



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

В Г.ВОЛГОДОНСКЕ РОСТОВСКОЙ ОБЛАСТИ

(Филиал ДГТУ в г. Волгодонске)



УТВЕРЖДАЮ

И.о. директора

Н.М. Сидоркина

«22» апреля 2024 г.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(ОЦЕНОЧНЫЕ СРЕДСТВА)**

**для проведения текущего контроля и промежуточной аттестации
по дисциплине**

«Информационная безопасность»

для обучающихся по направлению подготовки (специальности)

09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

программа бакалавриата

2024 года набора

Волгодонск
2024

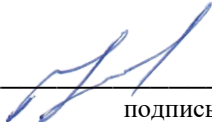
Лист согласования


Оценочные материалы (оценочные средства) по дисциплине
«Информационная безопасность»
(наименование)

составлены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности)
09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ,
(код направления (специальности), наименование)

Рассмотрены и одобрены на заседании кафедры «Технический сервис и информационные технологии» протокол № 9 от «22» апреля 2024 г

Разработчики оценочных материалов (оценочных средств)

Доцент  Н.В.Кочковая
подпись

Заведующий кафедрой  Н.В.Кочковая.
подпись

Согласовано:
Директор НПЦ
«Микроэлектроника»  С.Л. Бондаренко
подпись

Начальник отдела ПО
ООО «Топаз-сервис»  Д.В. Чубукин
подпись

**Лист визирования оценочных материалов (оценочных средств)
на очередной учебный год**

Оценочные материалы (оценочные средства) по дисциплине «Информационная безопасность» проанализированы и признаны актуальными для использования на 20__ - 20__ учебный год.

Протокол заседания кафедры «Технический сервис и информационные технологии» от «__» _____ 20__ г. № _____

Заведующий кафедрой «ТСиИТ» _____ Н.В.Кочковая
«__» _____ 20__ г.

Оценочные материалы (оценочные средства) по дисциплине «Информационная безопасность» проанализированы и признаны актуальными для использования на 20__ - 20__ учебный год.

Протокол заседания кафедры «Технический сервис и информационные технологии» от «__» _____ 20__ г. № _____

Заведующий кафедрой «ТСиИТ» _____ Н.В.Кочковая
«__» _____ 20__ г.

Оценочные материалы (оценочные средства) по дисциплине «Информационная безопасность» проанализированы и признаны актуальными для использования на 20__ - 20__ учебный год.

Протокол заседания кафедры «Технический сервис и информационные технологии» от «__» _____ 20__ г. № _____

Заведующий кафедрой «ТСиИТ» _____ Н.В.Кочковая
«__» _____ 20__ г.

Оценочные материалы (оценочные средства) по дисциплине «Информационная безопасность» проанализированы и признаны актуальными для использования на 20__ - 20__ учебный год.

Протокол заседания кафедры «Технический сервис и информационные технологии» от «__» _____ 20__ г. № _____

Заведующий кафедрой «ТСиИТ» _____ Н.В.Кочковая
«__» _____ 20__ г.

1 Паспорт оценочных материалов (оценочных средств)

1.1 Перечень компетенций, формируемых дисциплиной (модулем), с указанием этапов их формирования в процессе освоения ОПОП

1.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования

1.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, описание шкал оценивания

2 Контрольные задания (демоверсии) для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

1 Паспорт оценочных материалов (оценочных средств)

Оценочные материалы (оценочные средства) прилагаются к рабочей программе дисциплины и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения обучающимся установленных результатов обучения.

Оценочные материалы (оценочные средства) используются при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся.

1.1 Перечень компетенций, формируемых дисциплиной, с указанием этапов их формирования в процессе освоения ОПОП

Перечень компетенций, формируемых в процессе изучения дисциплины:

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решения задач профессиональной деятельности.

ОПК-5: Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем.

Конечными результатами освоения дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование дескрипторов происходит в течение всего семестра по этапам в рамках контактной работы, включающей различные виды занятий и самостоятельной работы, с применением различных форм и методов обучения (табл. 1).

