

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Арзамасский филиал ННГУ - Психолого-педагогический факультет

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

Экономика и финансы организаций (предприятий)

Форма обучения

очно-заочная

г. Арзамас

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-5: Способен использовать современные информационные технологии и программные средства при решении профессиональных задач. | ОПК-5.1: Осуществляет выбор инструментальных и программных средств для решения профессиональных задач. ОПК-5.2: Использует современные информационные технологии и программные средства для решения профессиональных задач. | ОПК-5.1: Знать основные методы, способы и средства преобразования информации Уметь работать с компьютером как средством управления информацией Владеть основными способами обнаружения информационных угроз и использования с антивирусных программ ОПК-5.2: Знать функции и задачи менеджмента и аудита систем информационной безопасности Уметь выявлять информационные угрозы, выбирать методы и средства управления и аудита систем информационной безопасности Владеть принципами менеджмента и аудита систем информационной безопасности | Тест Задания | Экзамен: Контрольные вопросы |
| ПК-3: Способен анализировать и интерпретировать данные отечественной и зарубежной финансовой, | ПК-3.1: Формирует, анализирует и интерпретирует финансово-экономическую информацию. ПК-3.2: Выявляет тенденции и использует | ПК-3.1: Знать нормативные, организационные средства защиты информации при формировании отчетности, планов, проектов хозяйствующих субъектов | Тест Задания | Экзамен: Контрольные вопросы |

| | | | | |
|--|--|---|--|--|
| бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений | результаты анализа информации для принятия управленческих решений. | <p>Уметь использовать современные средства и технологии защиты данных. Владеть средствами сбора, обработки и анализа данных с применением систем информационной безопасности.</p> <p>ПК-3.2: Знать: современные средства и возможности систем информационной безопасности при обработке отчетности в целях принятия управленческих решений Уметь: использовать средства информационных технологий при решении профессиональных задач. Владеть: навыками работы с современными системами информационной безопасности при принятии управленческих решений</p> | | |
|--|--|---|--|--|

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

| | |
|--|-----------------------------|
| | очно-заочная |
| Общая трудоемкость, з.е. | 3 |
| Часов по учебному плану | 108 |
| в том числе | |
| аудиторные занятия (контактная работа): | |
| - занятия лекционного типа | 6 |
| - занятия семинарского типа (практические занятия / лабораторные работы) | 8 |
| - КСР | 2 |
| самостоятельная работа | 56 |
| 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 | Самостоятельная |

| | | взаимодействии с преподавателем), часы из них | | | работа обучающегося, часы |
|--|------------------|--|--|------------------|---------------------------------|
| | | Занятия лекционного типа | Занятия семинарского типа (практические занятия/ лабора торные работы), часы | Всего | |
| | о з ф о | о з ф о | о з ф о | о з ф о | о з ф о |
| Тема 1. Теоретические аспекты информационной безопасности экономических систем | 18 | 2 | 2 | 4 | 14 |
| Тема 2. Принципы построения системы информационной безопасности | 18 | 2 | 2 | 4 | 14 |
| Тема 3. Организация системы защиты информации экономических систем | 17 | 1 | 2 | 3 | 14 |
| Тема 4. Информационная безопасность отдельных экономических систем | 17 | 1 | 2 | 3 | 14 |
| Аттестация | 36 | | | | |
| КСР | 2 | | | 2 | |
| Итого | 108 | 6 | 8 | 16 | 56 |

Содержание разделов и тем дисциплины

Тема 1. Теоретические аспекты информационной безопасности экономических систем

Основные понятия. Экономическая информация как товар и объект безопасности. Понятие информационных угроз и их виды. Информационные угрозы. Вредоносные программы. Компьютерные преступления и наказания.

Тема 2. Принципы построения системы информационной безопасности

Государственное регулирование информационной безопасности. Подходы, принципы, методы и средства обеспечения безопасности. Организационно-техническое обеспечение компьютерной безопасности. Защита от компьютерных вирусов. Электронная цифровая подпись и особенности ее применения. Защита информации в Интернете.

Тема 3. Организация системы защиты информации экономических систем

Этапы построения системы защиты информации. Политика безопасности. Оценка эффективности инвестиций в информационную безопасность.

Тема 4. Информационная безопасность отдельных экономических систем

Обеспечение информационной безопасности автоматизированных банковских систем (АБС).

Информационная безопасность электронной коммерции (ЭК). Обеспечение компьютерной безопасности учетной информации.

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=2142>.

Иные учебно-методические материалы:

Учебно-методические документы, регламентирующие самостоятельную работу
адреса доступа к документам

<https://arz.unn.ru/sveden/document/>

https://arz.unn.ru/pdf/Metod_all_all.pdf

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-5:

1. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

1. Список стандартов, процедур и политик для разработки программы безопасности
2. Текущая версия ISO 17799
3. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
4. Открытый стандарт, определяющий цели контроля

2. Из каких четырех доменов состоит CobiT?

1. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
2. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
3. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
4. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

3. Что представляет собой стандарт ISO/IEC 27799?

