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 № 6 от 31.05.2023 г.

Рабочая программа дисциплины

Информационная безопасность

(наименование дисциплины)

Уровень высшего образования
бакалавриат
(бакалавриат / магистратура / специалитет)

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

Направленность образовательной программы
Системное и прикладное программирование
(указывается профиль / магистерская программа / специализация)

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

Год начала подготовки 2022
Арзамас
2023 год

1. Место дисциплины (модуля) в структуре ООП

Дисциплина Б1.О.22 «Информационная безопасность» относится к обязательной части, образовательной программы направления 09.03.03 Прикладная информатика, направленность (профиль) Системное и прикладное программирование.

Дисциплина предназначена для освоения студентами очной/очно-заочной/заочной формы обучения в 3 семестре/3 семестре/6 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) ****	
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.	*Знать* принципы, методы и средства решения стандартных задач профессиональной деятельности *Уметь* выбрать принципы, методы и средства решения стандартных задач профессиональной деятельности *Владеть* навыками применения методов и средств решения стандартных задач профессиональной деятельности	*Тест*
	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.	*Знать* принципы решения стандартных задач профессиональной деятельности *Уметь* выбрать способы решения задач профессиональной деятельности *Владеть* навыками выбора способа решения задач профессиональной деятельности	*Учебно-исследовательские реферативные работы*
	ОПК-3.3. Имеет практический опыт решения стандартных задач профессиональной деятельности с соблюдением требований информационной безопасности.	*Знать* особенности подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности *Уметь* подготовить обзоры, аннотации, рефераты, научные публикации, и библиографию по научно-исследовательской работе с учетом требований информационной безопасности *Владеть* навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информаци-	*Контрольные задания по теоретическим основам дисциплины*

		онной 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.	*Знать* принципы выбора основной нормативно-справочной документации при разработке ИС *Уметь* выбирать основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы *Владеть* навыками применения нормативно-справочной документации при разработке ИС	*Тест*
	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.	*Знать* инструменты выбора стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы *Уметь* выбирать стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы *Владеть* навыками использования стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы	*Учебно-исследовательские реферативные работы*
	ОПК-4.3. Имеет практический опыт разработки технической документации на различных этапах проектирования и поддержки жизненного цикла информационной системы.	*Знать* принципы составления технической документации на различных этапах жизненного цикла информационной системы *Уметь* использовать ПО для составления технической документации на различных этапах жизненного цикла информационной системы *Владеть* навыками составления технической документации на различных этапах жизненного цикла информационной системы	*Контрольные задания по теоретическим основам дисциплины*

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Трудоемкость	**очная форма обучения**	**очно-заочная форма обучения**	**заочная форма обучения**
Общая трудоемкость	3 з.е.	3 з.е	3 з.е
часов по учебному плану, из них	108	108	108
Контактная работа, в том числе: аудиторные занятия:			
– занятия лекционного типа	16	8	
– занятия семинарского типа	34	16	2
контроль самостоятельной работы	1	1	1
Промежуточная аттестация зачет			4
Самостоятельная работа	57	83	101

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
Тема 1. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.	**14**	**15**	**14**	2	2		4	2											8	11	14
Тема 2. Терминологические основы информационной безопасности. Основные понятия и определения.	**14**	**16**	**14**	2	2		4	2											8	12	14
Тема 3. Общие методологические принципы теория информационной безопасности. Комплексность.	**16**	**16**	**16**	2	2		6	2	1										8	12	15
Тема 4. Угрозы. Классификация и анализ угроз информационной безопасности.	**14**	**16**	**14**	2	2		4	2											8	12	14
Тема 5. Методы нарушения конфиденциальности, целостности и доступности информации.	**16**	**16**	**16**	2			6	4	1										8	12	15
Тема 6. Причины, виды, каналы утечки и искажения информации.	**15**	**14**	**15**	2			4	2											9	12	15
Тема 7. Функции и задачи защиты информации. Проблемы региональной информационной безопасности.	**18**	**14**	**14**	4			6	2											8	12	14
В том числе текущий контроль	**1**	**1**	**1**										**1**	**1**	**1**						
Зачет			**4**															**4**			
ИТОГО	**108**	**108**	**108**	**16**	**8**		**34**	**16**	**2**				**1**	**1**	**1**			**4**	**57**	**83**	**101**

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

4. Учебно-методическое обеспечение самостоятельной работы студентов

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

Для обеспечения самостоятельной работы обучающихся используется электронный управляемый курс «Информационная безопасность» https://e-

learning.unn.ru/course/view.php?id=2274, созданный в системе электронного обучения ННГУ https://e-learning.unn.ru/.

Самостоятельная работа студентов по дисциплине «Информационная безопасность» осуществляется в следующих видах: работа с основной и дополнительной литературой, выполнение заданий различных типов, составления тезисов литературных источников, подготовки рефератов, разработка проектных работ, подготовка презентаций.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.3.