Таблица 1 Формирование компетенций в процессе изучения дисциплины

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции	Планируемые результаты обучения (показатели достижения заданного уровня компетенции)	Вид учебных занятий, работы, формы и методы обучения, способствующие формированию и развитию компетенции	Контролируемые разделы и темы дисциплины	Оценочные материалы (оценочные средства), используемые для оценки уровня сформированности компетенции	Критерии оценивания компетенций
УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1: Знает принципы сбора, отбора и обобщения информации	методы обобщения информации в области ИБ	Лек, Прак.раб., Ср интерактивная лекция	1.1, 2.2, 3.3, 4.1, 4.2, 5.1, 6.1, 6.2, 6.4, 7.1, 8.1, 8.2, 9.1-9.3, 10.1, 12.1, 13.2, 14.1, 14.3	Контрольные вопросы	Ответы на контрольные вопросы; Выполнение практической работы и ее защита по контрольным вопросам в форме собеседования
	УК-1.2: Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности	систематизировать информацию в области ИБ	Лек, Прак.раб., Ср анализ практических работ		Практическая работа	
	УК-1.3: Имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов	практический опыт работы поиска информации по защите компьютерных систем	Лек, Прак.раб., Ср анализ практических работ		Практическая работа	
ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при	ОПК-2.1: Знает содержание и принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, используемых при решении задач профессиональной деятельности	современные ИТ и ПО для решения задач защиты информации	Лек, Прак.раб., Ср интерактивная лекция	2.1, 3.1, 3.2, 4.4, 4.5, 5.1, 6.1-6.4, 7.1, 7.2, 8.1-8.3, 9.2, 10.3, 11.2, 11.3, 12.2, 13.1, 14.2, 14.3	Контрольные вопросы	Ответы на контрольные вопросы; Выполнение практической работы и ее защита по контрольным вопросам в форме собеседования

решения задач профессиональной деятельности	ОПК-2.2: Умеет применять современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	выбирать современные ИТ и программные средства для защиты информации на предприятии	Лек, Прак. раб., Ср работа в малых группах, анализ практических работ		Практическая работа	
	ОПК-2.3: Владеет навыками решения задач профессиональной деятельности с помощью современных информационных технологий и программных средств, в том числе отечественного производства	навыками применения средств защиты информации	Лек, Прак. раб., Ср работа в малых группах, анализ практических работ		Практическая работа	
ОПК-5: Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем;	ОПК-5.1: Знает основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем	основы сетевого администрирования для обеспечения ИБ	Лек, Прак. раб., Ср интерактивная лекция	2.2, 2.3, 3.2, 3.3, 4.1, 4.4, 6.3, 7.2, 7.3, 9.1, 9.3, 11.2, 11.3, 12.2, 13.2, 13.3, 14.1, 14.3	Контрольные вопросы	Ответы на контрольные вопросы; Выполнение практической работы и ее защита по контрольным вопросам в форме собеседования
	ОПК-5.2: Умеет выполнять параметрическую настройку информационных и автоматизированных систем	выполнять настройку ИТ для защиты информации	Лек, Прак. раб., Ср работа в малых группах, анализ практических работ		Практическая работа	
	ОПК-5.3: Владеет навыками установки программного и аппаратного обеспечения информационных и автоматизированных систем	навыками установки ПО для защиты информации в компьютерных системах	Лек, Прак. раб., Ср работа в малых группах, анализ практических работ		Практическая работа	

1.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оценивание результатов обучения по дисциплине осуществляется в соответствии с Положением о текущем контроле и промежуточной аттестации обучающихся.

По дисциплине «Информационная безопасность» предусмотрены следующие виды контроля: текущий контроль (осуществление контроля всех видов аудиторной и внеаудиторной деятельности обучающегося с целью получения первичной информации о ходе усвоения отдельных элементов содержания дисциплины); промежуточная аттестация (оценивается уровень и качество подготовки по дисциплине в целом).

Текущий контроль в семестре проводится с целью обеспечения своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающихся. Текущий контроль служит для оценки объёма и уровня усвоения обучающимся учебного материала одного или нескольких разделов дисциплины (модуля) в соответствии с её рабочей программой и определяется результатами текущего контроля знаний обучающихся.

Текущий контроль осуществляется два раза в семестр по календарному графику учебного процесса.

Текущий контроль предполагает начисление баллов за выполнение различных видов работ. Результаты текущего контроля подводятся по шкале балльно-рейтинговой системы. Регламент балльно-рейтинговой системы определен Положением о системе «Контроль успеваемости и рейтинг обучающихся».

Текущий контроль является результатом оценки знаний, умений, навыков и приобретенных компетенций обучающихся по всему объёму учебной дисциплины, изученному в семестре, в котором стоит форма контроля в соответствии с учебным планом.

Текущий контроль успеваемости предусматривает оценивание хода освоения дисциплины: теоретических основ и практической части.

При обучении по заочной форме обучения текущий контроль не предусмотрен.

Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в форме экзамена в 8 семестре (для заочной формы обучения экзамена на 4 курсе).

В табл. 2 приведено весовое распределение баллов и шкала оценивания по видам контрольных мероприятий.

