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 ученого совета ННГУ
(протокол от 24.11.2021 г. № 14)

Рабочая программа дисциплины

Современные методы обеспечения информационной безопасности в информационных системах

(наименование дисциплины)

Уровень высшего образования
магистратура
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
09.04.03 Прикладная информатика
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Разработка и управление проектами в области информационных технологий
(указывается профиль / магистерская программа / специализация)

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

Арзамас
2021 год

1. Место дисциплины (модуля) в структуре ООП

Дисциплина Б1.В.01 «Современные методы обеспечения информационной безопасности в информационных системах» относится к части, формируемой участниками образовательных отношений образовательной программы направления подготовки 09.04.03 Прикладная информатика, направленность (профиль) Разработка и управление проектами в области информационных технологий.

Дисциплина предназначена для освоения студентами очной/очно-заочной/заочной формы обучения в 3 семестре/2 семестре/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-5. Способен планировать и организовывать аналитическую деятельность на всех этапах жизненного цикла ИС (ИИС).	ИПК-5.1. Способен использовать знания об основных этапах жизненного цикла ИС (ИИС).	*Знать* об основных этапах жизненного цикла ИС (ИИС) в предметной области, в рамках коммуникативной деятельности. *Уметь* использовать знания об основных этапах жизненного цикла ИС (ИИС). *Владеть* навыками использования знаний об основных этапах жизненного цикла ИС (ИИС).	*Тест*
	ИПК-5.2. Способен планировать и организовывать аналитическую деятельность на всех этапах жизненного цикла ИС (ИИС).	*Знать* основы планирования и организации аналитической деятельности на всех этапах жизненного цикла ИС (ИИС) *Уметь* планировать и организовывать аналитическую деятельность на всех этапах жизненного цикла ИС (ИИС) с учетом области коммуникации и взаимодействия с клиентами *Владеть* способностью продемонстрировать практический опыт планирования и организации аналитической деятельности в сфере коммуникации.	*Учебно-исследовательские реферативные работы*
	ИПК-5.3. Способен продемонстрировать практический опыт планирования и организации аналитической деятельности.	*Знать* основы практического опыта планирования и организации аналитической деятельности *Уметь* использовать практический опыт планирования и организации аналитической деятельности *Владеть* навыками использования практического опыта планирования и организации аналитической деятельности	*Контрольные задания по теоретическим основам дисциплины, практические контрольные задания*
ПК-9. Способен руководить проектами по созданию и модерниза-	ИПК-9.1. Способен использовать базовые принципы концепции системы, основанной на знаниях, и нейросетевой пара-	*Знать* требования к системе в целом и к методам обеспечения ее информационной безопасности, к функциям системы, видам обеспечения ин-	*Тест*

ции гибридных ИИС, базирующихся на концепции системы, основанной на знаниях, и современных нейросетевых технологиях принятия решений.	дигмы принятия решений при планировании проектов гибридных ИИС..	формационной безопасности, порядок контроля и приемки системы, значения технических, технологических, производственно-экономических или других показателей объекта автоматизации, которые должны быть достигнуты в результате создания ИС; критерии оценки достижения целей создания системы. *Уметь* формулировать состав и содержание работ, в том числе, и по обеспечению информационной безопасности обозначить назначение и цели разработки информационной системы, вырабатывать требования к системе в целом, к методам обеспечения ее информационной безопасности, к функциям системы, видам обеспечения ее информационной безопасности, определять порядок контроля и приемки системы *Владеть* навыками определения состава и содержания работ, обозначения назначения и цели разработки информационной системы, выработки требований к системе в целом, к методам обеспечения ее информационной безопасности, к функциям системы, видам обеспечения ее информационной безопасности, определения порядок контроля и приемки системы	
	ИПК-9.2. Способен организовать командный подход к созданию и модернизации гибридных ИИС.	*Знать* основы командного подхода к созданию и модернизации гибридных ИИС. *Уметь* организовать командный подход к созданию и модернизации гибридных ИИС. *Владеть* навыками по организации командного подхода к созданию и модернизации гибридных ИИС.	*Учебно-исследовательские реферативные работы*
	ИПК-9.3. Способен руководить конкретными проектами по созданию и модернизации гибридных ИИС	*Знать* основы руководства конкретными проектами по созданию и модернизации гибридных ИИС. *Уметь* руководить конкретными проектами по созданию и модернизации гибридных ИИС. *Владеть* навыками руководства конкретными проектами по созданию и модернизации гибридных ИИС.	*Контрольные задания по теоретическим основам дисциплины, практические контрольные задания*

