Приложение 4

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Балахнинский филиал ННГУ

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Рабочая программа дисциплины

Информационная безопасность

Уровень высшего образования
Бакалавриат

Направление подготовки / специальность
09.03.03 - Прикладная информатика

Направленность образовательной программы
Прикладная информатика в управлении производством

Форма обучения
очная, очно-заочная

г. Балахна

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

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

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

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**	
	Индикатор достижения компетенции (код, содержание индикатора)	**Результаты обучения по дисциплине**	**Для текущего контроля успеваемости**	**Для промежуточной аттестации**
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*ОПК-3.1: Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности* *ОПК-3.2: Демонстрирует умение применять информационно-коммуникационные технологии решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности* *ОПК-3.3: Имеет практический опыт решения стандартных задач профессиональной деятельности с соблюдением требований информационной безопасности*	*ОПК-3.1:* *Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности* *Умеет решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности* *Владеет навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом*	*Тест*	*Экзамен: Контрольные вопросы*

		основных требований информационной безопасности *ОПК-3.2:* *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* *ОПК-3.3:* *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		
ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	*ОПК-4.1: Демонстрирует знание основных стандартов, норм и правил оформления технической документации на различных стадиях проектирования и поддержки жизненного цикла информационных систем* *ОПК-4.2: Применяет стандарты, нормы и правила (в том числе установленные самостоятельно) при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла информационных систем* *ОПК-4.3: Имеет практический опыт разработки технической документации на различных этапах проектирования и поддержки жизненного цикла информационной системы*	*ОПК-4.1:* *Знать основные законодательные акты в сфере информационной безопасности* *Уметь использовать в практической деятельности существующие правовые знания в сфере информационных систем и информационных технологий* *Владеть навыками использования инструментов информационной безопасности при разработке технической документации* *ОПК-4.2:* *Знать основные законодательные акты в сфере информационной безопасности* *Уметь использовать в практической деятельности существующие правовые знания в сфере информационных систем и информационных технологий* *Владеть навыками использования инструментов информационной безопасности при разработке технической документации* *ОПК-4.3:* *Знать основные законодательные акты в сфере информационной безопасности* *Уметь использовать в практической деятельности существующие правовые знания в сфере*	*Тест*	*Экзамен: Контрольные вопросы*

		информационных систем и информационных технологий *Владеть навыками использования инструментов информационной безопасности при разработке технической документации*		

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная	**очно-заочная**
Общая трудоемкость, з.е.	**4**	**4**
Часов по учебному плану	**144**	**144**
в том числе		
аудиторные занятия (контактная работа):		
- занятия лекционного типа	**16**	**12**
- занятия семинарского типа (практические занятия / лабораторные работы)	**48**	**16**
- КСР	**2**	**2**
самостоятельная работа	**42**	**78**
Промежуточная аттестация	**36** **Экзамен**	**36** **Экзамен**

3.2. Содержание дисциплины

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

Наименование разделов и тем дисциплины	Всего (часы)		в том числе							
			Контактная работа (работа во взаимодействии с преподавателем), часы из них						Самостоятельная работа обучающегося, часы	
			Занятия лекционного типа		Занятия семинарского типа (практические занятия/лабораторные работы), часы		Всего			
	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно
Тема 1. Теоретические аспекты информационной безопасности экономических систем	43	61	8	4	16	12	24	16	19	45
Тема2. Понятие информационных угроз и их виды	63	45	8	8	32	4	40	12	23	33
Аттестация	36	36								
КСР	2	2					2	2		
Итого	144	144	16	12	48	16	66	30	42	78

Содержание разделов и тем дисциплины

Тема 1. Теоретические аспекты информационной безопасности экономических систем
Тема 2. Понятие информационных угроз и их виды

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:

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

Иные учебно-методические материалы:

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 _ПК-3___

1.Защита информации от сбоев оборудования и случайной потери

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. Например: Disk Doctor, ScanDisk . Подобные

программы позволяют обнаружить дефектные участки на поверхности диска и соответствующим образом их пометить, чтобы при записи информации эти участки были обойдены.

4 периодическая оптимизация (дефрагментация) диска для рационального размещения файлов на нем, ускорения работы и уменьшения его износа.