Таблица 2 – Весовое распределение баллов и шкала оценивания по видам контрольных мероприятий с формой контроля экзамен

Текущий контроль (50 баллов ¹)						Промежуточная аттестация (50 баллов)	Итоговое количество баллов по результатам текущего контроля и промежуточной аттестации
Блок 1			Блок 2				
Лекционные занятия (X ₁)	Практические занятия (Y ₁)	Лабораторные занятия (Z ₁)	Лекционные занятия (X ₂)	Практические занятия (Y ₂)	Лабораторные занятия (Z ₂)	от 0 до 50 баллов	Менее 41 балла – неудовлетворительно 41-60 баллов – удовлетворительно 61-80 баллов – хорошо; 81-100 баллов – отлично
5	-	20	5	-	20		
Сумма баллов за 1 блок = X ₁ + Y ₁ + Z ₁			Сумма баллов за 2 блок = X ₂ + Y ₂ + Z ₂				

¹ Вид занятий по дисциплине (лекционные, практические, лабораторные) определяется учебным планом. Количество столбцов таблицы корректируется в зависимости от видов занятий, предусмотренных учебным планом.

Распределение баллов по блокам, по каждому виду занятий в рамках дисциплины определяет преподаватель. Распределение баллов по дисциплине утверждается протоколом заседания кафедры

По заочной форме обучения мероприятия текущего контроля не предусмотрены.

Для определения фактических оценок каждого показателя выставляются следующие баллы (табл.3):

Таблица 3– Распределение баллов по дисциплине

Вид учебных работ по дисциплине	Количество баллов	
	1 блок	2 блок
<i>Текущий контроль (50 баллов)</i>		
Посещение занятий	5	5
Выполнение письменных заданий	10	10
Выполнение практических задач	5	5
Выполнение дополнительных заданий (доклад, публикация статьи)	5	5
<i>Промежуточная аттестация (50 баллов)</i>		
<i>Необходимо описать методику формирования результирующей оценки по дисциплине (форма проведения (устная, письменная), критерии получения оценки и др.)</i>		
<p>Экзамен по дисциплине «Информационная безопасность» проводится в устной форме в виде ответов на вопросы для промежуточной аттестации. Задание состоит из 3 вопросов. Первый и второй вопрос позволяют проконтролировать знания обучающегося, третий – умения и навыки. Правильные ответы на первый и второй вопросы оцениваются в 15 баллов, третий – в 20 баллов. За неверно выполненное задание – 0 баллов.</p>		
Сумма баллов по дисциплине 100 баллов		

Экзамен является формой итоговой оценки качества освоения обучающимся образовательной программы по дисциплине в целом или по разделу дисциплины. По результатам экзамена обучающемуся выставляется оценка «отлично», «хорошо», «удовлетворительно», или «неудовлетворительно».

Оценка «отлично» (81-100 баллов) выставляется обучающемуся, если:

- обучающийся набрал по текущему контролю необходимые и достаточные баллы для выставления оценки автоматом²;
- обучающийся знает, понимает основные положения дисциплины, демонстрирует умение применять их для выполнения задания, в котором нет явно указанных способов решения;
- обучающийся анализирует элементы, устанавливает связи между ними, сводит их в единую систему, способен выдвинуть идею, спроектировать и презентовать свой проект (решение);
- ответ обучающегося по теоретическому и практическому материалу, содержащемуся в вопросах экзаменационного билета, является полным, и удовлетворяет требованиям программы дисциплины;
- обучающийся продемонстрировал свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей дисциплины;

² Количество и условия получения необходимых и достаточных для получения автомата баллов определены Положением о системе «Контроль успеваемости и рейтинг обучающихся»

- на дополнительные вопросы преподавателя обучающийся дал правильные ответы.

Компетенция (и) или ее часть (и) сформированы на высоком уровне (уровень 3) (см. табл. 1).

Оценка «хорошо» (61-80 баллов) выставляется обучающемуся, если:

- обучающийся знает, понимает основные положения дисциплины, демонстрирует умение применять их для выполнения задания, в котором нет явно указанных способов решения; анализирует элементы, устанавливает связи между ними;

- ответ по теоретическому материалу, содержащемуся в вопросах экзаменационного билета, является полным, или частично полным и удовлетворяет требованиям программы, но не всегда дается точное, уверенное и аргументированное изложение материала;

- на дополнительные вопросы преподавателя обучающийся дал правильные ответы;

- обучающийся продемонстрировал владение терминологией соответствующей дисциплины.

Компетенция (и) или ее часть (и) сформированы на среднем уровне (уровень 2) (см. табл. 1).

Оценка «удовлетворительно» (41-60 баллов) выставляется обучающемуся, если:

- обучающийся знает и воспроизводит основные положения дисциплины в соответствии с заданием, применяет их для выполнения типового задания в котором очевиден способ решения;

- обучающийся продемонстрировал базовые знания важнейших разделов дисциплины и содержания лекционного курса;

- у обучающегося имеются затруднения в использовании научно-понятийного аппарата в терминологии курса;

- несмотря на недостаточность знаний, обучающийся имеется стремление логически четко построить ответ, что свидетельствует о возможности последующего обучения.