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Трудоемкость	**очная форма обучения**	**заочная форма обучения**	**заочная форма обучения**
Общая трудоемкость	4 з.е.	4 з.е	4 з.е
часов по учебному плану, из них	144	144	144
Контактная работа, в том числе: аудиторные занятия:			

– занятия лекционного типа	16	8	6
– занятия семинарского типа	32	16	6
контроль самостоятельной работы	2	2	2
Промежуточная аттестация экзамен	36	45	9
Самостоятельная работа	58	73	121

3.2. Содержание дисциплины

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

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
1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей	**6**	**13**	**7**	2	2	2				4	2								6	9	15
2. Виды противников или «нарушителей». Понятие о видах вирусов	**6**	**13**	**7**	2	2	2				4	2	2							6	9	15
3. Три вида возможных нарушений информационной системы. Защита.	**6**	**13**	**7**	2	2					4	2								6	9	15
4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	**6**	**13**	**7**	2	2	2				4	2	2							8	9	15
5. Криптографические методы защиты информации. Использование защищенных компьютерных систем	**6**	**11**	**5**	2						4	2	2							8	9	15
6. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности	**6**	**11**	**5**	2						4	2								8	9	15
7. Анализ способов наруше-	**6**	**11**	**5**	2						4	2								8	9	15

ний информационной безопасности																					
8. Место информационной безопасности экономических систем в национальной безопасности страны	**6**	**12**	**6**	2						4	2								8	10	16
В том числе текущий контроль	**2**	**2**	**2**										**2**	**2**	**2**						
Экзамен	**36**	**45**	**9**													**36**	**45**	**9**			
ИТОГО	**144**	**144**	**144**	**16**	**8**	**6**				**32**	**16**	**6**	**2**	**2**	**2**	**36**	**45**	**9**	**58**	**73**	**121**

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

4. Учебно-методические обеспечение самостоятельной работы студентов

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

Для обеспечения самостоятельной работы обучающихся используется электронный курс Современные методы обеспечения информационной безопасности в информационных системах, https://e-learning.unn.ru/course/view.php?id=8009, созданный в системе электронного обучения ННГУ - https://e-learning.unn.ru/.

Самостоятельная работа студентов по дисциплине «Современные методы обеспечения информационной безопасности в информационных системах» осуществляется в следующих видах: работа с основной и дополнительной литературой, учебно-исследовательские реферативные работы, самостоятельное изучение отдельных тем (вопросов), в соответствии со структурой дисциплины по учебной и специальной литературе, решение упражнений (стандартных задач) по образцу и инвариантных (нестандартных) упражнений (задач).

Рекомендации для работы с основной и дополнительной литературой

Работа с литературой должна сопровождаться записями в форме конспекта, плана, тезисов. При этом важно не только привлечь более широкий круг литературы, но и суметь на ее основе разобраться в степени изученности темы. Стоит выявить дискуссионные вопросы, нерешенные проблемы, попытаться высказать свое отношение к ним. Привести и аргументировать свою точку зрения или отметить, какой из имеющихся в литературе точек зрения по данной проблематике придерживаетесь и почему.

По завершении изучения рекомендуемой литературы полезно проверить уровень своих знаний с помощью контрольных вопросов для самопроверки. Необходимо вести систематическую работу над литературными источниками. Необходимо изучать не только литературу, рекомендуемую в данных учебно-методических материалах, но и новые, важные издания по курсу, вышедшие в свет после публикации. При этом следует выделять неясные, сложные для восприятия вопросы. В целях прояснения последних нужно обращаться к преподавателю.

Рекомендации для написания учебно-исследовательской реферативной работы

Учебно-исследовательская реферативная работа – изложение в письменном виде содержания научного труда (трудов), литературы по теме. Цель написания учебно-исследовательской реферативной работы – овладение навыками анализа и краткого изложения изученных материалов в соответствии с требованиями, предъявляемыми к таковым работам. Это самостоятельная работа студента, где раскрывается суть исследуемой проблемы, приводятся различные точки зрения, собственные взгляды на нее. Содержание работы должно быть логическим, изложение материала носит проблемно-тематический характер.

