Приложение 4

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»

Балахнинский филиал ННГУ

УТВЕРЖДЕНО

решением Ученого совета ННГУ

протокол № 10 от 02.12.2024 г.

Рабочая программа дисциплины

Информационная безопасность

Уровень высшего образования
Бакалавриат

Направление подготовки / специальность
09.03.03 - Прикладная информатика

Направленность образовательной программы
Прикладная информатика в управлении производством

Форма обучения
очная

г. Балахна

2025 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.21 Информационная безопасность относится к обязательной части образовательной программы.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**	
	Индикатор достижения компетенции (код, содержание индикатора)	**Результаты обучения по дисциплине**	**Для текущего контроля успеваемости**	**Для промежуточной аттестации**
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*ОПК-3.1: Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности* *ОПК-3.2: Демонстрирует умение применять информационно-коммуникационные технологии решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности* *ОПК-3.3: Имеет практический опыт решения стандартных задач профессиональной деятельности с соблюдением требований информационной безопасности*	*ОПК-3.1:* *Знать: основные методы и способы классификации конфиденциальной информации.* *Уметь: работать с компьютером как средством управления информационной безопасностью.* *Владеть: основными способами обнаружения информационных угроз и использования специального программного обеспечения.* *ОПК-3.2:* *Знать: нормативно-правовые и организационные требования защиты информации.* *Уметь: использовать современные средства и технологии защиты информации.* *Владеть: способами обработки и анализа данных с применением систем информационной безопасности.* *ОПК-3.3:* *Знать: современные возможности систем защиты информации при обработке отчетности в целях принятия*	*Тест* *Доклад*	*Экзамен:* *Контрольные вопросы*

		управленческих решений. *Уметь: использовать информационные технологии при решении профессиональных задач.* *Владеть: навыками работы с современными системами защиты информации при принятии управленческих решений.*		
ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	*ОПК-4.1: Демонстрирует знание основных стандартов, норм и правил оформления технической документации на различных стадиях проектирования и поддержки жизненного цикла информационных систем* *ОПК-4.2: Применяет стандарты, нормы и правила (в том числе установленные самостоятельно) при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла информационных систем* *ОПК-4.3: Имеет практический опыт разработки технической документации на различных этапах проектирования и поддержки жизненного цикла информационной системы*	*ОПК-4.1:* *Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.* *Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.* *Владеть: навыками составления технической документации на различных этапах жизненного цикла информационной системы.* *ОПК-4.2:* *Знать: виды и источники угроз безопасности информации для различных профессиональных областей.* *Уметь: определять актуальные источники угроз безопасности для различных профессиональных областей.* *Владеть: инструментальными средствами и методами сбора, анализа и формирования требований к информационной безопасности.* *ОПК-4.3:* *Знать: законодательную базу в сфере информационной безопасности и основные*	*Тест* *Доклад*	*Экзамен: Контрольные вопросы*

		требования информационной безопасности. *Уметь: проводить анализ нормативной базы для обеспечения информационной безопасности.* *Владеть: навыками работы с инструментальными средствами обеспечения информационной безопасности.*		

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	**4**
Часов по учебному плану	**144**
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	**16**
- занятия семинарского типа (практические занятия / лабораторные работы)	**48**
- КСР	**2**
самостоятельная работа	**42**
Промежуточная аттестация	**36** **Экзамен**

3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	Всего (часы)	в том числе			
		Контактная работа (работа во взаимодействии с преподавателем), часы из них			Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа (практические занятия/лабораторные работы), часы	Всего	
	ооо	ооо	ооо	ооо	ооо
Тема 1. Теоретические аспекты информационной безопасности экономических систем	17	2	8	10	7
Тема2. Понятие информационных угроз и их виды	17	2	8	10	7
Тема 3. Государственное регулирование информационной безопасности	16	3	8	11	5

