

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

УТВЕРЖДЕНО

решением Ученого совета ННГУ

протокол № 10 от 02.12.2024 г.

Рабочая программа дисциплины

Информационная безопасность

Уровень высшего образования

Бакалавриат

Направление подготовки / специальность

38.03.01 - Экономика

Направленность образовательной программы

Бухгалтерский учет

Форма обучения

очная

г. Нижний Новгород

2025 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.15 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-6: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-6.1: Понимает принципы работы современных информационных технологий ОПК-6.2: Использует принципы работы современных информационных технологий для решения задач профессиональной деятельности	ОПК-6.1: ОПК-6.1: 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-6.2: ОПК-6.2: Знать: основы менеджмента и аудита информационной безопасности Уметь: выявлять информационные риски, выбирать методы управления информационной безопасностью Владеть: принципами менеджмента и аудита информационной безопасности	Доклад-презентация Тест	Зачёт: Контрольные вопросы
ПК-3: Способен анализировать и	ПК-3.1: Формирует, анализирует и	ПК-3.1: Знать: нормативно-правовые	Доклад-презентация Тест	

интерпретировать данные отечественной и зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений	интерпретирует финансово-экономическую информацию ПК-3.2: Выявляет тенденции и использует результаты анализа информации для принятия управленческих решений	и организационные требования защиты информации Уметь: использовать современные средства и технологии защиты информации Владеть: способами обработки и анализа данных с применением систем информационной безопасности ПК-3.2: Знать: современные возможности систем защиты информации при обработке отчетности в целях принятия управленческих решений Уметь: использовать информационные технологии при решении профессиональных задач Владеть: навыками работы с современными системами защиты информации при принятии управленческих решений		Зачёт: Контрольные вопросы
---	--	---	--	-------------------------------

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	2
Часов по учебному плану	72
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	16
- занятия семинарского типа (практические занятия / лабораторные работы)	16
- КСР	1
самостоятельная работа	39
Промежуточная аттестация	0 Зачёт

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	
	0 Ф 0	0 Ф 0	0 Ф 0	0 Ф 0	0 Ф 0
Тема 1 Теоретические аспекты информационной безопасности экономических систем	13	3	2	5	8
Тема 2. Понятие информационных угроз и их виды	13	3	2	5	8
Тема 3. Государственное регулирование информационной безопасности	11	3	2	5	6
Тема 4. Подходы, принципы, методы и средства обеспечения безопасности	13	3	3	6	7
Тема 5. Организация системы защиты информации	12	2	4	6	6
Тема 6. Менеджмент и аудит систем информационной безопасности	9	2	3	5	4
Аттестация	0				
КСР	1			1	
Итого	72	16	16	33	39

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:

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 - Доклад-презентация) для оценки сформированности компетенции ОПК-6:

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. 19.Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

5.1.2 Типовые задания (оценочное средство - Доклад-презентация) для оценки сформированности компетенции ПК-3:

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. 17.Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

Критерии оценивания (оценочное средство - Доклад-презентация)

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 - Тест) для оценки сформированности компетенции ОПК-6:

1. Информационная война – это...

А. злословие в адрес другого человека;

Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;

В. акт применения информационного оружия.

2. Информационная безопасность – это...

А. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);

Б. предотвращение зла наносимого государственным структурам;

В. проведение природоохранных мероприятий.

3. 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.

4. 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.

5. Информация может составлять коммерческую тайну, если:

А. к ней нет свободного доступа на законном основании;

Б. содержится в учредительных документах;

В. содержится в бухгалтерском балансах.

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

1. Принцип системности означает:

А. Комплексный анализ угроз, средств защиты от этих угроз;

Б. Прозрачность для легальных пользователей;

В. Эшелонированность обороны.

2. Политика безопасности разрабатывается применительно к

- А. Одному верхнему уровню управления;
- Б. Трем уровням управления (верхнему, среднему и нижнему);
- В. Решению акционеров компании.
3. Программа безопасности синхронизируется с жизненным циклом системы?
- А. да;
- Б. нет;
- В. отчасти.
4. В политике безопасности основным принципом является усиление самого слабого звена?
- А. нет;
- Б. да;
- В. отчасти.
5. Криптография – это..?
- А. наука о шифровании (преобразовании) информации;
- Б. наука о вирусах;
- В. наука об информационных войнах.

