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

Факультет естественных и математических наук

УТВЕРЖДЕНО
решением президиума ученого совета ННГУ
(протокол от 14.12. 2021 г. № 4)

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(наименование дисциплины)

Уровень высшего образования
бакалавриат
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
38.03.01 Экономика
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Экономика и финансы организаций (предприятий)
(указывается профиль / магистерская программа / специализация)

Форма обучения
очная/очно-заочная
(очная / очно-заочная / заочная)

Арзамас
2022 год

1. Место дисциплины (модуля) в структуре ООП

Дисциплина Б1.О.15 «Информационная безопасность» относится к обязательной части ООП направления подготовки 38.03.01 Экономика, направленность (профиль) Экономика и финансы организаций (предприятий).

Дисциплина предназначена для освоения студентами очной и очно-заочной формы обучения во 2 семестре.

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** (дескрипторы компетенции)	
ПК-3. Способен анализировать и 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	ПК 3.1. Формирует, анализирует и интерпретирует финансово-экономическую информацию	**Знать** нормативные, организационные средства защиты информации при формировании отчетности, планов, проектов хозяйствующих субъектов **Уметь** использовать современные средства и технологии защиты данных. **Владеть** средствами сбора, обработки и анализа данных с применением систем информационной безопасности.	*Тест* *Эссе* *Практические задания*
	ПК 3.2. Выявляет тенденции и использует результаты анализа информации для принятия управленческих решений	**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	*Тест* *Эссе* *Практические задания*
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	**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	*Тест* *Эссе* *Практические задания*
	ОПК-5.2 Использует современные информационные технологии и программные средства для решения профессиональных задач	**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* *Эссе* *Практические задания*

3. Структура и содержание дисциплины

3.1.Структура дисциплины

Трудоемкость	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	4 з.е.	4 з.е.	
часов по учебному плану, из них	144	144	
Контактная работа, в том числе: аудиторные занятия:			
– занятия лекционного типа	32	6	
– занятия семинарского типа	32	8	
– контроль самостоятельной работы	2	2	
Промежуточная аттестация экзамен	36	36	
Самостоятельная работа	42	92	

3.2. Содержание дисциплины

Наименование разделов (Р) или тем (Т) дисциплины (модуля), Форма(ы) промежуточной аттестации по дисциплине	Всего (часы)			Контактная работа (работа во взаимодействии с преподавателем), часы, из них												Самостоятельная работа обучающегося, часы, в период					
				Занятия лекционного типа			Занятия семинарского типа (в т.ч. текущий контроль успеваемости)						Контроль самостоятельной работы			промежуточной аттестации (контроля)			теоретического обучения		
							семинары, практические занятия			лабораторные работы											
	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная
Тема 1 Теоретические аспекты информационной безопасности экономических систем	**26**	**26**		6	2		10	2											10	22	
Тема 2 Принципы построения системы информационной безопасности	**32**	**28**		10	2		10	2											12	24	
Тема 3 Организация системы защиты информации экономических систем	**24**	**25**		8	1		6	2											10	22	
Тема 4 Информационная безопасность отдельных экономических систем	**24**	**27**		8	1		6	2											10	24	
В том числе текущий контроль	**2**	**2**											**2**	**2**							
Экзамен	**36**	**36**														**36**	**36**				
ИТОГО	**144**	**144**		**32**	**6**		**32**	**8**					**2**	**2**		**36**	**36**		**42**	**92**	

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.

Текущий контроль успеваемости реализуется в рамках занятий семинарского типа, групповых или индивидуальных консультаций.

4. Учебно-методические обеспечение самостоятельной работы студентов

Самостоятельная работа является важнейшей составной частью учебного процесса и обязанностью каждого студента.

Самостоятельная работа студентов состоит в проработке теоретического материала, выполнении самостоятельных заданий в конце каждого практического занятия и выполнении внеаудиторных самостоятельных заданий (домашние задания и дополнительные задания по углубленному изучению разделов дисциплины). К самостоятельной работе студентов относится подготовка к экзамену.

Для обеспечения самостоятельной работы обучающихся используется электронный курс «Информационная безопасность» - https://e-learning.unn.ru/course/view.php?id=2142, созданный в системе электронного обучения ННГУ: https://e-learning.unn.ru.