Компетенция (и) или ее часть (и) сформированы на базовом уровне (уровень 1) (см. табл. 1).

Оценка «неудовлетворительно» (менее 41 балла) выставляется обучающемуся, если:

- обучающийся имеет представление о содержании дисциплины, но не знает основные положения (темы, раздела, метода т.д.), к которому относится задание, не способен выполнить задание с очевидным решением, не владеет навыками настройки параметров безопасности информационной системы, сети и операционных систем;

- у обучающегося имеются существенные пробелы в знании основного материала по дисциплине;

- в процессе ответа по теоретическому материалу, содержащемуся в вопросах экзаменационного билета, допущены принципиальные ошибки при изложении материала.

Компетенция(и) или ее часть (и) не сформированы.

1.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Практическая работа в форме отчета, защита отчета по контрольным вопросам к практической работе в форме собеседования.

Практическая работа – это один из основных видов работы обучающихся и важный этап их профессиональной подготовки. Основными целями практической работы являются: расширение и углубление знаний обучающихся, выработка умений и навыков самостоятельно выполнять эксперименты, выработка приемов и навыков в анализе теоретического и практического материала, использования известных закономерностей и статистической обработке экспериментального материала, его аналитического и графического представления, а также обучение логично, правильно, ясно, последовательно и кратко излагать свои мысли в письменном виде. Обучающийся, со своей стороны, при выполнении практической работы должен показать умение работать с литературой, давать сравнительный анализ известных экспериментальных данных по теме практической работы, обрабатывать массив экспериментальных данных и, главное, – правильно интерпретировать полученные результаты.

Студентам в процессе оформления отчета практической работы необходимо выполнить ряд требований:

1. Отчеты по практическим работам оформляются в электронном виде.
2. Текст должен быть написан грамотно. Все поля по 2 см. Шрифт 14 шт.
3. На первом листе отчета должны быть указаны: номер работы, название, цель. Далее приводится краткий теоретический материал по теме (термины, понятия, физические законы), этапы выполнения работы, расчетные формулы.
3. Таблицы с исходной информацией должны иметь концевые (в конце отчета в виде отдельного списка) ссылки на источники информации, откуда эта информация получена. Все таблицы должны быть пронумерованы и иметь названия;
4. Все части работы необходимо озаглавить, страницы – пронумеровать (нумерация отдельная по каждой практической работе);
5. Полученные экспериментальные данные представляются в виде скринов, таблиц и/или графического материала, если необходимо, то обрабатываются с помощью статистических методов. Работа обязательно должна иметь выводы, сформулированные по результатам ее выполнения.
6. При необходимости, работа может заканчиваться списком использованных источников в соответствии с порядком упоминания в тексте с указанием: для книг автора, названия литературного источника, города, издательства, года издания, количества страниц; для журнальных статей: авторы, название, журнал, год издания, том, номер, страницы.
7. Практической работой предусмотрены краткие ответы на контрольные вопросы в письменном виде после отчета о выполнении работы,

которые могут быть по решению преподавателя использованы в ходе собеседования.

2 Контрольные задания (демоверсии) для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

2.1 Задания для оценивания результатов обучения в виде знаний

Перечень примерных вопросов к экзамену

- 1 Информационная безопасность. Основные определения.
- 2 Угрозы информационной безопасности.
- 3 Модель системы защиты.
- 4 Организационные меры и меры обеспечения физической безопасности.
- 5 Идентификация и аутентификация. Методы аутентификации.
- 6 Особенности парольных систем аутентификации: рекомендации по практической реализации парольных систем, оценка стойкости парольных систем, методы хранения паролей.
- 7 Методы разграничения доступа.
- 8 Криптографические методы обеспечения конфиденциальности информации.
- 9 Методы защиты внешнего периметра.
- 10 Системы обнаружения вторжений (Intrusion Detection System, EDS)
- 11 Протоколирование и аудит.
- 12 Построение систем защиты от угроз нарушения целостности: типовая структура такой системы.
- 13 Криптографические методы обеспечения целостности информации: реализация механизма цифровой подписи, криптографические хэш-функции и ее преимущества, коды проверки подлинности.
- 14 Структура системы защиты от угроз нарушения доступности: поясните основные составляющие.
- 15 Формальные модели управления доступом: модель Харрисона-Рузсо-Ульмана, модель Белл-ЛаПалулы.
- 16 Формальные модели целостности: .модель Кларка-Вилсона, модель Биба.
- 17 Ролевая модель управления доступом
- 18 Классификация стандартов в области информационной безопасности
- 19 Структура профиля защиты
- 20 Структура задания по безопасности, структура класса доверия
- 21 Модель управления рисками по Британскому стандарту BS 7799-3:2006
- 22 Задачи государства в области информационной безопасности.
- 23 Законодательная база информатизации общества.
- 24 Структура государственных органов, обеспечивающих политику информационной безопасности в России.

