

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Институт экономики и предпринимательства

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Рабочая программа дисциплины

Методы и средства обеспечения информационной безопасности

Уровень высшего образования
Магистратура

Направление подготовки / специальность
38.04.01 - Экономика

Направленность образовательной программы
Информационная безопасность экономических процессов

Форма обучения
очная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.ДВ.03.01 Методы и средства обеспечения информационной безопасности относится к части, формируемой участниками образовательных отношений 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
ПК-11: Способен управлять ресурсами, процессами, службами и подразделениями, осуществляющими экономическую деятельность на предприятиях и организациях различных форм собственности, в органах государственной и муниципальной власти	ПК-11.1: Управляет ресурсами и процессами на предприятиях и организациях различных форм собственности, в органах государственной и муниципальной власти ПК-11.2: Руководит службами и подразделениями, осуществляющими аналитическую, производственно-хозяйственную, организационно-экономическую и внешнеэкономическую деятельность на предприятиях и организациях различных форм собственности	ПК-11.1: Знать принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности Уметь использовать принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности Владеть навыками решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности ПК-11.2: Знать принципы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности Уметь разработать	Практическое задание Тест	Экзамен: Контрольные вопросы

		<p>требования по информационной безопасности для решения стандартных задач профессиональной деятельности</p> <p>Владеть навыками подбора и использования программно-технических средств для решения</p>		
<p>ДПК-3: Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами</p>	<p>ДПК-3.1: Владеет базовыми программными методами защиты информации при работе с компьютерными системами; организационными мерами и приемами антивирусной защиты; методами и технологиями соблюдения</p>	<p>ДПК-3.1:</p> <p>Знать принципы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности</p> <p>Уметь разработать требования по информационной безопасности для решения стандартных задач</p> <p>Знать принципы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности</p> <p>Уметь разработать требования по информационной безопасности для решения стандартных задач профессиональной деятельности</p> <p>Владеть навыками подбора и Знать принципы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности</p> <p>Уметь разработать требования по информационной безопасности для</p>	<p>Практическое задание</p> <p>Тест</p>	<p>Экзамен:</p> <p>Контрольные вопросы</p>

		<p>решения стандартных задач профессиональной деятельности</p> <p>Владеть навыками подбора и использования программно-технических средств для решения использования программно-технических средств для решения</p> <p>решения профессиональной деятельности</p> <p>Владеть навыками подбора и использования программно-технических средств для решения</p>		
--	--	--	--	--

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)	32
- КСР	2
самостоятельная работа	40
Промежуточная аттестация	54
	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	
	о	о	о	о	о

	Ф О	Ф О	Ф О	Ф О	Ф О
Тема 1 Теоретические аспекты информационной безопасности экономических систем	22	4	8	12	10
Тема 2 Понятие информационных угроз и их виды	22	4	8	12	10
Тема 3 Принципы построения и организации системы информационной безопасности	22	4	8	12	10
Тема 4 Информационная безопасность отдельных экономических систем	22	4	8	12	10
Аттестация	54				
КСР	2			2	
Итого	144	16	32	50	40

Содержание разделов и тем дисциплины

Тема 1 Теоретические аспекты информационной безопасности экономических систем.

Системная классификация и общий анализ угроз безопасности информации. Основные концептуальные положения теории защиты информации. Источники угроз информационно безопасности. Защита информации от несанкционированного доступа. Принципиальная схема организации обмена документами, заверенными цифровой подписью. Криптографические методы защиты информации. Программы вирусы и средства антивирусной защиты.

Основные концептуальные положения теории защиты информации. Задачи защиты информации.. Методы идентификации и аутентификации пользователей.. Источники и каналы утечки информации. Концепция комплексной защиты информации. Причины нарушения информационной безопасности в вычислительной сети. Методы контроля доступа. Организационно-правовое обеспечение защиты информации.. Методология создания, организации и обеспечения функционирования системы. Методы контроля информации, обрабатываемой средствами вычислительной техники. Стандарты информационной безопасности и методическое обеспечение

Тема 2 Понятие информационных угроз и их виды

Наиболее распространенные угрозы в интегрированной информационной системе управления предприятием. Уязвимость информационных систем. Требования по обеспечению информационной безопасности корпоративной информационной системы предприятия. Требования к программно-аппаратным средствам. Требования к подсистеме идентификации и аутентификации. Требования к подсистеме управления доступом. Требования к подсистеме протоколирования аудита. Требования к подсистеме защиты повторного использования объектов. Требования к защите критичной информации. Требования к средствам обеспечения целостности. Требования к средствам управления ИБ
Требования к Межсетевому Экрану