Методические рекомендации к самостоятельной работе

Методические рекомендации к самостоятельному выполнению практических заданий

1. Внимательно прочитайте теоретический материал – конспект, составленный на лекционном занятии, материал учебника, пособия. Выпишите формулы из конспекта по изучаемой теме.
2. Выпишите ваш вариант задания, предложенного в методических указаниях по дисциплине, в соответствии с порядковым номером.
3. Решите предложенную задачу.
4. В случае необходимости воспользуйтесь справочными данными.
5. Проанализируйте полученный результат.
6. Решение задач должно сопровождаться необходимыми пояснениями. Расчётные формулы (при необходимости) приводите на отдельной строке, выделяя из текста, с указанием размерности величин. Формулы записывайте сначала в общем виде (буквенное выражение), затем подставляйте числовые значения без указания размерностей, после чего приведите конечный результат расчётной величины.

Показатели результатов работы для самопроверки:

- грамотная запись условия задачи и ее решения;
- грамотное использование формул;
- грамотное использование справочной литературы;
- обоснование решения задачи.

Методические рекомендации к подготовке докладов, эссе

Доклады, по сути своей, близки к рефератам, однако их область существенно уже. Подготовка доклада позволяет основательно изучить интересующий вопрос, изложить материал в компактном и доступном виде, привнести в текст полемику, приобрести навыки научно-исследовательской работы, устной речи, ведения научной дискуссии. В ходе подготовки доклада могут быть подготовлены презентации, раздаточные материалы. Доклады могут зачитываться и обсуждаться на семинарских занятиях, студенческих научных конференциях. При этом трудоемкость доклада, подготовленного для конференции обычно выше.

Эссе – небольшая по объему самостоятельная письменная работа на тему, предложенную преподавателем или выбранную студентом. Роль этой формы самостоятельной работы особенно важна при формировании компетенций, предполагающих приобретение основ знаний предметной области, формирования мировоззрения.

Эссе должно содержать чёткое изложение сути поставленной проблемы, включать самостоятельно проведенный анализ этой проблемы с использованием концепций и аналитического инструментария соответствующей дисциплины, выводы, обобщающие авторскую позицию по поставленной проблеме.

Структура эссе

1. *Титульный лист*.

2. *Введение* – суть и обоснование выбора данной темы, состоит из ряда компонентов, связанных логически и стилистически. На этом этапе очень важно правильно сформулировать вопрос, на который вы собираетесь найти ответ в ходе своего исследования. При работе над введением могут помочь ответы на следующие вопросы: «Надо ли давать определения терминам, прозвучавшим в теме эссе?», «Почему тема, которую я раскрываю, является важной в настоящий момент?».

3. *Основная часть* – теоретические основы выбранной проблемы и изложение основного вопроса. Данная часть предполагает развитие аргументации и анализа, а также обоснование их, исходя из имеющихся данных, других аргументов и позиций по этому вопросу. В этом заключается основное содержание эссе и это представляет собой главную трудность. Поэтому, большое значение имеют подзаголовки, на основе которых осуществляется структурирование аргументации; именно здесь необходимо обосновать (логически, используя данные или строгие рассуждения) предлагаемую аргументацию/анализ. Там, где это необходимо, в качестве аналитического инструмента можно использовать графики, диаграммы и таблицы.

В процессе построения эссе необходимо помнить, что один абзац должен содержать только одно утверждение и соответствующее доказательство, подкрепленное графическим и иллюстративным материалом. Следовательно, наполняя содержанием разделы аргументацией (соответствующей подзаголовкам), необходимо в пределах абзаца ограничить себя рассмотрением одной главной мысли. Хорошо проверенный (и для большинства – совершено необходимый) способ построения любого эссе – использование подзаголовков для обозначения ключевых моментов аргументированного изложения: это помогает посмотреть на то, что предполагается сделать (и ответить на вопрос, хорош ли замысел). Такой подход поможет следовать точно определенной цели в данном исследовании. Эффективное использование подзаголовков - не только обозначение основных пунктов, которые необходимо осветить. Их последовательность может также свидетельствовать о наличии или отсутствии логичности в освещении темы.

4. *Заключение* – обобщения и аргументированные выводы по теме с указанием области ее применения и т.д. Подытоживает эссе или еще раз вносит пояснения, подкрепляет смысл и

значение изложенного в основной части. Методы, рекомендуемые для составления заключения: повторение, иллюстрация, цитата, впечатляющее утверждение. Заключение может содержать такой очень важный, дополняющий эссе элемент, как указание на применение (импликацию) исследования, не исключая взаимосвязи с другими проблемами

Формы эссе могут значительно дифференцироваться. В некоторых случаях это может быть анализ собранных обучающимся конкретных данных по изучаемой проблеме, анализ материалов из средств массовой информации, подробный разбор предложенной преподавателем проблемы с развёрнутыми пояснениями и анализом примеров, иллюстрирующих изучаемую проблему и т.д.