Критерий оценки:

Полнота ответа на поставленный вопрос, умение использовать термины, формулы, приводить примеры, делать выводы и анализировать конкретные ситуации.

Шкала оценивания

Максимальное количество баллов, которое обучающийся может получить за промежуточную аттестацию (зачет) составляет 50 баллов.

Оценка «отлично» – 81-100 баллов;

Оценка «хорошо» – 61-80 баллов;

Оценка «удовлетворительно» – 41-60 баллов;

Оценка «неудовлетворительно» – менее 41 балла.

2.2 Задания для оценивания результатов в виде владений и умений

Темы практических работ указаны в рабочей программе дисциплины.

Выполнение практических работ, оформление отчета к практическим работам, включающим краткий теоретический материал, результаты эксперимента, их анализ и представление, защита в форме собеседования по контрольным вопросам.

Перечень контрольных вопросов для защиты практических работ приведен в конце каждой работы в методических указаниях к ним или в лабораторном практикуме.

Критерии оценки:

Критерий	Показатель	Максимальное количество баллов
1. Выполнение практической работы	- освоение методики настройки и исследования с использованием необходимого оборудования, включая подготовку инструмента и материалов.	5
2. Подготовка отчета по работе	- краткое теоретическое описание физических основ рассматриваемой методики, описание схемы сети и порядка настройки программы и исследования при проведении экспериментов, - достоверность полученных данных, - наглядность представления полученных результатов, - логичность, обоснованность сделанных в работе выводов.	10
2. Защита работы по контрольным вопросам в форме собеседования	- правильность и полнота ответов, их обоснованность - анализ недостатков и достоинств использованного метода исследования.	20
3. Соблюдение требований по оформлению отчета	- правильное оформление текста отчета, ссылок на используемые литературные источники; грамотность и культура изложения - правильность оформления графического материала с указанием единиц измерения величин	5

Отчет рассматривается как критерий оценки только при выполнении студентом лабораторной работы. Студент не допускается к защите лабораторной работы без ее выполнения и/или при отсутствии отчета.

Максимальное количество баллов, которое обучающийся может получить за проведение всех указанных в рабочей программе практических работ составляет 40 баллов. Баллы учитываются в процессе проведения текущего контроля.

- 40 баллов – оценка «отлично»;
- 30-40 баллов – оценка «хорошо»;
- 20 -30 баллов – оценка «удовлетворительно»
- Менее 20 баллов – оценка «неудовлетворительно»

2.3 Типовые экзаменационные материалы

Пример зачетного задания по дисциплине «Информационная безопасность»:

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
В Г.ВОЛГОДОНСКЕ РОСТОВСКОЙ ОБЛАСТИ
(Филиал ДГТУ в г. Волгодонске)

Факультет Технологии и менеджмент
Кафедра Технический сервис и информационные технологии

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1
на 2022 / 2023 учебный год

Дисциплина Информационная безопасность

- 1 Информационная безопасность. Основные определения
- 2 Общая характеристика организационных методов защиты информации в компьютерных системах
- 3 Основные положения ISO/IEC 15408. Критерии оценки безопасности информационных технологий. Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002

Преподаватель _____	Подпись	Семенов В.В.	Дата
Зав.кафедрой _____	Подпись	Н.В.Кочковая	27.11.2023
		Ф.И.О.	Дата

20__/20__ уч.год _____	Подпись	Ф.И.О. зав.каф.	АКТУАЛЬНО НА
			20__/20__ уч.год _____
			Подпись Ф.И.О. зав.каф.

20__/20__ уч.год _____	Подпись	Ф.И.О. зав.каф.	20__/20__ уч.год _____
			Подпись Ф.И.О. зав.каф.

Карта тестовых заданий

Компетенция:

ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решения задач профессиональной деятельности;

Дисциплина: Информационная безопасность

Описание теста:

1. Тест состоит из 85 заданий, которые проверяют уровень освоения компетенций обучающегося. При тестировании каждому обучающемуся предлагается 30 тестовых заданий по 15 открытого и закрытого типов разных уровней сложности.

2. За правильный ответ тестового задания обучающийся получает 1 условный балл, за неправильный ответ – 0 баллов. По окончании тестирования, система автоматически определяет «заработанный итоговый балл» по тесту, согласно критериям оценки

3 Максимальная общая сумма баллов за все правильные ответы составляет – 100 баллов.