Методические рекомендации к самостоятельной работе

Методические рекомендации по подготовке к занятиям семинарского типа

Подготовка к занятиям семинарского типа (практическим занятиям) – традиционная форма самостоятельной работы обучающихся, включает отработку лекционного материала, изучение рекомендованной литературы, конспектирование предложенных источников.

Подготовка к опросу, проводимому в рамках практического занятия, требует уяснения вопросов, вынесенных на конкретное занятие, подготовки выступлений, повторения основных терминов, запоминания формул и алгоритмов.

На практических занятиях рассматриваются наиболее важные, существенные, сложные вопросы, которые, как свидетельствует преподавательская практика, наиболее трудно усваиваются студентами. Готовиться к практическим занятиям необходимо заблаговременно.

Подготовка к семинарским (практическим) занятиям включает в себя:

- обязательное ознакомление с планом практического занятия, в котором содержатся основные вопросы, выносимые на обсуждение;
- изучение конспектов лекций, соответствующих разделов учебника, учебного пособия, содержания рекомендованных нормативных правовых актов;
- изучение дополнительной литературы по теме практического занятия с обязательным конспектированием материала, который понадобится при обсуждении на семинаре.

Помните, что необходимо:

- выписать основные термины и запомнить их дефиниции;
- записывать возникшие во время самостоятельной работы с учебниками и научной литературы вопросы, чтобы затем на семинаре получить на них ответы;
- иметь продуманные и аргументировано обоснованные формулировки собственной позиции по каждому вопросу плана практического занятия;
- обращаться за консультацией к преподавателю при возникновении затруднений в освоении материала практической работы.

Выступление на практических занятиях должно удовлетворять следующим требованиям: в выступлении излагаются теоретические подходы к рассматриваемому вопросу, дается анализ принципов, законов, понятий и категорий; теоретические положения подкрепляются фактами, примерами, выступление должно быть аргументированным. Для более углубленного изучения вопросов рекомендуется конспектирование основной и дополнительной литературы.

Большую помощь при подготовке к занятиям может оказать изучение публикаций в научных журналах, а также специальные Интернет-ресурсы по тематике дисциплины, указанные п. 6 настоящей рабочей программы дисциплины

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, Тест).

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, экзамену;

• 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	Минимально допустимый	Уровень знаний в объеме,	Уровень знаний в объ-

	минимальных требований. Имели место грубые ошибки.	уровень знаний. Допущено много негрубых ошибок.	соответствующем программе подготовки. Допущено несколько негрубых ошибок.	еме, 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 оценки выполнения практических контрольных заданий

Оценка **«зачтено»** - Ответ полный и правильный на основании изученной теории; теоретический материал и решение поставленных задач изложены в необходимой логической последовательности, грамотный научный язык; ответ самостоятельный. Могут быть допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

Оценка **«не зачтено» -** 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 зачёте

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 ОПК 3

1. Теория защиты информации. Основные направления.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная)
4. Требования к системе защиты информации.
5. Угрозы информации.
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления у грог
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.
14. Общая модель процесса нарушения физической целостности информации.
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
16. Методологические подходы к оценке уязвимости информации.
17. Модель защиты системы с полным перекрытием.
18. Рекомендации по использованию моделей оценки уязвимости информации.
19. Допущения в моделях оценки уязвимости информации.
20. Методы определения требований к защите информации.

21. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.

22. Классификация требований к средствам защиты информации.

для оценки сформированности компетенции ОПК 4

23. Требования к защите, определяемые структурой автоматизированной системы обработки данных.

24. Требования к защите, обусловливаемые видом защищаемой информации.

25. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.

26. Анализ существующих методик определения требований к защите информации

27. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах Министерства обороны США». Основные положения.

28. О Руководящем документе Гостехкомиссни России «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Ч. I.

29. Классы защищенности средств вычислительной техники от несанкционированного доступа.

30. Факторы, влияющие на требуемый уровень защиты информации.

31. Функции и задачи защиты информации. Основные положения механизмов непосредственной зашиты и механизмы управления механизмами непосредственной защиты.

32. Методы формирования функций защиты.

33. События, возникающие при формировании функций защиты,

34. Классы задач функций защиты.

35. Класс задач функций защиты 1 - уменьшение степени распознавания объектов.

36. Класс задач функций защиты 2 - защита содержания обрабатываемой, хранимой и передаваемой информации.

37. Класс задач функций защиты 3 - защита информации от информационного воздействия

38. Функции защиты информации.

39. Стратегии защиты информации.

40. Способы и средства защиты информации.

41. Способы «абсолютной системы защиты*'

42. Архитектура систем защиты информации. Требования.

43. Общеметодологические принципы архитектуры системы защиты информации.