Качество работы оценивается по следующим критериям: самостоятельность выполнения, способность аргументировать положения и выводы, обоснованность, четкость, лаконичность, оригинальность постановки проблемы, уровень освоения темы и изложения материала (обоснованность отбора материала, использование первичных источников, способность самостоятельно осмыслять факты, структура и логика изложения).

В целом при написании письменных работ следует обратить внимание на следующие рекомендации:

1. Выбор темы письменной работы. Тема письменной работы выбирается студентом на основе его научного интереса. Также помощь в выборе темы может оказать преподаватель.
2. Планирование написания письменной работы. План написания письменной работы должен начинаться с выбора и формулировки проблемы, далее следует сбор и изучение исходного материала, поиск литературы и анализ собранного материала. В заключении работа оформляется письменно, как правило, в электронном виде и на бумажном носителе.
3. Обсуждение работы (на занятии, в студенческом научном обществе, на конференции и т.п.).

Методические рекомендации к подготовке устного опроса на занятии

1. При подготовке сообщения, ответа используйте несколько источников литературы по выбранной теме (вопросу), используйте печатные издания и источники электронных библиотек или Интернет-ресурсов.
2. Сделайте цитаты из книг и статей по выбранной теме (обратите внимание на непонятные слова и выражения, уточните их значение в справочной литературе).
3. Проанализируйте собранный материал и составьте план сообщения или ответа, акцентируя внимание на наиболее важных моментах.
4. Напишите основные положения сообщения или ответа в соответствии с планом, выписывая по каждому пункту несколько предложений.
5. Перескажите текст сообщения или ответа, корректируя последовательность изложения материала.
6. Подготовленное сообщение может сопровождаться презентацией, иллюстрирующей его основные положения.

Показатели результатов работы для самопроверки:

- полнота и качественность информации по заданной теме;
- свободное владение материалом сообщения или доклада;
- логичность и четкость изложения материала;
- наличие и качество презентационного материала.

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 промежуточной аттестации по дисциплине

5.1. Описание шкал оценивания результатов обучения по дисциплине

В ходе промежуточной аттестации по дисциплине осуществляется оценка сформированности компонентов компетенций (полнота знаний/ наличие умений/ навыков), т.е. результатов обучения, указанных в таблице п.2 настоящей рабочей программы, на основе оценки усвоения содержания дисциплины.

Обобщенная оценка сформированности компонентного состава компетенции в ходе промежуточной аттестации по дисциплине проводится на основе учета текущей успеваемости в ходе освоения дисциплины и учета результата сдачи промежуточной аттестации.

Выявленные признаки несформированности компонентов (индикаторов) хотя бы одной компетенции не позволяют выставить интегрированную положительную оценку сформированности компетенций и освоения дисциплины на данном этапе обучения.

Обобщенная оценка сформированности компонентного состава компетенций на промежуточной аттестации, которая вносится в зачетно-экзаменационную ведомость по дисциплине и зачетную книжку студента, осуществляется по следующей оценочной шкале.

Шкала оценки сформированности компонентного состава компетенций на промежуточной аттестации

Оценка		**Уровень подготовки**
Зачтено	Отлично	сформированность компонентного состава (индикаторов) компетенций соответствует требованиям компетентностной модели будущего выпускника на данном этапе обучения, основанным на требованиях ОС ННГУ по направлению подготовки, студент готов самостоятельно решать стандартные и нестандартные профессиональные задачи в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы
	Хорошо	сформированность компонентного состава (индикаторов) компетенций соответствует требованиям компетентностной модели будущего выпускника на данном этапе обучения, основанным на требованиях ОС ННГУ по направлению подготовки, но студент готов самостоятельно решать только различные стандартные профессиональные задачи в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы
	Удовлетвори-тельно	сформированность компонентного состава (индикаторов) компетенций соответствует в целом требованиям компетентностной модели будущего выпускника на данном этапе обучения, основанным на требованиях ОС ННГУ по направлению подготовки, но студент способен решать лишь минимум стандартных профессиональных задач в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы
Не зачтено	Неудовлетвор ительно	сформированность компонентного состава (индикаторов) компетенций не соответствует требованиям компетентностной модели будущего выпускника на данном этапе обучения, основанным на требованиях ОС ННГУ по направлению подготовки, студент не готов решать профессиональные задачи в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы

Шкала оценивания сформированности компетенции

Уровень сформированности компетенции (индикатора достижения компетенции)				
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
	не зачтено	**зачтено**		
Знания	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

				требованиям программы подготовки, без ошибок.
Умения	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 с отдельными несущественными недочетами, выполнены все задания в полном объеме.
Навыки	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 навыки при решении нестандартных задач без ошибок и недочетов.