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

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

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатор)	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				

атор достиж ения							
<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 отдельными 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 некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продemonстрирован 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-6

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности. 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. Информационные угрозы для государства. 10. Информационные угрозы для компании. 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. Государственное регулирование информационной безопасности. 22. Деятельность международных организаций в сфере информационной безопасности. 23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации. 24. Доктрина информационной безопасности России. 25. Уголовно-правовой контроль над компьютерной преступностью в России. 26. Федеральные законы по ИБ в РФ. 27. Политика безопасности и ее принципы. 28. Фрагментарный и системный подход к защите информации.

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

1. Методы и средства защиты информации. 2. Организационное обеспечение ИБ. 3. Организация конфиденциального делопроизводства. 4. Комплекс организационно-технических мероприятий по обеспечению защиты информации. 5. Инженерно-техническое обеспечение компьютерной безопасности. 6. Организационно-правовой статус службы безопасности. 7. Защита информации в Интернете. 8. Электронная почта и ее защита. 9. Защита от компьютерных вирусов. 10. Популярные антивирусные программы и их классификация. 11. Организация системы защиты информации экономических объектов. 12. Криптографические методы защиты информации. 13. Этапы построения системы защиты информации. 14. Оценка эффективности инвестиций в информационную безопасность. 15. План обеспечения непрерывной работы и восстановления функционирования автоматизированной

информационной системы. 16. Управление информационной безопасности на государственном уровне. 17. Аудит ИБ автоматизированных банковских систем. 18. Электронная коммерция и ее защита. 19. Менеджмент и аудит информационной безопасности на уровне предприятия. 20. Информационная безопасность предпринимательской деятельности. 21. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов. 22. Какие признаки классифицируют нейронные сети. 23. Виды обучения нейронных сетей. 24. Типы нейронных сетей применяются в социально-экономических исследованиях. 25. Этапы обучения нейронной сети. 26. Применение искусственного интеллекта для выявления информационных угроз. 27. Применение нейросетевых технологий в системе защиты информации. 28. Угрозы использования искусственного интеллекта.

Критерии оценивания (оценочное средство - Контрольные вопросы)

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

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

Основная литература:

- Басыня Е. А. Сетевая информационная безопасность : учебник / Басыня Е. А. - Москва : НИЯУ МИФИ, 2023. - 224 с. - Книга из коллекции НИЯУ МИФИ - Информатика. - ISBN 978-5-7262-2949-2., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=884189&idb=0>.
- Гилязова Р. Н. Информационная безопасность. Лабораторный практикум / Гилязова Р. Н. - 3-е изд., стер. - Санкт-Петербург : Лань, 2022. - 44 с. - Книга из коллекции Лань - Информатика. - ISBN 978-5-8114-9138-4., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=880909&idb=0>.
- Чернова Е. В. Информационная безопасность человека : учебное пособие / Е. В. Чернова. - 3-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 327 с. - (Высшее образование). - ISBN 978-5-534-16772-6. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=871518&idb=0>.

Дополнительная литература:

- Пугин В. В. Основы информационной безопасности : методические указания к лабораторным работам для студентов очной формы обучения по направлению подготовки 10.05.02 «информационная безопасность телекоммуникационных систем» / Пугин В. В. - Самара : ПГУТИ, 2021. - 39 с. - Книга из коллекции ПГУТИ - Информатика., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=859685&idb=0>.
- Никулин В. В. Информационная безопасность. Лабораторный практикум : учебно-методическое пособие для студентов направления подготовки 09.03.03 прикладная информатика / Никулин В. В. - Брянск : Брянский ГАУ, 2021. - 84 с. - Книга из коллекции Брянский ГАУ - Информатика.,

<https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=860117&idb=0>.

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

Консультант плюс

1. www.cyberpol.ru Компьютерная преступность и способы борьбы.
2. www.iso27000.ru Информационный портал, посвященный вопросам управления информационной безопасностью.
3. www.itsec.ru Интернет-журнал «Информационная безопасность».
4. www.inside-zi.ru Информационно-методический журнал «Защита информации. Инсайд».
5. www.kaspersky.ru Лаборатория Касперского.
6. www.comss.ru.
7. www.drweb.com.
8. www.esethod32.ru.
9. www.kaspersky.ru.
10. <http://free.avg.com>
11. www.kaspersky.ru/removaltools
12. www.freedrweb.com/cureit/
13. www.computerologia.ru
14. www.free-av.com
15. www.mcafee.com
16. <http://www.viruslab.ru/>
17. www.bitdefender.com.

7. Материально-техническое обеспечение дисциплины (модуля)

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

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 38.03.01 - Экономика.

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

Заведующий кафедрой: Трифонов Юрий Васильевич, доктор экономических наук.

Программа одобрена на заседании методической комиссии от 12.11.2024 г., протокол № № 5.