44. Построение средств защиты информации

45. Ядро системы защиты информации

46. Семирубежная модель

Типовые практические контрольные задания по дисциплине
для оценки сформированности компетенций ОПК 3

Задание № 1. «Безопасность информационных систем»

Вопросы:

1. Что вы представляете под безопасностью информационный системы.
2. Что относиться к основным характеристикам защищаемой информации?
3. Что вы отнесете к информации ограниченного доступа?
4. По каким направлениям будет осуществляться дальнейшее развитие системы безопасности?

Задание:

Определите в каких формах представлена информация на вашей домашней ЭВМ. Опишите, как обеспечивается информационная безопасность вашей ПЭВМ и отвечает ли современным требованиям развития систем безопасности.

Задание № 2. «Информационные и иные угрозы»

Вопросы:

1. Что такое угроза безопасности информации.

2. Приведите примеры программно-математических угроз.

3. Какие организационные угрозы вы знаете. Приведите примеры.

4. Как по вашему мнению возможна утечка информации по физическому каналу в аудиториях информатики филиала?

Задание:

Определите и классифицируйте угрозы безопасности вашего домашнего ПЭВМ.

Задание №3. «Организация защиты информации»

Вопросы:

1. Какие модели защиты информации вы знаете и их основные достоинства и недостатки?

2. Приведите примеры организации защиты информации (см.Таблицу 1)?

Таблица 1. Виды информационного пространства для организации защиты информации по вариантам

№ варианта	Вид информационного пространства для защиты
1, 5, 9 ,13	Корпоративная сеть
2, 6, 10,14	Локальная сеть
3, 7, 11,15	Сеть Internet
4, 8, 12,16	Файловая система

Задание:

В приведенном вами примере организации защиты информации найдите недостатки системы, предложите пути их устранения.

Задание №4. «Удаленное администрирование в сети»

Вопросы:

1. Какие способы аутентификации пользователей могут применяться в компьютерных системах?
2. В чем заключаются недостатки парольной аутентификации и как она может быть усилена?
3. Какова недостатки межсетевых экранов вы можете привести?
4. В чем сущность удаленного администрирования?

Задание:

Предложите схему удаленного администрирования сети филиала. Выбор схемы и соответствующего ПО обоснуйте.

Задание №5. «Безопасность автоматизированной информационной системы»

Вопросы:

1. В чем состоит предмет и объекты защиты информации в АСОД?
2. Что такое надежность информации и ее уязвимость?
3. Перечислите каналы несанкционированного получения информации в АСОД?
4. Каковы методы подтверждения подлинности пользователей и разграничения их доступа к компьютерным ресурсам?
5. Перечислите методы идентификации и установления подлинности субъектов и различных объектов.
6. В чем состоят задачи информационной целостности?
7. Что значит разграничение и контроль доступа к информации?

8. Какие имеются методы и средства защиты информации от случайных воздействий?

Задание:

Опишите каким образом осуществлено разграничение доступа к информационным ресурсам на вашей ПЭВМ, в случае отсутствия его обоснуйте.

для оценки сформированности компетенции ОПК 4

Задание № 6. «Антивирусная безопасность»

Вопросы:

1. В чем состоит проблема вирусного заражения программ?
2. Приведите пример современного вируса, способы его обнаружения и наносимый ущерб?
3. Какие вредоносные программные закладки кроме вирусов вам известны?
4. Какие существуют методы борьбы с компьютерными вирусами?

Задание:

Раскройте сущность приведенного вируса.

№ варианта	Вид вируса
1, 5, 9 ,13	Стелс-вирус
2, 6, 10,14	Boot- вирус
3, 7, 11,15	Макровирус
4, 8, 12,16	Вирус-червь

Задание № 7. «Антивирусные программы»

Вопросы:

1. Какие основные антивирусные программы вы знаете, кратко охарактеризуйте их.
2. Каким образом происходит лечение зараженных дисков?
3. Что такое программа – полифаг?
4. Что такое программа - детектор?

Задание:

Опишите антивирусные программы, которые вы использовали и используете в данный момент. Ваш выбор обоснуйте.

Задание №8. «Обеспечение технической безопасности»

Вопросы:

1. В чем заключается проблема обеспечения технической безопасности?
2. Приведите примеры отказа аппаратного обеспечения, создающего угрозу информационной безопасности.
3. В чем заключается сущность резервного копирования информации?
4. Какое программное и техническое обеспечение применяется при дублировании информации?
5. Каковы основные аспекты восстановления удаленной информации?
6. Опишите основные программы для восстановления информации?
7. В чем заключается необходимость разбивки жесткого диска на логические и каким программным обеспеченьем можно это произвести?

Задание:

Приведите примеры, когда вам приходилось восстанавливать удаленную информацию. Опишите и обоснуйте логическую разбивку вашего жесткого диска.

Задание №9. «Организационное обеспечение информационной безопасности»

Вопросы:

1. Что входит в понятие организационного обеспечения?