Примерный алгоритм действий при написании реферата:

1. Подберите и изучите основные источники по теме (как правило, при разработке реферата или доклада используется не менее 8-15 различных источников).
2. Составьте библиографию.
3. Разработайте план реферата или доклада исходя из имеющейся информации.
4. Обработайте и систематизируйте подобранную информацию по теме.
5. Отредактируйте текст реферата или доклад с использованием компьютерных технологий.
6. Подготовьте публичное выступление по материалам реферата или доклада, желательно подготовить презентацию, иллюстрирующую основные положения работы.

Критерии результатов работы для самопроверки:

- актуальность темы исследования;
- соответствие содержания теме;
- глубина проработки материала;
- правильность и полнота использования источников;
- соответствие оформления реферата или доклада предъявляемым требованиям.

Самостоятельное изучение отдельных тем (вопросов)
в соответствии со структурой дисциплины
по учебной и специальной литературе

Активизация учебной деятельности и индивидуализация обучения предполагает вынесение для самостоятельного изучения отдельных тем или вопросов. Выбор тем (вопросов) для самостоятельного изучения – одна из ключевых проблем педагога в организации эффективной работы обучающихся по овладению учебным материалом.

Особую роль самостоятельное изучение отдельных тем (вопросов) дисциплины играет для студентов заочной формы обучения.

При этом, как правило, основанием выбора является наилучшая обеспеченность литературой и учебно-методическими материалами по данной теме, ее обобщающий характер, сформированный на аудиторных занятиях алгоритм изучения. Обязательным условием результативности самостоятельного освоения темы (вопроса) является контроль выполнения задания.

Вопросы для самостоятельного изучения тем (вопросов) указаны в рабочей программе дисциплины (модуля)».

Результаты самостоятельного изучения вопросов, будут проверены преподавателем в форме: опросов, конспектов, рефератов, ответов на экзаменах.

Самостоятельное выполнение расчетных заданий

1. Внимательно прочитайте теоретический материал – конспект, составленный на лекционном занятии, материал учебника, пособия. Выпишите формулы из конспекта по изучаемой теме.
2. Обратите внимание, как использовались данные формулы при решении задач на занятии.
3. Решите предложенную задачу, используя выписанныеформулы.
4. В случае необходимости воспользуйтесь справочными данными.
5. Проанализируйте полученный результат (проверьте размерности величин, правильность подстановки в формулы численных значений, правильность расчетов, правильность вывода неизвестной величины из формулы).
6. Решение задач должно сопровождаться необходимыми пояснениями. Расчётные формулы 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;
- точность и правильность расчетов;
- обоснование решения задачи.

Методические рекомендации
по подготовке к зачету

Зачет проводится в традиционной форме (ответ на вопросы, тестирование).

Подготовка к зачету начинается с первого занятия по дисциплине. При этом важно с самого начала планомерно осваивать материал, руководствуясь требованиями, конспектировать важные для решения учебных задач источники, обращаться к преподавателю за консультацией по неусвоенным вопросам.

Для подготовки к сдаче зачета необходимо первоначально прочитать лекционный материал, а также соответствующие разделы рекомендуемых изданий. Лучшим вариантом является тот, при котором при подготовке используется несколько источников информации. Это способствует разностороннему восприятию каждой конкретной темы дисциплины.

В обобщённом варианте подготовка к сдаче зачета включает в себя:

• просмотр программы учебной дисциплины, перечня вопросов к зачету;

• подбор рекомендованных преподавателем источников (учебников, нормативных правовых актов, дополнительной литературы и т.д.),

• использование конспектов лекций, материалов занятий и их изучение;

• консультирование у преподавателя.

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
	Удовлетворительно	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	Неудовлетворительно	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 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 учебно-исследовательских реферативных работ

Оценка «отлично» – реферативная работа полностью раскрывает основные вопросы теоретического материала. Студент приводит информацию из первоисточников и изданий периодической печати, приводит практические примеры, в докладе отвечает на дополнительные вопросы преподавателя и студентов.

Оценка «хорошо» – реферативная работа частично раскрывает основные вопросы теоретического материала. Студент приводит информацию из первоисточников, отвечает на дополнительные вопросы преподавателя и студентов (при докладе), но при этом дает не четкие ответы, без достаточно их аргументации.

Оценка «удовлетворительно» – реферативная работа в общих чертах раскрывает основные вопросы теоретического материала. Студент приводит информацию только из учебников. При ответах на дополнительные вопросы в докладе путается в ответах, не может дать понятный и аргументированный ответ.