4. Тест успешно пройден, если обучающийся правильно ответил на 70% тестовых заданий (61 балл).

5. На прохождение тестирования, включая организационный момент, обучающимся отводится не более 45 минут. На каждое тестовое задание в среднем по 1,5 минуты.

6. Обучающемуся предоставляется одна попытка для прохождения компьютерного тестирования.

Кодификатором теста по дисциплине является раздел рабочей программы «4. Структура и содержание дисциплины (модуля)»

Комплект тестовых заданий

Задания закрытого типа

Задания альтернативного выбора

Выберите один правильный ответ

Простые (1 уровень)

1 Кто является основным ответственным за определение уровня классификации информации?

- А. Руководитель среднего звена
- Б. Высшее руководство
- В. Владелец**
- Г. Пользователь

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

- А. Сотрудники**
- Б. Хакеры
- В. Атакующие
- Г. Контрагенты (лица, работающие по договору)

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

- А. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
- Б. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
- В. Улучшить контроль за безопасностью этой информации**

4 Что самое главное должно продумать руководство при классификации данных?

- А. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
- Б. Необходимый уровень доступности, целостности и конфиденциальности**
- В. Оценить уровень риска и отменить контрмеры
- Г. Управление доступом, которое должно защищать данные

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

- А. Владельцы данных
- Б. Пользователи
- В. Администраторы
- Г. **Руководство**

Средне–сложные (2 уровень)

6 Что такое процедура?

- А. Правила использования программного и аппаратного обеспечения в компании
- Б. **Пошаговая инструкция по выполнению задачи**
- В. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
- Г. Обязательные действия

7 Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

- А. **Поддержка высшего руководства**
- Б. Эффективные защитные меры и методы их внедрения
- В. Актуальные и адекватные политики и процедуры безопасности
- Г. Проведение тренингов по безопасности для всех сотрудников

8 Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

- А. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- Б. Когда риски не могут быть приняты во внимание по политическим соображениям
- В. Когда необходимые защитные меры слишком сложны
- Г. **Когда стоимость контрмер превышает ценность актива и потенциальные потери**

9 Что такое политики безопасности?

- А. Пошаговые инструкции по выполнению задач безопасности
- Б. Общие руководящие требования по достижению определенного уровня безопасности
- В. **Широкие, высокоуровневые заявления руководства**
- Г. Детализированные документы по обработке инцидентов безопасности

10 Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- А. Анализ рисков
- Б. **Анализ затрат / выгоды**
- В. Результаты ALE
- Г. Выявление уязвимостей и угроз, являющихся причиной риска

11 Что лучше всего описывает цель расчета ALE?

- А. Количественно оценить уровень безопасности среды
- Б. Оценить возможные потери для каждой контрмеры
- В. Количественно оценить затраты / выгоды
- Г. **Оценить потенциальные потери от угрозы в год**

12 Тактическое планирование – это:

- А. **Среднесрочное планирование**

- Б. Долгосрочное планирование
 - В. Ежедневное планирование
 - Г. Планирование на 6 месяцев
- 13 Что является определением воздействия (exposure) на безопасность?
- А. Нечто, приводящее к ущербу от угрозы**
 - Б. Любая потенциальная опасность для информации или систем
 - В. Любой недостаток или отсутствие информационной безопасности
 - Г. Потенциальные потери от угрозы
- 14 Эффективная программа безопасности требует сбалансированного применения:
- А. Технических и нетехнических методов**
 - Б. Контрмер и защитных механизмов
 - В. Физической безопасности и технических средств защиты
 - Г. Процедур безопасности и шифрования
- 15 Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
- А. Внедрение управления механизмами безопасности
 - Б. Классификацию данных после внедрения механизмов безопасности
 - В. Уровень доверия, обеспечиваемый механизмом безопасности**
 - Г. Соотношение затрат / выгод
- 16 Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
- А. Только военные имеют настоящую безопасность
 - Б. **Коммерческая компания обычно больше заботится о целостности и доступности** данных, а военные – о конфиденциальности
 - В. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
 - Г. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности
- 17 Как рассчитать остаточный риск?
- А. Угрозы x Риски x Ценность актива
 - Б. (Угрозы x Ценность актива x Уязвимости) x Риски
 - В. SLE x Частоту = ALE
 - Г. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля**
- 18 Что из перечисленного не является целью проведения анализа рисков?
- А. Делегирование полномочий**
 - Б. Количественная оценка воздействия потенциальных угроз
 - В. Выявление рисков
 - Г. Определение баланса между воздействием риска и стоимостью необходимых контрмер
- 19 Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
- А. Поддержка
 - Б. Выполнение анализа рисков**
 - В. Определение цели и границ
 - Г. Делегирование полномочий

20 Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

- А. Чтобы убедиться, что проводится справедливая оценка
- Б. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
- В. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа**
- Г. г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21 Что является наилучшим описанием количественного анализа рисков?