Тема 4.Подходы, принципы, методы и средства обеспечения безопасности	18	3	8	11	7
Тема 5. Организация системы защиты информации	18	2	8	10	8
Тема 6. Менеджмент и аудит систем информационной безопасности	20	4	8	12	8
Аттестация	36				
КСР	2			2	
Итого	144	16	48	66	42

Содержание разделов и тем дисциплины

Тема 1. Теоретические аспекты информационной безопасности экономических систем
1.1. Основные понятия информационной безопасности управленческих систем
1.2. Экономическая информация как товар и объект безопасности
Тема 2. Понятие информационных угроз и их виды
2.1. Понятие информационной угрозы
2.2 Классификация угроз информационной безопасности
2.3 Виды и способы воздействия информационных угроз
2.4 Понятие и виды компьютерных преступлений
2.5. Вредоносные программы для ПК и мобильных устройств
Тема 3. Государственное регулирование информационной безопасности
3.1. Деятельность международных организаций в сфере информационной безопасности
3.2. Органы государственной власти Российской Федерации в сфере информационной безопасности
3.3. Нормативно-правовые акты в области информационной безопасности в РФ
Тема 4. Подходы, принципы, методы и средства обеспечения безопасности
4.1. Политика информационной безопасности
4.2. Подходы, методы и средства обеспечения ИБ
Тема 5. Организация системы защиты информации
5.1. Организационное обеспечение информационной безопасности
5.2. Защита информации в Интернет
5.3. Защита от компьютерных вирусов
5.4. Этапы построения системы защиты информации
5.5 Искусственный интеллект и нейросети в информационной безопасности
Тема 6. Менеджмент и аудит систем информационной безопасности
6.1. Менеджмент и аудит информационной безопасности на уровне предприятия
6.2. Аудит информационной безопасности электронной коммерции
6.3. Менеджмент информационной безопасности электронной коммерции

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Для обеспечения самостоятельной работы обучающихся используются:
Электронные курсы, созданные в системе электронного обучения ННГУ:

Информационная безопасность, https://e-learning.unn.ru/course/view.php?id=1809.

Иные учебно-методические материалы:
A. www.gks.ru / Федеральная служба государственной статистики.
B. Операционная система Microsoft Windows
C. Прикладное программное обеспечение Microsoft Office
D. Справочно-правовая система «КонсультантПлюс»

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:

5.1.1 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-3:

Прочитайте текст и выберите все правильные варианты ответов

№	Вопрос
1	**Принцип системности означает:** А. Комплексный анализ угроз, средств защиты от этих угроз; Б. Прозрачность для легальных пользователей; В. Эшелонированность обороны. **Ответ:**
2	**Программа безопасности синхронизируется с жизненным циклом системы?** А. да; Б. нет; В. отчасти. **Ответ:**
3	**В политике безопасности основным принципом является усиление самого слабого звена?** А. нет: Б. да; В. отчасти. **Ответ:**
4	**Криптографические средства – это?**

	А. регламентация правил использования, обработки и передачи информации ограниченного доступа; Б. средства защиты с помощью преобразования информации (шифрование); В. средства, в которых программные и аппаратные части полностью взаимосвязаны. **Ответ:**
5	**Как нейросети помогают анализировать вредоносное ПО?** А. Путем запуска вирусов в песочнице Б. Через автоматическое выделение признаков из бинарных файлов В. Блокировкой всех исполняемых файлов **Ответ:**

Прочитайте текст и дайте ответ, соответствующий смысловому содержанию вопроса

№	Вопрос
1	Информационная безопасность на уровне предприятия – это…
2	Что относится к объектам информационной безопасности на предприятие?
3	Назовите угрозы информационной безопасности на уровне государства
4	Назовите угрозы информационной безопасности на уровне предприятия
5	Что такое «персональные данные»?