Тема 3 Принципы построения и организации системы информационной безопасности

Системы разграничения доступа (полномочий) . Электронный замок. Идентификация и аутентификация пользователей. Регистрация попыток доступа к ПЭВМ. Контроль целостности программной среды и запрет загрузки со съемных носителей. Построение системы защиты распределенных вычислительных сетей от внутренних внешних посягательств на информацию и ресурсы различного назначения. Управление безопасностью в корпоративных распределенных вычислительных системах и сетях связи. Защита документов и товаров с использованием электронной цифровой подписи. Перспективы развития аппаратных средств защиты от несанкционированного доступа к информации

Тема 4 Информационная безопасность отдельных экономических систем

Организация системы информационной безопасности предприятия. Анализ рисков нарушения информационной безопасности предприятия. Разновидности аналитических работ по оценке защищенности

Политика информационной безопасности России

Практические занятия /лабораторные работы организуются, в том числе, в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

На проведение практических занятий / лабораторных работ в форме практической подготовки отводится: очная форма обучения - 4 ч.

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.

-

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 - Практическое задание) для оценки сформированности компетенции ПК-11:

Задание по поиску нормативных документов с использованием «Консультант Плюс»

- 1) Запустим систему Консультант Плюс.
- 2) Создадим папку в системе «Консультант Плюс» с именем Информационная безопасность Иванов (Ваше фамилия) (траектория Избранное – Создать папку).
- 3) Найдем основной закон о защите информации принятый летом 2006 года. Для этого перейдем в Карточку поиска. 4) Для этого заполним поля: «Вид документа», «Дата» и «Название документа».
- 5) Поле «Дата» заполняется с помощью Диапазона дат. 6) Построим список документов
- 7) Нами был найден Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.04.2011) «Об информации, информационных технологиях и о защите информации».
- 8) Откроем найденный закон, дважды щелкнув на его название 9) В текущем документе найдем понятие «Конфиденциальность информации» с помощью кнопки «Найти»
- 10) Поставим закладку рядом с найденным понятием. Для этого щелкнем слева от него и далее выберем «Добавить – Закладки» и «Документы – кнопка Добавить».

11) Вернемся в «Карточку поиска» и выберем «Избранное». В поле «Закладки 18 и документы» появилась закладка.

12) Аналогично поставим закладки для понятий «информация», «электронный документ» и статьи «Защита информации».

13) Добавим найденный закон в папку Информационная безопасность по траектории: Добавить – Папки – Информационная безопасность.

14) Вернемся в «Карточку поиска» и выберем «Избранное». В поле Папки - Информационная безопасность появилась ФЗ №149.

15) Найти документ «Доктрина информационной безопасности Российской Федерации» и Федеральный закон №152-ФЗ «О персональных данных». Сохраним их в папку «Информационная безопасность»

16) В найденных документах поставим закладки для понятий «персональные данные», «уничтожение персональных данных» и правовые методы информационной безопасности.

17) Проверьте наличие созданных закладок.

18) Закончить работу с программой.

5.1.2 Типовые задания (оценочное средство - Практическое задание) для оценки сформированности компетенции ДПК-3:

Задание 1. Наделение прав пользователей в системе 1С:Предприятие

Запуская систему, пользователь должен обязательно работать с какой-либо информационной базой (далее - ИБ). ИБ содержит Конфигурацию, Базу Данных (БД), список пользователей и некоторые другие параметры. Конфигурация состоит из отдельных объектов.

Среди всех объектов, которые есть в конфигурации, имеются объекты, относящиеся, согласно документации, к Прикладным объектам системы.

Конфигурация (в терминах документации 1С:Предприятия) представляет собой совокупность описания структуры данных, алгоритмов обработки, печатных и экранных форм, а также другой информации необходимой для автоматизации той или иной прикладной задачи.

Конфигурацией в системе 1С Предприятие называется совокупность трех взаимосвязанных частей:

- Структуры метаданных
- Набора пользовательских интерфейсов
- Набора прав

Метаданными (данными о данных) называется совокупность объектов метаданных, настроенных на хранение и обработку информации о хозяйственной деятельности конкретного предприятия.