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

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

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

Тесты для оценки компетенции «ОПК-3»

Вариант 1

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

Вопрос 6. Два принципиальных подхода к обеспечению компьютерной безопасности:

а. фрагментарный и комплексный

б. комплексный и системный

в. сегментный и фрагментарный

г. сегментный и системный

Вопрос 7. Сколько методов защиты данных выделяют?
а. 3
б. 6
в. 4
г. 5
Вопрос 8. Результатом этапа планирования является план
а. атаки
б. контроля в. внедрения г. защиты
Вопрос 9. В целях борьбы с компьютерной преступностью российским законодательством предусмотрена
а. уголовная ответственность
б. административная ответственность
в. материальная ответственность
г. все ответы неверны
Вопрос 10. Маскировка – это
а. метод защиты, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.
б. метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.
в. метод защиты в автоматизированной информационной системе предприятия путем ее криптографического закрытия.
г. метод защиты, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Вариант 2
Вопрос 1. Информационная безопасность – это…
а. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой
б. предотвращение зла наносимого государственным структурам
в. проведение природоохранных мероприятий.
г. Все ответы верны
Вопрос 2. К понятию информационной безопасности НЕ относятся:
а. природоохранные мероприятия
б. надежность работы компьютера в. сохранность ценных данных
Вопрос 3. Аппаратные средства защиты информации - это
а. организационно-технические и организационно-правовые мероприятия по регламентации поведения персонала.
б. правовые акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил.
в. нормы, традиции в обществе.
г. это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками.
Вопрос 4. Терапия предполагает
а. разбиение магнитного диска на ряд логических разделов, часть из которых имеет статус READ_ONLY, и в которых реализованы схемы парольного доступа.

б. проверку всех поступающих программ детекторами, а также проверка длин и контрольных сумм вновь поступающих программ на соответствие значениям, указанным в документации.
в. дезактивацию конкретного вируса в зараженных программах специальными программами (фагами).
г. использование специальных алгоритмов, позволяющих после запуска программы определить, были ли внесены изменения в ее файл.
Вопрос 5. ШИФРОВАНИЕ ДАННЫХ – процесс
а. процесс преобразования открытых данных в зашифрованные с помощью шифра.
б. процесс зашифрования и расшифрования данных.
в. процесс преобразования закрытых данных в открытые с помощью шифра.
г. процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме.

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

Вариант 1
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
Вопрос 6. Умышленные угрозы подразделяются на:
а. пассивные и активные
б. внутренние и внешние
в. все ответы верны
Вопрос 7. Бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы а. утечка конфиденциальной информации
б. разглашение конфиденциальной информации
в. несанкционированный доступ к защищаемой информации г. разглашение информации ее владельцем или обладателем Вопрос 8. Уничтожение компьютерной информации это

а. блокирование компьютерной информации
б. удаление с внешних носителей информации в. копирование компьютерной информации
г. модификация компьютерной информации
Вопрос 9. К видам компьютерных преступлений относят а. физические злоупотребления
б. операционные злоупотребления
в. программные злоупотребления
г. все ответы верны
Вопрос 10. Достоинством фрагментарного подхода является
а. высокая избирательность относительно конкретной угрозы
б. локальность действия
в. высокая чувствительность к ошибкам установки и настройки средств защиты г. сложность управления
д. узкое, несистемное понимание проблемы безопасности объекта

Вариант 2
Вопрос 1. К методам защиты данных – препятствие относится следующие средства защиты данных
а. физические
б. аппаратные
в. организационные
г. программные
д. законодательные
Вопрос 2. К методам защиты данных – маскировка относится следующее средство защиты данных
а. законодательные б. аппаратные
в. программные
г. организационные д. физические
Вопрос 3. К средству защиты информации – законодательные относится следующая группа методов защиты данных
а. регламентация б. управление
в. принуждение г. Побуждение
д. маскировка
Вопрос 4. Под комплексной защитой от компьютерных вирусов понимают реализацию направлений
а. защиты внешних каналов связи
б. защита серверов электронной почты
в. защита Web-серверов
г. защита файловых серверов и рабочих станций сотрудников
д. все ответы верны
Вопрос 5. Этапы построения системы защиты информации
а. сопровождение системы защиты, анализ, планирование системы защиты, реализация системы защиты.
б. анализ, планирование системы защиты, реализация системы защиты, сопровождение системы защиты.
в. реализация системы защиты, сопровождение системы защиты, планирование системы защиты, анализ.
г. планирование системы защиты, анализ, сопровождение системы защиты, реализация системы защиты.
Вопрос 6. Выявление рисков, на которые повлияет проект относится к
а. анализу выгод от реализации проекта
б. анализу затрат
в. дополнительным процедурам и расчетам
Вопрос 7. Определение ставки дисконтирования относится к
а. анализу выгод от реализации проекта
б. анализу затрат
в. дополнительным процедурам и расчетам
Вопрос 8. К сведениям составляющим коммерческую тайну не относится
а. производство

б. управление в. финансы
г. рынок
д. продукция
Вопрос 9. Источником конфиденциальной информации не является
а. цена
б. люди
в. документы
г. публикация
д. отходы

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
зачтено	
не зачтено	

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

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	**плохо**	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	не зачтено		**зачтено**				
Знания	Отсутствие знаний 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.
Умения	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые	Продемонстрированы все основные умения. Решены все основные задачи с отдельными несущественными	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов

			полном объеме	объеме, но некоторые с недочетами	с недочетами.	недочетами, выполнены все задания в полном объеме	
Навыки	Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценивания при промежуточной аттестации

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

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

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

- 1. Функции материально-технического снабжения в организации производства.
- 2. Материально технические ресурсы предприятия.