- А. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- Б. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
- В. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
- Г. Метод, основанный на суждениях и интуиции

22 Почему количественный анализ рисков в чистом виде не достижим?

- А. Он достижим и используется
- Б. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
- В. Это связано с точностью количественных элементов
- Г. Количественные измерения должны применяться к качественным элементам

Сложные (3 уровень)

23 Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

- А. Много информации нужно собрать и ввести в программу**
- Б. Руководство должно одобрить создание группы
- В. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
- Г. Множество людей должно одобрить данные

24 Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

- А. Стандарты
- Б. Должный процесс (Due process)
- В. Должная забота (Due care)**
- Г. Снижение обязательств

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

- А. Список стандартов, процедур и политик для разработки программы безопасности
- Б. Текущая версия ISO 17799
- В. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
- Г. Открытый стандарт, определяющий цели контроля**

Задания на установление соответствия*Установите соответствие между левым и правым столбцами.***Простые (1 уровень)**

26 Установите соответствие:

(1В, 2А)

- | | |
|--|--|
| 1 Из каких четырех доменов состоит CobIT? | А) Стандарт по защите персональных данных о здоровье |
| 2 Что представляет собой стандарт ISO/IEC 27799? | Б) Определения для новой серии ISO 27000
В) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка |

27 Установите соответствие:

(1Б, 2А)

- | | |
|---|---|
| 1 CobIT был разработан на основе структуры COSO. Что является основными целями и задачами COSO? | А) NIST и OCTAVE ориентирован на ИТ
Б) COSO относится к стратегическому уровню, тогда как CobIT больше направлен на операционный уровень |
| 2 OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами? | В) COSO – это система отказоустойчивости |

Средне-сложные (2 уровень)

28 Установите соответствие:

(1Б, 2В)

- | | |
|--|--|
| 1 Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой? | А) AS/NZS
Б) Анализ сбоев и дефектов
В) OECD |
| 2 Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом? | |

29 Укажите все верные варианты:

(1Б, 2В)

- | | |
|---|---|
| 1 Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод: | А) подстановки;
Б) перестановки;
В) гаммирования; |
| 2 Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод: | |

30 Установите соответствие:

(1В, 2Б)

- | | | |
|---|--|--|
| 1 | Защита информации от утечки это деятельность по предотвращению | А) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа; |
| 2 | Защита информации это | Б) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
В) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; |

31 Укажите все верные варианты:
(1Б, 2В)

- | | | |
|---|---|---|
| 1 | Естественные угрозы безопасности информации вызваны | А) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
Б) воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
В) деятельностью человека; |
| 2 | Искусственные угрозы безопасности информации вызваны: | |

32 Укажите все верные варианты:
(1В, 2А, 3Б)

- | | | |
|---|--|-----------------|
| 1 | Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п | А) фишинг; |
| 2 | Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей | Б) детектор |
| 3 | Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы | В) черный пиар; |

33 Укажите все верные варианты:
(1Б, 2А, 3В)

- | | | |
|---|---|--------------------------|
| 1 | Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние | А) ревизор;
Б) доктор |
| 2 | Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а | |

затем периодически или по команде пользователя сравнивает текущее состояние с исходным

- 3 Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов
- В) сторож;

34 Укажите все верные варианты:
(1А, 2Б)

- 1 Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
- А) конфиденциальность
- 2 Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано
- Б) надежность

Сложные (3 уровень)

35 Укажите все верные варианты:
(1А, 2В, 3Б)

- 1 Активный перехват информации это перехват, который
- А) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера
- 2 Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации
- Б) пассивный перехват;
- 3 Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций
- В) аудиоперехват;

Задания открытого типа

Задания на дополнение

Напишите пропущенное слово.

Простые (1 уровень)

36 Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы это ...**основные непреднамеренные искусственные угрозы, непреднамеренные искусственные угрозы**

37 Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п называется ... **черный пиар**

38 Перехват, который осуществляется путем использования оптической техники называется ... **видеоперехват**

39 Технический персонал, обслуживающий здание относится к ... нарушителям информационной безопасности. **внутренним**

40 Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это... **комплексное обеспечение ИБ, комплексное обеспечение**

41 Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются ... **черви**

42 Системы, обнаружения атаки на ОС; системы, обнаружения атаки на конкретные приложения; системы, обнаружения атаки на удаленных БД все вместе относятся к ... **видам системы обнаружения атак**

Средне-сложные (2 уровень)

43 Автоматизированная система должна обеспечивать... **доступность и целостность**

44 Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это **пароль пользователя**

45 К вирусам изменяющим среду обитания относятся **полиморфные**

46 Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это... **защита информации**

47 Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных это ... **Компьютерная безопасность**

48 Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это... **информационное оружие**

49 Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это ... **коммерческая тайна**

50 Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений ... **целостность**

51 Гарантия точного и полного выполнения команд в АС это ... **точность**

52 Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми – это принцип ... **разумной достаточности**

53 Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности это ... **политика безопасности**

54 Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется... **сканером, сканер**

55 Охранное освещение НЕ бывает:

дежурное

световое

тревожное.