Пользовательским интерфейсом называется совокупность команд главного меню и панелей инструментов, настроенных на работу с конкретными объектами данных – документами, справочниками, журналами и т.д. Как правило, пользовательский интерфейс создается для конкретной категории пользователей. Цель создания интерфейса – обеспечить быстрый доступ пользователей к той информации, которая необходима им в соответствии с их обязанностями.

Права определяют полномочия пользователей на работу с информацией, которая обрабатывается в системе. Совокупность предоставляемых пользователю прав определяется, как правило, кругом его обязанностей.

Критерии оценивания (оценочное средство - Практическое задание)

Оценка	Критерии оценивания
превосходно	Задание выполнено в полном объеме (все задания решены), ответ логичен и обоснован, видно изучение дополнительного материала
отлично	Задание выполнено в полном объеме (все задания решены), есть незначительные погрешности
очень хорошо	Задание выполнено в полном объеме (все задания решены), ответ логичен и обоснован, допущено не более 1 неточности непринципиального характера
хорошо	Задание выполнено в полном объеме (все задания решены), ответ логичен и обоснован, допущены 2-3 неточности непринципиального характера, но обучающийся показывает систему знаний по теме своими ответами на поставленные вопросы
удовлетворительно	Задание выполнено не в полном объеме (решено более 60% заданий), но обучающийся допускает ошибки, нарушена последовательность ответа, но в целом раскрывает содержание основного материала
неудовлетворительно	Задание выполнено не в полном объеме (решено менее 60% заданий), обучающийся дает неверную информацию при ответе на поставленные задачи, допускает грубые ошибки при толковании материала, демонстрирует незнание основных терминов и понятий
плохо	Задание не выполнено, обучающийся демонстрирует полное незнание материала

5.1.3 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ПК-11:

Вопрос 1. Политика безопасности не включает в себя

- а. объект информационной безопасности
- б. обеспечение информационной безопасности
- в. угрозы объекту информационной безопасности
- г. все ответы верны

Вопрос 2. К объектам информационной безопасности на предприятии не относят

- а. информационные ресурсы
- б. средства и системы информатизации
- в. субъекты информационной безопасности
- г. коммерческое предприятие

Вопрос 3. Сегмент деловой информации относится к следующему виду рынка

- а. финансовый
- б. информационный
- в. товарный
- г. услуг
- д. биржевой

Вопрос 4. К свойствам информации как товара относят

- а. репрезентативность
- б. адекватность
- в. несамостоятельность
- г. достоверность
- д. доступность

Вопрос 5. Объекты профессиональной тайны

- а. врачебная тайна
- б. тайна страхования в. тайна связи
- г. тайна усыновления
- д. все ответы верны

5.1.4 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ДПК-3:

Вопрос 1. Объектом информационной безопасности может

- а. коммерческое предприятие
- б. некоммерческое предприятие

в. государственный орган

г. все ответы верны

Вопрос 2. Управление экономическими объектами всегда связано с преобразованием

а. социальной информации

б. экономической информации в. демографической информации

г. юридической информации

Вопрос 3. Свойства информации как товара:

а. неисчерпаемость, сохраняемость, несамостоятельность

б. исчерпаемость, несохраняемость, самостоятельность

в. неисчерпаемость, сохраняемость, самостоятельность

г. исчерпаемость, сохраняемость, несамостоятельность

Вопрос 4. Информация может считаться служебной тайной, если она отвечает следующим требованиям

а. отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости

б. является охраноспособной конфиденциальной информацией ("чужой тайной") другого лица

в. Все ответы верны

г. Все ответы неверны

Вопрос 5. Если ценность информации теряется при ее хранении и/или распространении, то реализуется

а. угроза целостности информации

б. угроза оперативности использования или доступности информации

в. угроза нарушения конфиденциальности информации

г. все ответы верны

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
превосходно	100% правильных ответов
отлично	95-99% правильных ответов

Оценка	Критерии оценивания
очень хорошо	85-94% правильных ответов
хорошо	75-84% правильных ответов
удовлетворительно	60-74% правильных ответов
неудовлетворительно	46-59% правильных ответов
плохо	45% и меньше правильных ответов

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			
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Ошибок нет.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи с отдельным и несущественными недочетами, выполнены все задания в полном объеме	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

<u>Навыки</u>	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 некоторым и недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторым и 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 ПК-11