2. Приведите примеры и укажите области применения.
3. Какие основные виды организационного обеспечения безопасности используются в работе филиала.

Задание:

Определите какие организационные меры вы используете в своем быту, приведите примеры использования в учебном процессе.

Задание №10. «Правовое обеспечение информационной безопасности»

Вопросы:

1. Приведите основные законодательные и нормативные документы?
2. Каким образом можно их классифицировать?
3. Каковы перспективы дальнейшего развития в этой области вы видете?

Задание:

Определите какими нормативными документами ограничен круг задач, решаемых вами с использованием вашей домашней ПЭВМ.

Темы учебно-исследовательских реферативных работ

для оценки сформированности компетенции ОПК 3

1. Проблемы информационной безопасности.
2. Основные критерии классификации угроз информационной безопасности..
3. Наиболее распространенные угрозы доступности.
4. Вредоносное программное обеспечение.
5. Основные угрозы целостности.
6. Основные угрозы конфиденциальности.
7. Основные угрозы доступности.
8. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".
9. Административный уровень информационной безопасности.
10. Программа безопасности. Пример для предприятия.
11. Управление рисками.
12. Основные программно-технические меры.

для оценки сформированности компетенции ОПК 4

13. Идентификация и аутентификация.
14. Управление доступом.
15. Протоколирование и аудит.
16. Шифрование.
17. Алгоритмы шифрования.
18. Контроль целостности и Цифровые сертификаты.
19. Экранирование.
20. Классификация межсетевых экранов.
21. Туннелирование и управление доступом.
22. Информационная безопасность личности, общества, государства
23. Обеспечение информационной безопасности в сетях IP
24. Стандартизация в области информационной безопасности в сетях передачи данных
25. Стратегия обеспечения Информационной Безопасности предприятия

Типовые тестовые задания

для оценки сформированности компетенций ОПК 3

Вопрос 1. Защита информации от утечки включает в себя следующие мероприятия:

а) защиту информации от разглашения;

б) защиту информации от несанкционированного воздействия;

в) защиту информации от непреднамеренного воздействия;

г) защиту информации от несанкционированного доступа.

Вопрос 2. Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации – это:

а) защита информации от несанкционированного воздействия;

б) защита информации от непреднамеренного воздействия;

в) защита информации от разглашения;

г) защита информации от несанкционированного доступа.

Вопрос 3. Дайте определение конфиденциальности информации.

а) гарантия доступа санкционированных пользователей к информации;

б) обеспечение надежной идентификации источника сообщения, а также гарантия того, что источник не является поддельным;

в) обеспечение неизменности информации при ее передаче;

г) обеспечение просмотра информации в приемлемом формате только для пользователей, имеющих право доступа к этой информации.

Вопрос 4. Модификация передаваемой информации со стороны третьего лица приводит к нарушению:

а) конфиденциальности передаваемой информации;

б) доступности информации;

в) аутентичности передаваемой информации;

г) конфиденциальности и целостности передаваемой информации.

Вопрос 5. К какому уровню модели взаимодействия открытых систем относится фильтрующий маршрутизатор?

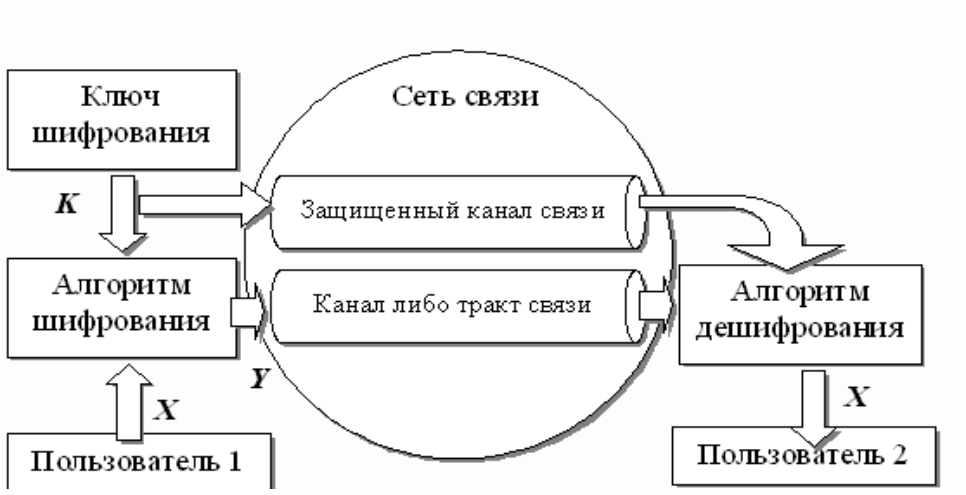
а) приложений;

б) транспортному;

в) сетевому;

г) сеансовому.

Вопрос 6. К какой криптосистеме относится приведенный рисунок?