Критерии оценки выполнения контрольных заданий по теоретическим основам дисциплины

Оценка **«отлично»** - Ответ полный и правильный на основании изученной теории; материал изложен в необходимой логической последовательности, грамотный научный язык; ответ самостоятельный.

Оценка **«хорошо»** - Ответ полный и правильный на основании изученной теории; материал изложен в необходимой логической последовательности при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

Оценка **«удовлетворительно»** - Ответ полный, но при этом допущена существенная ошибка или неполный, несвязный ответ.

Оценка **«неудовлетворительно»** - Ответ обнаруживает непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые не могут быть исправлены при наводящих вопросах преподавателя.

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

Примерные контрольные задания по теоретическим основам дисциплины для оценки сформированности компетенции ПК 5

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.
13. Какие основные законы в области защиты информации в РФ?
14. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
15. Что такое концепция информационной безопасности?
16. Что такое конфиденциальная информация?
17. Что такое персональные данные?
18. В каких случаях возможно использовать персональные данные без согласия обладателя?
19. Охарактеризуйте биометрические данные как персональные данные.
20. Что такое профессиональная тайна?
21. Что такое коммерческая тайна?
22. Что такое режим коммерческой тайны?
23. Что такое государственная тайна?
24. Опишите правовой режим государственной тайны.
25. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
26. Какие основные международные стандарты в области информационной безопасности существуют?
27. Что такое "Единые критерии"
28. Как связаны международные стандарты и стандарты РФ?
29. Какие основные стандарты РФ в области информационной безопасности существуют?
30. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.

для оценки сформированности компетенции ПК 9

31. Что такое политика безопасности?
32. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?
33. Что такое инженерная защита объектов?
34. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?
35. Что такое технические каналы утечки информации?
36. Перечислите основные виды технических каналов утечки ин-формации?
37. Перечислите методы защиты информации от утечки по визуальному каналу.
38. Перечислите методы защиты информации от утечки по воздушному каналу.
39. Перечислите методы защиты информации от утечки по вибрационному каналу.
40. Перечислите методы защиты информации от утечки по индукционному каналу.
41. Перечислите средства и методы защиты информации от утечки в телефонных линиях.

42. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.
43. Какие виды компьютерных угроз существуют?
44. Что такое брандмауэр?
45. Что такое антивирусная программа?
46. Что такое эвристический алгоритм поиска вирусов?
47. Что такое сигнатурный поиск вирусов?
48. Методы противодействия сниффингу?
49. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
50. Что такое механизм контроля и разграничения доступа?
51. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
52. Что такое средства стеганографической защиты информации?
53. Что такое криптография?
54. Какие используются симметричные алгоритмы шифрования?
55. Какие используются ассиметричные алгоритмы шифрования?
56. Что такое криптографическая хеш-функция?
57. Какие используются криптографические хеш-функции?
58. Что такое цифровая подпись?
59. Что такое инфраструктура открытых ключей?
60. Какие российские и международные стандарты на формирование цифровой подписи существуют?
61. Какие основные криптографические протоколы используются в сетях?

Темы учебно-исследовательских реферативных работ
для оценки сформированности компетенции ПК 5

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы

для оценки сформированности компетенции ПК 9

6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ

Типовые тестовые задания
для оценки сформированности компетенции ПК 5

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется
   a) Компилятор
   b) Интернет-черви
   c) Вирус
2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется
   a) Воздействием (влиянием)
   b) Потерей

c) Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется

   a) Троянской программой

   b) Червем

   c) Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата, называется

   a) Устойчивостью

   b) Терпимостью по отношению к риску

   c) Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд

   a) Две

   b) Одну

   c) Сколько зададут

для оценки сформированности компетенции ПК 9

6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:

   a) Статическими алгоритмами

   b) Алгоритмы RMS

   c) Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:

   a) Каталоги
   b) Символьные файлы
   c) Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются

   a) Вирусами
   b) Руткитами
   c) Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:

   a) Правилами безопасности
   b) Требованием безопасности
   c) Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

    a) Управление риском
    b) Предупреждением рисков
    c) Анализом рисков

11. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется

    a) Мультипроцессоры типа «хозяин-подчиненный»
    b) Симметричный мультипроцессор
    c) Мультипроцессор с общей памятью

Контрольные вопросы для промежуточной аттестации (к экзамену)