5.2 Критерии и процедуры оценивания результатов обучения по дисциплине

Критерии оценки практических заданий

Оценивание знаний, умений и навыков, приобретенных в ходе решения практических задач, осуществляется по шкале «зачтено» - «не зачтено».

«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.

Критерии оценки тестирования

Оценка **«отлично»** - 85-100% правильных ответов;
Оценка **«хорошо»** 66-84% правильных ответов;
Оценка **«удовлетворительно»** – 50-65% правильных ответов;
Оценка **«неудовлетворительно»** - меньше 50%.

Критерии оценки эссе

Оценка **«отлично»** - Эссе полностью раскрывает основные вопросы теоретического материала. Студент приводит информацию из первоисточников и изданий периодической печати, приводит практические примеры, отвечает на дополнительные вопросы преподавателя и студентов (в процессе выступления с докладом).

Оценка **«хорошо»** - Эссе частично раскрывает основные вопросы теоретического материала. Студент приводит информацию из первоисточников, отвечает на дополнительные вопросы преподавателя и студентов (в процессе выступления с докладом), но при этом дает не четкие ответы, без достаточно их аргументации.

Оценка **«удовлетворительно»** - Эссе в общих чертах раскрывает основные вопросы теоретического материала. Студент приводит информацию только из учебников. При ответах на дополнительные вопросы (в процессе выступления с докладом) путается в ответах, не может дать понятный и аргументированный ответ.

Оценка **«неудовлетворительно»** ставится за Эссе, в которых нет информации о проблематике работы и ее месте в контексте других работ по исследуемой теме.

Критерии устного ответа студента при опросе на экзамене

Оценка **«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.

Оценка **«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.

Оценка **«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.

Оценка **«неудовлетворительно»** выставляется студенту, в ответе которого обнаружились существенные пробелы в знании основного содержания учебной программы дисциплины и / или неумение использовать полученные знания.

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения и для контроля формирования компетенции

Контрольные вопросы для промежуточной аттестации (к экзамену)

Вопрос	Код компетенции
1. Необходимость обеспечения безопасности в информационных системах.	ПК-3
2. Прогресс информационных технологий и информационная безопасность.	ОПК-5
3. Классификация угроз безопасности информационных объектов.	ПК-3
4. Основные виды каналов утечки информации.	ПК-3
5. Естественные угрозы информационной безопасности.	ПК-3
6. Внешние угрозы информационной безопасности.	ПК-3
7. Мотивы и цели компьютерных преступлений.	ПК-3
8. Предупреждение компьютерных преступлений.	ОПК-5
9. Человеческие факторы, обусловливающие информационные угрозы.	ПК-3
10. Способы воздействия угроз на информационный объект.	ПК-3
11. Признаки воздействия вирусов на компьютерную систему. Системный подход к защите информации.	ОПК-5
12. Нормативно-правовая характеристика компьютерных преступлений.	ПК-3
13. Причины и условия, способствующие совершению компьютерных преступлений.	ПК-3
14. Меры предупреждения преступлений в сфере компьютерной информации.	ПК-3
15. История вредоносных программ. Защита учетной информации коммерческих фирм.	ОПК-5
16. Исторические аспекты компьютерных преступлений.	ПК-3
17. Экономическая информация как объект безопасности.	ПК-3
18. Виды тайн и как их сохранить.	ПК-3
19. Причины разглашения конфиденциальной информации.	ПК-3
20. Разглашение и утечка информации.	ПК-3
21. Теоретические аспекты информационной безопасности экономических систем.	ПК-3
22. Объекты информационной безопасности на предприятии.	ПК-3
23. Методы и средства обеспечения информационной безопасности.	ОПК-5
24. Физическая защита информационных систем.	ПК-3
25. Программно-технические методы обеспечения информационной безопасности.	ОПК-5
26. Идентификация и аутентификация.	ОПК-5
27. Государственное регулирование информационной безопасности в России.	ОПК-5
28. Защита от компьютерных вирусов.	ОПК-5
29. Электронная цифровая подпись и особенности ее применения.	ОПК-5