а) с одним ключом;

б) с двумя ключами;

в) классическая криптосистема;

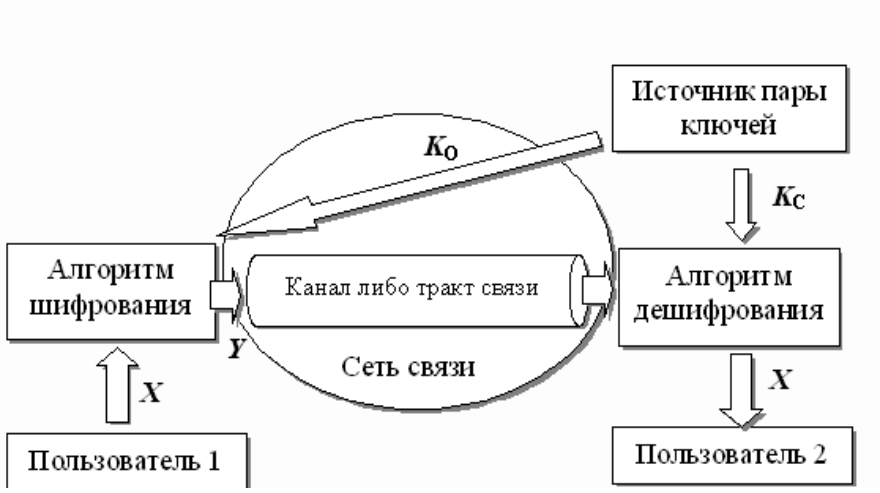
г) не относится к системе криптографии;

д) относится к симметричным криптосистемам;

е) относится к асимметричным криптосистемам.

1. верны варианты б, г, д;
2. верны варианты а, в, д;
3. верны варианты а, г, е;

Вопрос 7. К какой криптосистеме относится приведенный рисунок?



а) с одним ключом;
б) с двумя ключами;
в) классическая криптосистема;
г) не относится к системе криптографии;
д) относится к симметричным криптосистемам;
е) относится к асимметричным криптосистемам.
1. верны варианты б, г;
2. верны варианты а, в, г, д;
3. верны варианты а, в, г, е.

Вопрос 8. Известны следующие методы распределения открытых ключей:
1) индивидуальное публичное объявление открытых ключей пользователями;
2) использование публично доступного каталога открытых ключей;
3) участие авторитетного источника открытых ключей;
4) сертификаты открытых ключей.
Какой из методов не обеспечивает аутентификацию отправителя открытого ключа (КО)?
1. вариант 1;
2. вариант 2;
3. вариант 3;
4. вариант 4.

Вопрос 9. Совокупность требований безопасности и спецификаций, которая является основой для оценки конкретной системы информационной технологии – это:
а) задание по безопасности;
б) политика безопасности объекта оценки;
в) политика безопасности организации.

Вопрос 10. «Общие критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408 содержат:
а) критерии оценки безопасности, касающиеся административных мер безопасности, непосредственно не относящихся к мерам безопасности информационных технологий;
б) оценку специальных физических аспектов безопасности информационных технологий;
в) процедуры использования результатов оценки при аттестации продуктов и систем информационных технологий;
г) критерии для оценки специфических качеств криптографических алгоритмов;
д) механизмы для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий.

для оценки сформированности компетенции ОПК 4

Вопрос 11. «Общие критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408 для пользователя дают возможность:

1) руководство и справочник при формулировании требований к функциям безопасности;

2) справочник по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки;

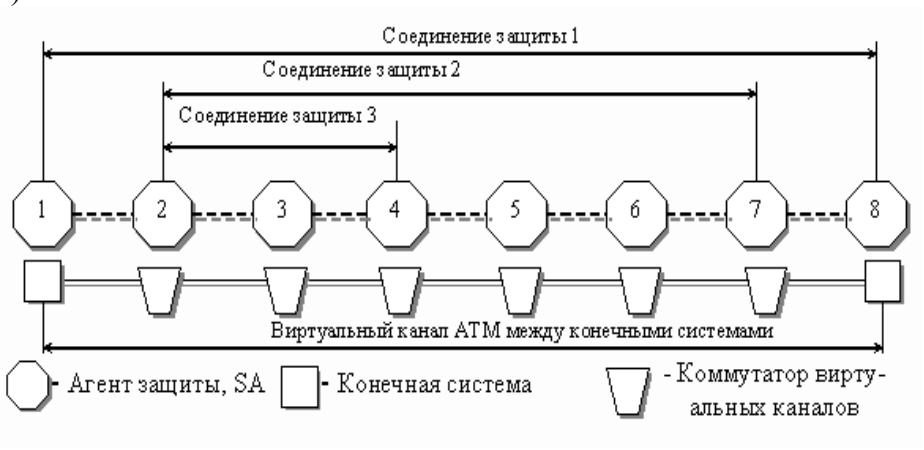
3) руководство по определению требуемого уровня доверия;

4) обязательное изложение критериев оценки, используемых при определении доверия к объектам оценки и оценки профилей защиты и заданий по безопасности.

