IT.
33. Правовые основы использования искусственного интеллекта.
34. Правовые аспекты внедрения IoT (Интернета вещей).
35. Особенности правового регулирования электронной коммерции.
36. Правовые аспекты защиты интеллектуальной собственности в цифровой среде.
37. Роль законодательства в регулировании использования Big Data.
38. Правовые нормы, регулирующие работу с открытыми данными.
39. Правовые аспекты использования криптовалют.
40. Правовые основы защиты информации в условиях цифровизации.

Курсовые работы

41. Разработка системы защиты персональных данных в организации.
42. Проектирование правовой базы для внедрения электронного документооборота.
43. Создание системы управления доступом к конфиденциальной информации.
44. Разработка рекомендаций по защите авторских прав на программное обеспечение.
45. Проектирование системы защиты информации в облачных сервисах.
46. Создание правовой модели для работы с биометрическими данными.
47. Разработка системы управления рисками при обработке персональных данных.
48. Проектирование системы юридической защиты информации в электронной коммерции.
49. Создание системы мониторинга соблюдения законодательства о персональных данных.

50. Разработка правовых рекомендаций для использования искусственного интеллекта.
51. Проектирование системы защиты информации при использовании IoT.
52. Создание правовой базы для работы с открытыми данными.
53. Разработка системы управления правовыми рисками в IT-проектах.
54. Проектирование системы защиты информации в государственных учреждениях.
55. Создание системы правового регулирования использования криптовалют.
56. Разработка системы защиты информации в условиях цифровой трансформации.
57. Проектирование правовой модели для работы с Big Data.
58. Создание системы управления правовыми аспектами кибербезопасности.
59. Разработка рекомендаций по защите информации в мобильных приложениях.
60. Проектирование системы правового регулирования использования блокчейн-технологий.

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Перечислите и объясните основные виды информации ограниченного доступа.
3. Перечислите направления защиты информации на объекте, согласно ГОСТ Р 50922 – 2006 «Защита информации. Основные термины и определения»
4. Напишите определения следующих терминов: информационная безопасность; доступность информации; целостность информации.
5. Начертите и объясните классификацию видов угроз информационной безопасности.

6. Начертите и объясните классификацию средств защиты информации.
7. Начертите и объясните базовую модель передачи данных.
8. Перечислите существующие методы взлома.
9. Перечислите существующие методы криптоанализа.
10. Начертите и объясните жизненный цикл системы информационной безопасности.
11. Начертите и объясните классификацию источников информационных угроз для РФ.
12. Начертите и объясните классификацию основных видов информационных угроз.
13. Перечислите и объясните любые пять фундаментальных законов информационной безопасности.
14. Перечислите национальные интересы РФ в информационной сфере с точки зрения ДИБ.
15. Перечислите негативные факторы, влияющие на состояние ИБ с точки зрения ДИБ.
16. Что такое манифест свободного информационного пространства и в чем его суть?
17. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.
18. Перечислите существующие программные средства защиты информации.

зачет