Вопрос	Код формируемой компетенции
1. Международные стандарты информационного обмена. Понятие угрозы.	ПК-5
2. Информационная безопасность в условиях функционирования в России глобальных сетей. Стандарты в области информационной безопасности.	ПК-5
3. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность.	ПК-9
4. Виды противников или «нарушителей». Понятие о видах вирусов. Понятие нарушителя информационной безопасности.	ПК-9
5. Хакеры. Виды хакеров. Примеры хакерских атак.	ПК-5
6. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	ПК-5
7. Три вида возможных нарушений информационной безопасности. Три составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз.	ПК-9
8. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	ПК-9
9. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны	ПК-5
10. Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности.	ПК-5
11. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.	ПК-9
12. Криптографические методы защиты информации. Симметричные и ассиметричные системы шифрования.	ПК-9
13. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.	ПК-5
14. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности.	ПК-5
15. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.	ПК-9
16. .Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.	ПК-9
17. Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике	ПК-5
18. Криптография. Криптоанализ. Основные понятия криптологии.	ПК-5
19. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера.	ПК-9
20. Программы для криптографии. Электронная цифровая подпись.	ПК-9
21. Основные технологии построения защищенных систем. Физические устройства. Их виды и использование.	ПК-5
22. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы.	ПК-5
23. Правовые особенности использования средств информационной защиты.	ПК-9
24. Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией.	ПК-9

25. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов.	ПК-5
26. Концепция информационной безопасности. Основные сведения и положения.	ПК-5

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433715
2. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/444046
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/432966
4. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/441287

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, 2019. — 178 с. — (Университеты России). — ISBN 978-5-534-08223-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437377
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437163
3. Информационное право : учебник для бакалавриата, специалитета и магистратуры / М. А. Федотов [и др.] ; под редакцией М. А. Федотова. — Москва : Издательство Юрайт, 2019. — 497 с. — (Бакалавр. Специалист. Магистр). — ISBN 978-5-534-10593-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/430915
4. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2019. — 220 с. — (Университеты России). — ISBN 978-5-9916-9244-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437667
5. Крупский, В. Н. Теория алгоритмов. Введение в сложность вычислений : учебное пособие для бакалавриата и магистратуры / В. Н. Крупский. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 117 с. — (Авторский учебник). — ISBN 978-5-534-04817-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/444131

в) программное обеспечение и Интернет-ресурсы:

Лицензионное программное обеспечение: Операционная система Windows.

Лицензионное программное обеспечение: Microsoft Office.

Профессиональные базы данных и информационные справочные системы

Российский индекс научного цитирования (РИНЦ), платформа Elibrary: национальная информационно-аналитическая система. Адрес доступа: http://elibrary.ru/project_risc.asp

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

Scopus: реферативно-библиографическая база научных публикаций и цитирования. Адрес доступа: http://www.scopus.com

Свободно распространяемое программное обеспечение:

программное обеспечение LibreOffice;
программное обеспечение Yandex Browser;
программное обеспечение Paint.NET;

программное обеспечение 1С:

* "Бухгалтерия предприятия", редакция 3.0, см. http://v8.1c.ru/buhv8/ ,
* "Управление торговлей", редакция 11.1, см. http://v8.1c.ru/trade/ ,
* "Зарплата и управление персоналом", редакция 3.0, см. http://v8.1c.ru/hrm/ ,
* "Управление небольшой фирмой", редакция 1.5, см. http://v8.1c.ru/small.biz/ ,
* "ERP Управление предприятием 2.0", см. http://v8.1c.ru/erp/ .
* "Бухгалтерия государственного учреждения", редакция 1.0, см. http://v8.1c.ru/stateacc/ ,
* "Зарплата и кадры государственного учреждения", редакция 1.0, http://v8.1c.ru/statehrm/ .

программное обеспечение PascalABC.NET

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

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

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 **Современные методы обеспечения информационной безопасности в информационных системах** составлена в соответствии с ОС ННГУ по направлению подготовки 09.04.03 Прикладная информатика (уровень магистратуры) (приказ ННГУ от 21.06.2021 № 348-ОД).

Автор(ы):
к.п.н., доцент Статуев А.А.

Рецензент (ы):
д.т.н., профессор Ямпурин Н.П.

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

Председатель МК факультета естественных и математических наук
к.п.н., доцент Володин А.М.

П.6. а) СОГЛАСОВАНО:

Заведующий библиотекой Федосеева Т.А.