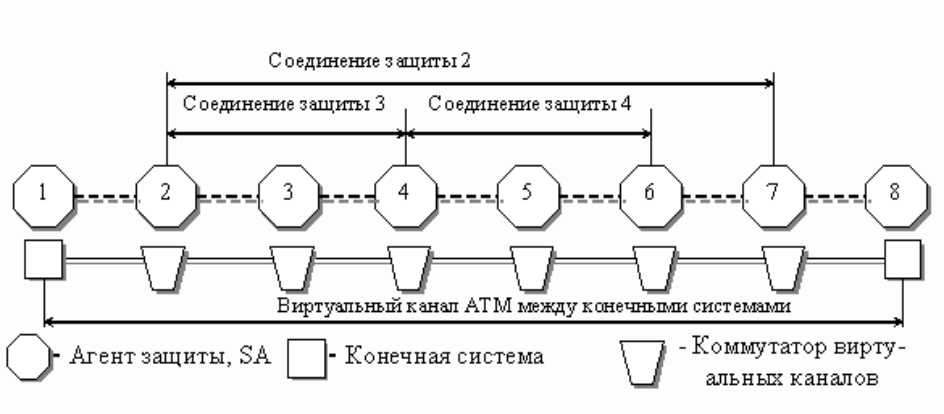
1. верны варианты 1, 3;
2. верны варианты 2, 4;
3. верны варианты 2, 3.

Вопрос 12. Определите правильный вариант организации соединений защиты информации.

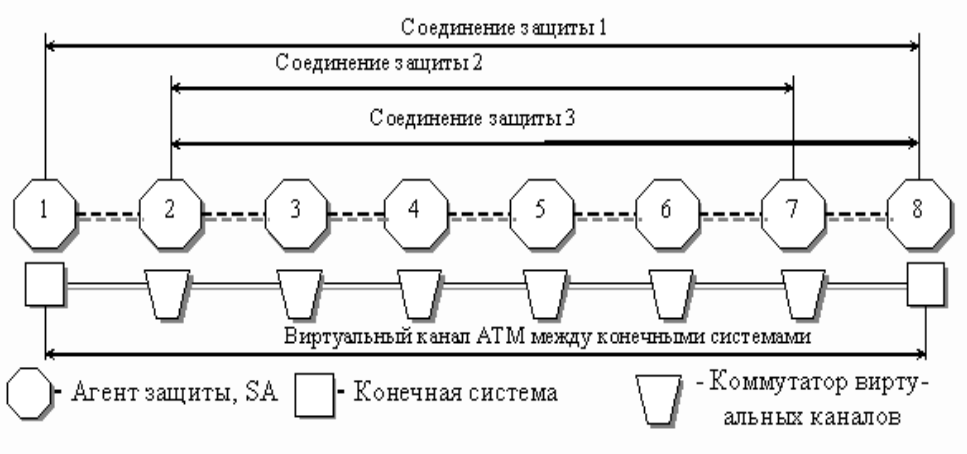
а)



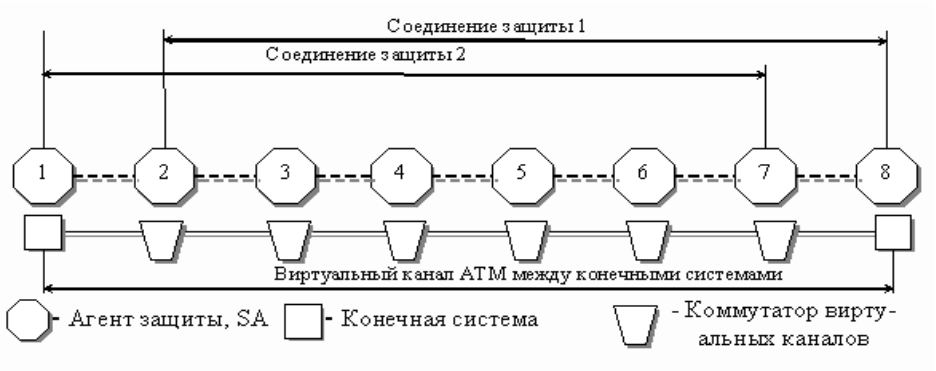
б)



в)



г)



д) верны варианты а, б.

Вопрос 13. Какое предельное количество уровней вложения соединений защиты возможно для технологии ATM?