5.1.2 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-4:

Прочитайте текст и выберите все правильные варианты ответов

№	Вопрос
1	**Организационное обеспечение информационной безопасности – это?** А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.; Б. совокупность средств;

	В. нормативные документы по ИБ, требование которых являются обязательными в рамках сферы действия каждого подразделения. **Ответ:**
2	**Правовое обеспечение информационной безопасности – это..?** А. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения; Б. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы; В. широкое использование технических средств защиты информации. **Ответ:**
3	**В организационную основу системы обеспечения информационной безопасности** РФ входит: А. Совет безопасности РФ; Б. Министерство образования и науки РФ; В. ЦРУ США. **Ответ:**
4	**К актам федерального законодательства по ИБ в РФ входят:** А. Приказы ФСБ; Б. Международные стандарты; В. Конституция РФ. **Ответ:**
5	**Федеральный закон «Об информации, информационных технологиях и о защите** информации» А. пока не принят; Б. принят в 2000 году; В. принят в 2006 году. **Ответ:**

Прочитайте текст и дайте ответ, соответствующий смысловому содержанию вопроса

№	Вопрос
1	Как нейросети помогают анализировать вредоносное ПО?
2	Как нейросети применяются в антифишинге?
3	Какой метод помогает обнаруживать DDoS-атаки с помощью нейросетей
4	Характеристика Указа Президента Российской Федерации от 05.12.2016 г. №646
5	Менеджмент информационной безопасности - это…

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
зачтено	Ставится в случае, если студент отвечает четко и последовательно, показывая глубокие знания по теме и уверенное владение основным материалом
не зачтено	Ставится в случае, если студент при ответе на вопросы допускает грубые ошибки, демонстрирует незнание основных терминов и понятий

5.1.3 Типовые задания (оценочное средство - Доклад) для оценки сформированности компетенции ОПК-3:

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
4. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
5. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
6. Правовые основы защиты конфиденциальной информации.
7. Экономические основы защиты конфиденциальной информации.
8. Организационные основы защиты конфиденциальной информации.
9. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
10. Составление инструкции по обработке и хранению конфиденциальных документов.
11. Направления и методы защиты документов на бумажных носителях.
12. Направления и методы защиты машиночитаемых документов.
13. Архивное хранение конфиденциальных документов.
14. Направления и методы защиты аудио- и визуальных документов.
15. Порядок подбора персонала для работы с конфиденциальной информацией.
16. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
17. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
18. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

5.1.4 Типовые задания (оценочное средство - Доклад) для оценки сформированности компетенции ОПК-4:

1. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
2. Порядок защиты информации в рекламной и выставочной деятельности.
3. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
4. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
5. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
6. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
7. Назначение, виды, структура и технология функционирования системы защиты информации.
8. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
9. Аналитическая работа по выявлению каналов утечки информации фирмы.
10. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
11. Направления и методы защиты профессиональной тайны.
12. Направления и методы защиты служебной тайны.
13. Направления и методы защиты персональных данных о гражданах.
14. Методы защиты личной и семейной тайны.
15. Построение и функционирование защищенного документооборота.
16. Защита секретов в дореволюционной России.

Критерии оценивания (оценочное средство - Доклад)

Оценка	Критерии оценивания
зачтено	Ставится в случае, если студент отвечает четко и последовательно, показывая глубокие знания по теме и уверенное владение основным материалом
не зачтено	Ставится в случае, если студент при ответе на вопросы допускает грубые ошибки, демонстрирует незнание основных терминов и понятий

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	**плохо**	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	не зачтено		**зачтено**				
Знания	Отсутствие знаний	Уровень знаний ниже	Минимально	Уровень знаний в	Уровень знаний в	Уровень знаний в	Уровень знаний в

	теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	минимальных требований. Имели место грубые ошибки	допустимый уровень знаний. Допущено много негрубых ошибок	объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	объеме, соответствующем программе подготовки. Ошибок нет.	объеме, превышающем программу подготовки.
Умения	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценивания при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	**превосходно**	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой
	отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо».
	удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»