1. Стандарт по защите персональных данных о здоровье
2. Новая версия BS 17799
3. Определения для новой серии ISO 27000
4. Новая версия NIST 800-60

4. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

1. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
2. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
3. COSO учитывает корпоративную культуру и разработку политик
4. COSO – это система отказоустойчивости

5. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

1. NIST и OCTAVE являются корпоративными
2. NIST и OCTAVE ориентирован на ИТ
3. AS/NZS ориентирован на ИТ
4. NIST и AS/NZS являются корпоративными

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

1. Кто является основным ответственным за определение уровня классификации информации?

1. Руководитель среднего звена
2. Высшее руководство
3. Владелец
4. Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

1. Сотрудники
2. Хакеры
3. Атакующие
4. Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

3. Улучшить контроль за безопасностью этой информации

4. Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

2. Необходимый уровень доступности, целостности и конфиденциальности

3. Оценить уровень риска и отменить контрмеры

4. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

1. Владельцы данных

2. Пользователи

3. Администраторы

4. Руководство

Критерии оценивания (оценочное средство - Тест)

| Оценка | Критерии оценивания |
|---------------------|----------------------------|
| отлично | 85-100% правильных ответов |
| хорошо | 66-84% правильных ответов |
| удовлетворительно | 50-65% правильных ответов |
| неудовлетворительно | меньше 50% |

5.1.3 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-5:

1. Ответьте на вопрос: «Что подразумевается под сбоем оборудования?», «Что означает случайная потеря информации?»

2. Определите методы защиты:

3. периодическое архивирование программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);

4. автоматическое резервирование файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.
5. периодическая проверка исправности оборудования (в частности - поверхности жесткого диска) при помощи специальных программ.

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

1. Определить место и роль информационной безопасности при использовании личного компьютера и мобильных устройств. Охарактеризовать последствия взлома ваших личных аккаунтов в соц. сетях, электронной почты.
2. Вы работаете бухгалтером-экономистом. Под Вашим логином и паролем со счета предприятия ушли большие суммы денег неизвестным контрагентам. Последствия, Ваша ответственность.
3. Вы работаете клиентским менеджером. С Вашего компьютера похищена клиентская база. Конкуренты предложили Вашим клиентам более привлекательные условия и цены. Последствия. Ваша ответственность.
4. Приведите примеры нарушения информационной безопасности из собственной практики. Охарактеризуйте последствия. Какие действия предпринимало руководство Вашей организации? Как в дальнейшем складывалась карьера виновных сотрудников?

Критерии оценивания (оценочное средство - Задания)

| Оценка | Критерии оценивания |
|------------|---|
| зачтено | выставляется студенту, если задание выполнено полностью; в решении задач отсутствуют ошибки и пробелы, возможны неточности, не являющиеся следствием незнания или непонимания учебного материала. |
| не зачтено | выставляется студенту, если задание выполнено не полностью; имеются существенные ошибки и пробелы в решении задач, являющиеся следствием незнания или непонимания учебного материала. |

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

Шкала оценивания сформированности компетенций

| Уровень сформированности компетенций (индикатора достижения компетенций) | неудовлетворительно | удовлетворительно | хорошо | отлично |
|--|--|--|---|---|
| | не зачтено | зачтено | | |
| <u>Знания</u> | 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, без ошибок |
| <u>Умения</u> | 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 с отдельными несущественными недочетами, выполнены все задания в полном объеме |
| <u>Навыки</u> | 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 навыки при решении нестандартных задач без ошибок и недочетов |

Шкала оценивания при промежуточной аттестации

| Оценка | | Уровень подготовки |
|------------|---------------------|--|
| зачтено | отлично | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично» |
| | хорошо | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «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». |

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-5

1. Прогресс информационных технологий и информационная безопасность.
2. Предупреждение компьютерных преступлений.
3. Признаки воздействия вирусов на компьютерную систему. Системный подход к защите информации.
4. История вредоносных программ. Защита учетной информации коммерческих фирм.
5. Методы и средства обеспечения информационной безопасности.
6. Программно-технические методы обеспечения информационной безопасности.
7. Идентификация и аутентификация.
8. Государственное регулирование информационной безопасности в России.
9. Защита от компьютерных вирусов.
10. Электронная цифровая подпись и особенности ее применения.
11. Защита информации в Интернете.
12. Организация системы защиты информации экономических систем.
13. Этапы построения системы защиты информации.
14. Политика безопасности.
15. Информационная безопасность электронной коммерции (ЭК).
16. Сущность криптографических методов.

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

1. Необходимость обеспечения безопасности в информационных системах.
2. Классификация угроз безопасности информационных объектов.
3. Основные виды каналов утечки информации.
4. Естественные угрозы информационной безопасности.
5. Внешние угрозы информационной безопасности.
6. Мотивы и цели компьютерных преступлений.
7. Человеческие факторы, обуславливающие информационные угрозы.
8. Способы воздействия угроз на информационный объект.
9. Нормативно-правовая характеристика компьютерных преступлений.
10. Причины и условия, способствующие совершению компьютерных преступлений.