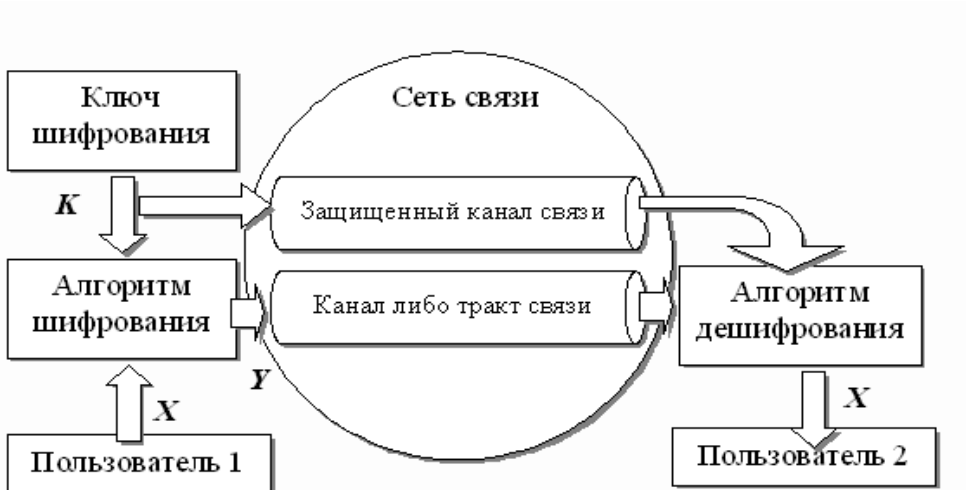
а) до 16 уровней;

б) до 32 уровней;

в) до 8 уровней;

г) до 8 уровней;

Вопрос 14. К какой криптосистеме относится приведенный рисунок?



а) с одним ключом;

б) с двумя ключами;

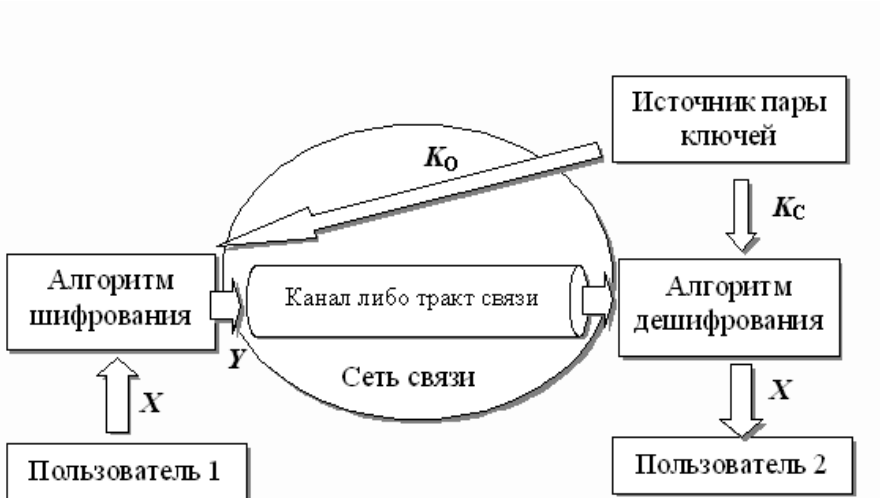
в) классическая криптосистема;

г) не относится к системе криптографии;

д) относится к симметричным криптосистемам;

е) относится к асимметричным криптосистемам.

Вопрос 15. К какой криптосистеме относится приведенный рисунок?



а) с одним ключом;
б) с двумя ключами;
в) классическая криптосистема;
г) не относится к системе криптографии;
д) относится к симметричным криптосистемам;
е) относится к асимметричным криптосистемам.

Вопрос 16. Какой оценочный уровень доверия позволяет разработчикам достичь высокого доверия путем применения специальных методов проектирования безопасности в строго контролируемой среде разработки с целью получения высококачественного объекта оценки для защиты высоко оцениваемых активов от значительных рисков?

а) 3;
б) 5;
в) 6;
г) 7;
д) 9.

Вопрос 17. Известны следующие методы распределения открытых ключей:

1) индивидуальное публичное объявление открытых ключей пользователями;
2) использование публично доступного каталога открытых ключей;
3) участие авторитетного источника открытых ключей;
4) сертификаты открытых ключей.

Какой из методов не обеспечивает аутентификацию отправителя открытого ключа (КО)?

1. вариант 1;
2. вариант 2;
3. вариант 3;
4. вариант 4.

Вопрос 18. Совокупность требований безопасности и спецификаций, которая является основой для оценки конкретной системы информационной технологии – это:

а) задание по безопасности;
б) политика безопасности объекта оценки;
в) политика безопасности организации.

Вопрос 19. «Общие критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408 содержат:

а) критерии оценки безопасности, касающиеся административных мер безопасности, непосредственно не относящихся к мерам безопасности информационных технологий;
б) оценку специальных физических аспектов безопасности информационных технологий;
в) процедуры использования результатов оценки при аттестации продуктов и систем информационных технологий;

г) критерии для оценки специфических качеств криптографических алгоритмов;

д) механизмы для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий.