- 3. Обоснование необходимости образования запасов.
- 4. Структура и классификация производственных запасов.
- 5. Значение и функции запасов и их влияние на затраты предприятия.
- 6. Управление процессом распределения продукции.
- 7. Основные задачи службы сбыта.
- 8. Маркетинговые исследования рынка сбыта.
- 9. Опыт сбытовой логистики разных стран.
- 10. Факторы, влияющие на стимулирование сбыта.
- 11. Разработка и обоснование сбытовой политики.
- 12. Затраты по сбытовой деятельности.
- 13. Сбытовая политика транспортного предприятия.
- 14. Затраты по сбыту продукции предприятия водного транспорта.
- 15. Виды сбытовой организации предприятия
- 16. Концепция международного управления сбытом
- 17. Типы снабженческо-сбытовых систем
- 18. Классификация цен
- 19. Стратегическое планирование снабжения и сбыта
- 20. Стратегия международного ценообразования
- 21. Контроллинг в системе управления снабжением и сбытом
- 22. Организационная структура службы снабжения и сбыта с ориентацией по регионам, рынкам, покупателям, их достоинства и недостатки
- 23. Выбор стратегии целевых сегментов рынка
- 24. Конкурентные стратегии в системе снабжения
- 25. Специфика международной снабженческо-сбытовой
- 26. Развитие снабженческо-сбытовой структуры на предприятиях России

- 27. Базисные концепции сбытовой стратегии
- 28. Стратегическое планирование снабженческо-сбытовой системы
- 29. Характеристика разделов плана снабжения и сбыта
- 30. Стратегия снабженческо-сбытовой системы коммуникаций

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

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.

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.

32. История вредоносных программ.

33. Защита учетной информации коммерческих фирм.

34. Свойства экономической информации, нарушаемые при несанкционированном доступе.

35. Исторические аспекты компьютерных преступлений.

36. Экономическая информация как объект безопасности.

37. Перечень сведений, которые не могут составлять коммерческую тайну.

38. Виды тайн и как их сохранить.

39. Причины разглашения конфиденциальной информации.

40. Разглашение и утечка информации.

41. Стратегия злоумышленника при несанкционированном доступе.

42. Организация конфиденциального делопроизводства.

43. Структура службы безопасности компании.

44. Теоретические аспекты информационной безопасности экономических систем.

45. Основные понятия информационной безопасности экономических систем.

46. Экономическая информация как товар и объект безопасности.

47. Понятия информационных угроз и их виды.

48. Вредоносные программы.

49. Компьютерные преступления и наказания.

50. Принципы построения системы информационной безопасности.

51. Подходы, принципы, методы и средства обеспечения безопасности.

52. Организационно-техническое обеспечение компьютерной безопасности.

53. Электронная цифровая подпись и особенности ее применения.

54. Защита информации в Интернете.

55. Организация системы защиты информации экономических систем.

56. Этапы построения системы защиты информации.

57. Политика безопасности.

58. Оценка эффективности инвестиций в информационную безопасность.

59. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).

60. Информационная безопасность электронной коммерции (ЭК).

61. Обеспечение компьютерной безопасности учетной информации.

62. Сущность криптографических методов.

63. Организационно-административные мероприятия обеспечения компьютерной безопасности.

64. Организация конфиденциального делопроизводства.

65. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечен

66. Типы и субъекты информационных угроз.

Критерии оценивания (оценочное средство - Контрольные вопросы)

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

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

Основная литература:

1. Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев ; ННГУ им. Н. И. Лобачевского. - Нижний Новгород : Изд-во ННГУ, 2017. - 198 с. - Текст : электронный., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=823079&idb=0.
2. Баранова Елена Константиновна. Информационная безопасность и защита информации : Учебное пособие / Национальный исследовательский университет "Высшая школа экономики". - 4. - Москва : Издательский Центр РИОР, 2022. - 336 с. - ВО - Бакалавриат. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=832410&idb=0.

Дополнительная литература:

1. Баранова Елена Константиновна. Информационная безопасность и защита информации :

Учебное пособие / Национальный исследовательский университет "Высшая школа экономики". - 4. - Москва : Издательский Центр РИОР, 2022. - 336 с. - ВО - Бакалавриат. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=832410&idb=0.

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

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

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

7. Материально-техническое обеспечение дисциплины (модуля)

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

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

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

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

Заведующий кафедрой: Трифонов Юрий Васильевич, доктор экономических наук.

Программа одобрена на заседании методической комиссии от 12.01.24, протокол № 5.