1. Необходимость обеспечения безопасности в информационных системах.
2. Прогресс информационных технологий и информационная безопасность.
3. Нормативно-правовые аспекты информационной безопасности.
4. Классификация угроз безопасности информационных объектов.
5. Основные виды каналов утечки информации.
6. Умышленные и неумышленные угрозы информационной безопасности.
7. Внешние угрозы информационной безопасности.
8. Мотивы и цели компьютерных преступлений.
9. Статьи уголовного кодекса о компьютерных преступлениях.
10. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.
11. Объекты информационной безопасности на предприятии.
12. Организационные методы обеспечения информационной безопасности.
13. Физическая защита информационных систем.
14. Программно - технические методы обеспечения информационной безопасности.
15. Идентификация и аутентификация.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ДПК-3

16. Доктрина информационной безопасности Российской Федерации.
17. Государственное регулирование информационной безопасности в России.
18. Несанкционированный доступ и защита от него.
19. Проблема информационной безопасности в историческом аспекте.
20. Предупреждение компьютерных преступлений.
21. Типы компьютерных вирусов и защита от них.
22. Человеческие факторы, обуславливающие информационные угрозы.
23. Способы воздействия угроз на информационный объект.
24. Признаки воздействия вирусов на компьютерную систему.

25. Фрагментарный и системный подходы к защите информации.
26. Уголовно-правовая характеристика компьютерных преступлений.
27. Субъективная сторона компьютерных преступлений.
28. Объективная сторона компьютерных преступлений.
29. Способы совершения компьютерных преступлений («за хвост», «маскарад» и др.).
30. Причины и условия, способствующие совершению компьютерных преступлений.
31. Меры предупреждения преступлений в сфере компьютерной информации.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
превосходно	Задание выполнено в полном объеме (все задания решены), ответ логичен и обоснован, видно изучение дополнительного материала
отлично	Задание выполнено в полном объеме (все задания решены), есть незначительные погрешности
очень хорошо	Задание выполнено в полном объеме (все задания решены), ответ логичен и обоснован, допущено не более 1 неточности непринципиального характера
хорошо	Задание выполнено в полном объеме (все задания решены), ответ логичен и обоснован, допущены 2-3 неточности непринципиального характера, но обучающийся показывает систему знаний по теме своими ответами на поставленные вопросы
удовлетворительно	Задание выполнено не в полном объеме (решено более 60% заданий), но обучающийся допускает ошибки, нарушена последовательность ответа, но в целом раскрывает содержание основного материала
неудовлетворительно	Задание выполнено не в полном объеме (решено менее 60% заданий), обучающийся дает неверную информацию при ответе на поставленные задачи, допускает грубые ошибки при толковании материала, демонстрирует незнание основных терминов и понятий
плохо	Задание не выполнено, обучающийся демонстрирует полное незнание

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

Основная литература:

1. Сычев Юрий Николаевич. Защита информации и информационная безопасность : Учебное пособие / Российский экономический университет им. Г.В. Плеханова. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 201 с. - ВО - Бакалавриат. - ISBN 978-5-16-014976-9. - ISBN 978-5-16-107471-8., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=837052&idb=0>.
2. Башлы П.Н. Информационная безопасность и защита информации : Учебник. - Москва : Издательский Центр РИОР, 2013. - 222 с. - ВО - Бакалавриат., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=613461&idb=0>.

Дополнительная литература:

1. Баранова Елена Константиновна. Информационная безопасность. История специальных методов криптографической деятельности : Учебное пособие / Национальный исследовательский университет "Высшая школа экономики"; Национальный исследовательский университет "Высшая школа экономики". - 1. - Москва : Издательский Центр РИОР, 2022. - 236 с. - ВО - Магистратура. - ISBN 978-5-369-01788-3. - ISBN 978-5-16-106992-9. - ISBN 978-5-16-014478-8., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=791676&idb=0>.

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

1. MS Office;
2. ИПС «Консультант +»;
3. ИПС «Гарант»;
4. Поисковые система «Яндекс», «Google»;
5. ЭБС znanium.com;
6. ЭБС «biblio-online.ru».

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 38.04.01 - Экономика.

Автор(ы): Винник Валерия Константиновна, кандидат педагогических наук.

Заведующий кафедрой: Болдыревский Павел Борисович, доктор физико-математических наук.

Программа одобрена на заседании методической комиссии от 12.12.2023, протокол № 6.