Правильный ответ - **световое**

56 Что не относится к информационной инфекции:

Троянский конь

Фальсификация данных

Черви

Вирусы

Логическая бомба

Правильный ответ - **Фальсификация данных, Фальсификация**

57 Устройства, осуществляющие воздействие на человека путем передачи информации через вневещественное восприятие, называются ... **Средства специального программно-технического воздействия**

58 Идентификатор субъекта доступа, который является его секретом, это ... **пароль**

59 Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации это ... **защита от утечки информации**

60 Исследование возможности расшифрования информации без знания ключей называется ... **криптоанализ**

61 Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это ... **информационная безопасность**

62 Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это ... **информационная война**

63 К какому уровню доступа информации относится следующая информация: «Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия...» -... **Информация с ограниченным доступом**

64 Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов – это ... **Принцип системности**

65 Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте называется **Банковская тайна**

66 Реализация конституционных прав на доступ к информации относится к национальным интересам в ... сфере - ... **информационной**

Сложные (3 уровень)

67 Логические закладки («мины») – это основные типы средств воздействия на ...
компьютерную сеть, сеть

68 Секретность закрытого сообщения определяется секретностью ключа – это суть принципа ... **Кирхгофа**

69 Аудит, анализ уязвимостей, риск-ситуаций – это наиболее важные защитные меры при реализации политики ... **безопасности**

70 Проверка способности успешно противостоять угрозам - это...**аудит информационной безопасности**

является: - Аудит, анализ затрат на проведение защитных мер - Аудит, анализ безопасности +

Карта учета тестовых заданий

Компетенция	ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решения задач профессиональной деятельности;			
Дисциплина	Информационная безопасность			
Уровень освоения	Тестовые задания			Итого
	Закрытого типа		Открытого типа	
	Альтернативный выбор	Установление соответствия/ последовательности	На дополнение	
1.1.1 (20%)	5	2	7	14
1.1.2 (70%)	17	7	24	48
1.1.3 (10%)	3	1	4	8
Итого:	25 шт.	10 шт.	35 шт.	70 шт.

Критерии оценивания

Критерии оценивания тестовых заданий

Критерии оценивания: правильное выполнение одного тестового задания оценивается 1 условным баллом, неправильное – 0 баллов.

Максимальная общая сумма баллов за все правильные ответы составляет наивысший балл – 100 баллов.

Шкала оценивания результатов компьютерного тестирования обучающихся (рекомендуемая)

Оценка	Процент верных ответов	Баллы
«удовлетворительно»	70-79%	61-75 баллов
«хорошо»	80-90%	76-90 баллов
«отлично»	91-100%	91-100 баллов

Ключи ответов

№ задания	Номер и вариант правильного ответа
1	В
2	А
3	В
4	Б
5	Г
6	Б
7	А
8	Г
9	В
10	Б
11	Г
12	А
13	А
14	А
15	В
16	Б
17	Г
18	А
19	Б
20	В
21	В
22	Г
23	А
24	В
25	Г
26	1-В, 2-А
27	1-Б, 2-А
28	1-Б, 2-В
29	1-Б, 2-В
30	1-В, 2-Б
31	1-Б, 2-В
32	1В, 2А, 3Б
33	1Б, 2А, 3В
34	1А, 2Б
35	1А, 2В, 3Б

36	основные непреднамеренные искусственные угрозы, непреднамеренные искусственные угрозы, непреднамеренные угрозы
37	черный пиар
38	видеоперехват
39	внутренним
40	комплексное обеспечение ИБ, комплексное обеспечение
41	черви
42	видам системы обнаружения атак
43	доступность и целостность
44	пароль пользователя
45	полиморфные
46	защита информации
47	Компьютерная безопасность
48	информационное оружие
49	коммерческая тайна
50	целостность
51	точность
52	разумной достаточности
53	политика безопасности
54	сканером, сканер
55	световое
56	Фальсификация данных, Фальсификация
57	Средства специального программно-технического воздействия
58	пароль
59	защита от утечки информации
60	криптоанализ
61	информационная безопасность
62	информационная война
63	Информация с ограниченным доступом
64	Принцип системности
65	Банковская тайна
66	информационной
67	компьютерную сеть, сеть
68	Кирхгофа
69	безопасности
70	аудит информационной безопасности