30. Защита информации в Интернете.	ОПК-5
31. Организация системы защиты информации экономических систем.	ОПК-5
32. Этапы построения системы защиты информации.	ОПК-5
33. Политика безопасности.	ОПК-5
34. Информационная безопасность электронной коммерции (ЭК).	ОПК-5
35. Сущность криптографических методов.	ОПК-5
36. Организационно-административные мероприятия обеспечения компьютерной безопасности.	ПК-3

Типовые тестовые задания
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

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

30. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

1. Анализ связующего дерева
2. AS/NZS
3. NIST
4. Анализ сбоев и дефектов

Примерная тематика эссе для проверки сформированности компетенций

Содержание этапа	Формируемые компетенции
Обзор литературы, обоснование актуальности темы, практической значимости	ПК-3
Аналитическая часть	ПК-3
Интерпретация полученных результатов	ОПК-5
Выводы	ОПК-5

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
7. Информационная безопасность **(**по материалам зарубежных источников и литературы).

8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
12. Составление инструкции по обработке и хранению конфиденциальных документов.
13. Направления и методы защиты документов на бумажных носителях.
14. Направления и методы защиты машиночитаемых документов.
15. Архивное хранение конфиденциальных документов.
16. Направления и методы защиты аудио- и визуальных документов.
17. Порядок подбора персонала для работы с конфиденциальной информацией. 18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
23. Порядок защиты информации в рекламной и выставочной деятельности.
24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
28. Назначение, виды, структура и технология функционирования системы защиты информации.
29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
30. Аналитическая работа по выявлению каналов утечки информации фирмы.
31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
32. Направления и методы защиты профессиональной тайны.
33. Направления и методы защиты служебной тайны.
34. Направления и методы защиты персональных данных о гражданах.
35. Методы защиты личной и семейной тайны.
36. Построение и функционирование защищенного документооборота.

Типовые задания/задачи

Типовые 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?

Типовые 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

1 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.);

2 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.

3 периодическая проверка исправности оборудования (в частности - поверхности жесткого диска) при помощи специальных программ.

Проанализируйте следующие ситуации

1. Связь основных понятий информационной безопасности

В издательство "Тезис" поступил звонок от провайдера. Предприятию отключили доступ к сети, потому что была зарегистрирована рассылка спама. Пришли большие счета, при сравнительно малом использовании ресурсов сети. В результате отключения Интернета были просрочены заказы, нарушена связь с несколькими клиентами, Оказалось, что менеджеры имеет несложный пароль, в основном даты рождения. У некоторых на мониторе приклеен стикер с паролем. Какие ошибки в информационном поведении сотрудников. Как действовать в данной ситуации. Как избежать подобных ситуаций позднее?

2. Основные уязвимости

Иногда изменяются содержательные данные, порой — служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) возбудила судебный иск против президента корпорации, обвиняя его в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее боссом президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что он (босс) в указанное время разговаривал по мобильному телефону, находясь за рулем автомобиля вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарь знала пароль своего босса, поскольку ей было поручено его регулярное изменение), и иск был отвергнут... Участники обсуждения делятся на защитников секретаря и защитников босса компании Oracle и доказывают правоту защищаемой стороны и возможность фальсификации доказательств противника.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711

2. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1094244.

3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

4. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467370

б) дополнительная литература:

1. Нетёсова, О. Ю. Информационные системы и технологии в экономике : учебное пособие для вузов / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 178 с. — (Высшее образование). — ISBN 978-5-534-08223-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/471403

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469758

4. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/476294

в) программное обеспечение и Интернет-ресурсы

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)

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: ноутбук, проектор, экран.

Компьютерный класс. Помещения для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

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

Программа дисциплины **«Информационная безопасность»** составлена в соответствии с образовательным стандартом высшего образования (ОС ННГУ) бакалавриат по направлению подготовки 38.03.01 Экономика (приказ ННГУ от 21.06.2021г. №349-ОД).

Автор(ы):
к.п.н., доцент Статуев А.А.

Рецензент (ы):
д.п.н., доцент Фролов И.В.

Программа одобрена на заседании кафедры экономики, управления и информатики от 17.11.2021 года, протокол № 9
зав. кафедрой
к.п.н., доцент Статуев А.А.

Председатель УМК факультета естественных и математических наук
к.э.н., доцент Люшина Э.Ю.

П.6. а) СОГЛАСОВАНО:

Заведующий библиотекой Федосеева Т.А.