11. Меры предупреждения преступлений в сфере компьютерной информации.
12. Исторические аспекты компьютерных преступлений.
13. Экономическая информация как объект безопасности.
14. Виды тайн и как их сохранить.
15. Причины разглашения конфиденциальной информации.
16. Разглашение и утечка информации.
17. Теоретические аспекты информационной безопасности экономических систем.
18. Объекты информационной безопасности на предприятии.
19. Физическая защита информационных систем.
20. Организационно-административные мероприятия обеспечения компьютерной безопасности.

Критерии оценивания (оценочное средство - Контрольные вопросы)

| Оценка | Критерии оценивания |
|---------------------|---|
| отлично | выставляется, когда студент глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется с ситуационными заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок. |
| хорошо | выставляется, если студент твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при анализе информации. |
| удовлетворительно | выставляется в том случае, при котором студент освоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении анализа информации. |
| неудовлетворительно | выставляется студенту, в ответе которого обнаружились существенные пробелы в знании основного содержания учебной программы дисциплины и / или неумение использовать полученные знания. |

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", 2022. - 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=791742&idb=0>.
2. Информационная безопасность и защита информации : практикум / Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А. - Дубна : Государственный университет «Дубна», 2020. - 85 с. - Рекомендовано учебно-методическим советом университета «Дубна» в качестве практикума для студентов, обучающихся по направлениям подготовки «Системный анализ и управление», «Прикладная информатика», «Прикладная математика и информатика (магистратура)». - Библиогр.: доступна в карточке книги, на сайте ЭБС Лань. - Книга и, <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=730800&idb=0>.
3. Суворова Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. - Москва : Юрайт, 2022. - 253 с. - (Высшее образование). - URL: <https://urait.ru/bcode/496741> (дата обращения: 14.08.2022). - ISBN 978-5-534-13960-0 : 1039.00. - Текст : электронный // ЭБС "Юрайт", <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=820839&idb=0>.

Дополнительная литература:

1. Нетёсова О. Ю. Информационные системы и технологии в экономике / Нетёсова О. Ю. - 3-е изд. ; испр. и доп. - Москва : Юрайт, 2022. - 178 с. - (Высшее образование). - URL: <https://urait.ru/bcode/491479> (дата обращения: 05.01.2022). - ISBN 978-5-534-08223-4 : 499.00. - Текст : электронный // ЭБС "Юрайт", <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=789321&idb=0>.
2. Полякова Т. А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум / под редакцией Т. А. Поляковой, А. А. Стрельцова. - Москва : Юрайт, 2022. - 325 с. - (Высшее образование). - URL: <https://urait.ru/bcode/498844> (дата обращения: 14.08.2022). - ISBN 978-5-534-03600-8 : 1289.00. - Текст : электронный // ЭБС "Юрайт", <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=822057&idb=0>.
3. Васильева И. Н. Криптографические методы защиты информации / Васильева И. Н. - Москва : Юрайт, 2022. - 349 с. - (Высшее образование). - URL: <https://urait.ru/bcode/489919> (дата обращения: 05.01.2022). - ISBN 978-5-534-02883-6 : 1079.00. - Текст : электронный // ЭБС "Юрайт", <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=787933&idb=0>.

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

Лицензионное программное обеспечение: операционная система: Microsoft Windows.

Лицензионное программное обеспечение: Microsoft Office.

Электронные библиотечные системы и библиотеки:

Электронная библиотечная система "Лань" <https://e.lanbook.com/>

Электронная библиотечная система "Консультант студента" <http://www.studentlibrary.ru/>

Электронная библиотечная система "Юрайт" <http://www.urait.ru/ebs>

Электронная библиотечная система "Znanium" <http://znanium.com/>

Электронно-библиотечная система Университетская библиотека ONLINE <http://biblioclub.ru/>

Фундаментальная библиотека ННГУ www.lib.unn.ru/

Сайт библиотеки Арзамасского филиала ННГУ. – Адрес доступа: lib.arz.unn.ru

Ресурс «Массовые открытые онлайн-курсы Нижегородского университета им. Н.И. Лобачевского»
<https://mooc.unn.ru/>

Портал «Современная цифровая образовательная среда Российской Федерации»
<https://online.edu.ru/public/promo>

Официальный сайт Федеральной службы государственной статистики [Электронный ресурс]. –
Режим доступа: www.gks.ru

ГАРАНТ. Информационно-правовой портал [Электронный ресурс].– Режим доступа:
<http://www.garant.ru>

«КонсультантПлюс» [Электронный ресурс].– Режим доступа: <http://www.consultant.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 38.03.01 - Экономика.

Автор(ы): Статуев Алексей Анатольевич, кандидат педагогических наук, доцент.

Рецензент(ы): Фокеев Максим Игоревич, кандидат педагогических наук.

Заведующий кафедрой: Нестерова Лариса Юрьевна, кандидат педагогических наук.

Программа одобрена на заседании методической комиссии от 27.11.2024 г., протокол № №9.