Вопрос 20. «Общие критерии оценки безопасности информационных технологий» ГОСТ Р ИСО/МЭК 15408 для пользователя дают возможность:

1) руководство и справочник при формулировании требований к функциям безопасности;

2) справочник по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки;

3) руководство по определению требуемого уровня доверия;

4) обязательное изложение критериев оценки, используемых при определении доверия к объектам оценки и оценки профилей защиты и заданий по безопасности.

1. верны варианты 1, 3;
2. верны варианты 2, 4;
3. верны варианты 2, 3.

Вопрос 21. Профиль защиты – это:

а) совокупность требований безопасности;

б) базовый набор требований доверия для оценки;

в) краткая спецификация объекта оценки совместно с требованиями и целями безопасности.

Вопрос 22. Какое количество оценочных уровней доверия предложено ГОСТ Р ИСО/МЭК 15048?

а) 3;

б) 5;

в) 7;

г) 9.

Контрольные вопросы для промежуточной аттестации (к зачету)

№	Вопрос	Код формируемой компетенции
	1.Общая характеристика компьютерных вирусов.	*ОПК-3*
	2.Классификация компьютерных вирусов.	*ОПК-4*
	3. Принципы проявления вирусов.	*ОПК-3*
	4. Структура вируса.	*ОПК-3*
	5. Пути распространения вирусов.	*ОПК-4*
	6. Основные особенности наиболее распространенных вирусов.	*ОПК-3*
	7. Модели поведения вирусов и их деструктивные действия: файловые вирусы.	*ОПК-3*
	8. Модели поведения вирусов и их деструктивные действия: загрузочные вирусы.	*ОПК-4*
	9. Модели поведения вирусов и их деструктивные действия: steals-вирусы.	*ОПК-3*
	10. Модели поведения вирусов и их деструктивные действия: полиморфные вирусы.	*ОПК-3*
	11. Модели поведения вирусов и их деструктивные действия: макровирусы.	*ОПК-4*
	12. Модели поведения вирусов и их деструктивные действия: сетевые вирусы.	*ОПК-3*
	13. Модели поведения вирусов и их деструктивные действия: резидентные вирусы.	*ОПК-3*
	14. Программы-шпионы: понятие, назначение, виды и группы.	*ОПК-4*
	15. Взлом парольной защиты.	*ОПК-3*
	16. Защита от воздействия вирусов: архивирование, входной контроль.	*ОПК-3*
	17. Защита от воздействия вирусов: профилактика, ревизия, карантин.	*ОПК-4*
	18. Защита от воздействия вирусов: сегментация, фильтрация, вакцинация, автоконтроль целостности, терапия.	*ОПК-3*
	19. Состав программного комплекса защиты от компьютерных вирусов (перечислить и объяснить компоненты).	*ОПК-3*
	20. Перечислить и объяснить средства нейтрализации компьютерных вирусов.	*ОПК-4*
	21. История становления российского законодательства в области информационных технологий.	*ОПК-3*
	22. Объяснить основные принципы главы 1 и 2 закона РФ «О правовой охране программ для ЭВМ и баз данных» -1.	*ОПК-3*
	23. Объяснить основные принципы главы 3 и 4 закона РФ «О правовой охране программ для ЭВМ и баз данных» -1.	*ОПК-4*

	24. Виды компьютерных правонарушений: несанкционированный доступ, встраивание в программное обеспечение «логических бомб», разработка и распространение компьютерных вирусов.	*ОПК-3*
	25. Виды компьютерных правонарушений: подделка компьютерной информации, хищение компьютерной информации, нарушение авторского права.	*ОПК-3*

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

а) основная литература:

1. Васильев В.И. Интеллектуальные системы защиты информации: учеб. пособие/ В. И. Васильев. 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - 172 с. – ЭБС «Консультант обучающегося»: [Электронный ресурс]. – Адрес доступа: http://www.studentlibrary.ru/book/ISBN9785942756673.html

2. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие: / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2017. - 239 с.: ил. – ЭБС Znanium.com: [Электронный ресурс]. – Адрес доступа: http://znanium.com/catalog/product/612572

3. 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

4. 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

б) дополнительная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. ЭБС Znanium.com: [Электронный ресурс]. – Адрес доступа: http://znanium.com/catalog.php?bookinfo=405000

2. Ковалев Д.В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1 - Режим доступа: http://znanium.com/catalog/product/997105

3. Внуков, А. А. Защита информации в банковских системах: учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083

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

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 **Информационная безопасность** составлена в соответствии с образовательным стандартом высшего образования (ОС ННГУ) по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата) (приказ ННГУ от 17.05.2023 года № 06.49-04-0214/23)

Автор(ы):
старший преподаватель Сазанов А.А.

Рецензент (ы):
к.п.н., доцент Фокеев М.И.

Кафедра математики, физики и информатики

д.п.н., доцент Фролов И.В.

Программа одобрена на заседании методической комиссии от 24.05.2023 года, протокол № 5

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

П.6. а) СОГЛАСОВАНО:

Заведующий библиотекой Федосеева Т.А.