не зачтено	**неудовлетворительно**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

5.3.1 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ОПК-3

1. Объекты информационной безопасности на предприятии.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Угрозы информационной безопасности на уровне государства.
10. Угрозы информационной безопасности на уровне предприятия
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно -профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.
17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Деятельность международных организаций в сфере информационной безопасности.
22. Фрагментарный и системный подход к защите информации

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ОПК-4

1. Государственное регулирование информационной безопасности.
2. Характеристика Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об
3. информации, информационных технологиях и о защите информации».
4. Характеристика Указа Президента Российской Федерации от 05.12.2016 г. №646
5. Нормативно-правовые аспекты в области информационной безопасности в Российской
6. Федерации.
7. Доктрина информационной безопасности России.
8. Уголовно-правовой контроль над компьютерной преступностью в России.
9. Федеральные законы по ИБ в РФ.
10. Политика безопасности и ее принципы.

11. Оценка эффективности инвестиций в информационную безопасность.
12. План обеспечения непрерывной работы и восстановления функционирования
13. автоматизированной информационной системы.
14. Обеспечение безопасности в системе интернет-банкинга
15. Электронная коммерция и ее защита.
16. Менеджмент информационной безопасности предприятия.
17. Информационная безопасность предпринимательской деятельности.
18. Обеспечение информационной безопасности должностных лиц и представителей деловых
19. кругов.
20. Какие признаки классифицируют нейронные сети
21. Виды обучения нейронных сетей
22. Типы нейронных сетей применяются в социально-экономических исследованиях
23. Этапы обучения нейронной сети
24. Применение искусственного интеллекта для выявления информационных угроз
25. Применение нейро-сетевых технологий в системе защиты информации
26. Угрозы использования искусственного интеллекта

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой.
отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо».
удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев ; ННГУ им. Н. И. Лобачевского. - Нижний Новгород : Изд-во ННГУ, 2017. - 198 с. - Текст : электронный., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=823079&idb=0.
2. Баланов А. Н. Комплексная информационная безопасность : учебное пособие для вузов / Баланов А. Н. - Санкт-Петербург : Лань, 2024. - 400 с. - Книга из коллекции Лань - Информатика. - ISBN 978-5-507-49250-3., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=898841&idb=0.
3. Баранова Елена Константиновна (Национальный исследовательский университет "Высшая школа экономики"). Информационная безопасность и защита информации : Учебное пособие / Национальный исследовательский университет "Высшая школа экономики". - 4. - Москва : Издательский Центр РИОР, 2024. - 336 с. - (СПО). - ВО - Бакалавриат. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7 (электр. издание). - ISBN 978-5-16-013849-7 (ISBN соиздателя)., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=915122&idb=0.
4. Зенков А. В. Информационная безопасность и защита информации : учебное пособие / А. В. Зенков. - 2-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 107 с. - (Высшее образование). - ISBN 978-5-534-16388-9. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=871683&idb=0.

Дополнительная литература:

1. Бурова Маргарита Сергеевна. Методические указания для выполнения практических заданий по дисциплине «Информационная безопасность» для обучающихся по направлению подготовки 09.03.03 «Прикладная информатика», направленность образовательной программы «Прикладная информатика в экономике» : учебно-методическое пособие / М. С. Бурова, А. В. Дорожкин ; ННГУ им. Н. И. Лобачевского. - Нижний Новгород : Изд-во ННГУ, 2024. - 26 с. - Текст : электронный., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=892495&idb=0.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

Консультант плюс

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки/специальности 09.03.03 - Прикладная информатика.

Автор(ы): Дорожкин Артем Владиславович, кандидат экономических наук.

Рецензент(ы): Ясенев Вячеслав Николаевич, кандидат экономических наук.

Заведующий кафедрой: Трифонов Юрий Васильевич, доктор экономических наук.

Программа одобрена на заседании методической комиссии от 27 ноября 2024, протокол № 3.