МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
технологий обработки и защиты информации

А.А. Сирота

23.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.39 Основы информационной безопасности

1. Шифр и наименование направления подготовки/специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализации: Анализ безопасности компьютерных систем

3. Квалификация (степень) выпускника: специалист

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Мальцев Алексей Сергеевич, доцент, к.т.н.

7. Рекомендована:
Научно-методическим советом ФКН, протокол № 5 от 05.03.2024 г.

8. Учебный год: 2025-2026 **Семестр(ы):** 3

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:

- изучение основ и принципов организации и информационной безопасности в рамках комплексного обеспечения безопасности;
- получение профессиональных компетенций в области информационной безопасности.

Задачи учебной дисциплины:

- обучение студентов базовым основам обеспечения информационной безопасности государства;
- обучение студентов базовым методологиям создания систем защиты информации;

− обучение студентов базовым основам процесса сбора, передачи, накопления и обработки информации;

− обучение студентов основам методов и средств ведения информационных противоборств;

− обучение студентов базовым способам оценки защищенности и обеспечения информационной;

− обучение студентов базовым принципам обеспечения безопасности объектов информатизации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к блоку Б1 обязательных дисциплин общепрофессиональной части.

Входные знания в области нормативной и законодательной базы в области информационной безопасности, физики, распространения сигналов, теории вероятностей и математической статистики, информатики.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1	знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	**знать:** основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; **уметь:** проводить анализ средств, способов и принципов построения систем обеспечения информационной; **владеть:** практическими навыками выбора средств и способов обеспечения информационной безопасности в зависимости от условий и особенностей объекта защиты, навыками построения систем защиты информации.
		ОПК-1.2	знает классификацию защищаемой информации по видам тайны и степеням конфиденциальности;	**знать:** содержание основных классификаций защищаемой информации; **уметь:** проводить анализ защищаемой информации; **владеть:** практическими навыками классификации защищаемой информации.
		ОПК-1.3	знает классификацию и основные угрозы информационной безопасности для объекта информатизации;	**знать:** содержание классификаций и основных угроз информационной безопасности объекта информатизации **уметь:** проводить анализ угроз информационной безопасности объекта информатизации; **владеть:** практическими навыками выявления угроз информационной безопасности объекта информатизации.
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.1	знает источники и классификацию угроз информационной безопасности	**знать:** основные источники угроз безопасности информации; **уметь:** анализировать возможные источники угроз безопасности информации; **владеть:** практическими навыками классификации потенциально опасных угроз информационной безопасности.
		ОПК-5.2	знает место и роль информационной безопасности в системе национальной безопасности Российской Фе-	**знать:** место информационной безопасности в системе национальной безопасности страны; источники угроз информационной безопасности и меры по их предотвращению;

			дерации, основы государственной информационной политики;	**уметь**: определять основные угрозы национальной безопасности, связанные с информационной безопасностью; **владеть**: основами государственной информационной политики
		ОПК-5.3	умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	**знать:** содержание основных классификаций защищаемой информации; **уметь:** проводить анализ защищаемой информации; **владеть:** практическими навыками классификации защищаемой информации.
		ОПК-5.4	умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	**знать:** особенности классификации и оценки угроз информационной безопасности; **уметь:** применять основные принципы классификации и оценки угроз информационной безопасности; **владеть:** практическими навыками классификации и оценки угроз информационной безопасности

12. Объем дисциплины в зачетных единицах/час — 4/144.
Форма промежуточной аттестации: *зачет с оценкой*.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 3	№ семестра	Итого
Аудиторные занятия		68	68		68
в том числе:	лекции	34	34		34
	практические	34	34		34
	лабораторные	-	-		-
Самостоятельная работа		40	40		40
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – 36 час.)*		36	36		36
Итого:		144	144		144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.	Тема 1. Понятие, сущность и актуальность предмет и объект защиты информации. Основные определения и задачи информационной безопасности.	1. Понятие, сущность и актуальность предмет и объект защиты информации. 2. Основные определения и задачи информационной безопасности.	
2.	Тема 2. Государственная система защиты информации	1. Определение, структура и задачи Государственной системы защиты информации. 2. Цели защиты информации. 3. Органы защиты государственной тайны.	
3.	Тема 3.1. Общие положения законодательной и нормативно-правовой базы в области защиты информации	1. Законодательные акты РФ в сфере защиты информации. 2. Нормативные правовые акты РФ в сфере защиты информации.	
4.	Тема 3.2. Анализ методических документов и стандар-	1. Нормативно-методические документы в области защиты информации.	

	тов в области защиты информации		
5.	Тема 4.1. Виды угроз и нарушители информационной безопасности	1. Понятие угрозы безопасности информации. 2. Виды угроз безопасности информации. 3. Источники угроз безопасности информации. 4. Нарушители информационной безопасности.	
6.	Тема 4.2. Виды угроз и нарушители информационной безопасности	1. Виды и цели нарушителей. 2. Потенциал и возможности нарушителей. 3. Способы реализации угроз нарушителем.	
7.	Тема 5. Модель угроз безопасности информации	1. Назначение модели угроз безопасности информации. 2. Идентификация угроз безопасности информации и их источников. 3. Модель нарушителя. 4. Принцип оценки актуальности угроз. 5. Оценка возможности реализации угрозы. 6. Оценка степени ущерба. 7. Оценка актуальности угрозы.	
8.	Тема 6. Общее содержание методологических основ информационной безопасности	1. Модели, стратегии и системы обеспечения информационной безопасности. 2. Определение и структура научно-методологических основ информационной безопасности 3. Система принципов формирования теоретических основ комплексной защиты информации 4. Системный подход к управлению защитой информации. Системные принципы создания комплексной защиты информации.	
9.	Тема 7. Методы и технологии защиты информации. Антивирусная защита	1. Методы и технологии защиты информации. Классификация методов и средств защиты информации. 2. Антивирусная защита.	
10.	Тема 8. Системы идентификации и аутентификации. Системы разграничения доступа	1. Системы идентификации и аутентификации. 2. Системы разграничения доступа. Дискреционное и мандатное управление доступом.	
11.	Тема 9. Протоколирование и аудит. Стеганографические и криптографические методы защиты информации	1. Протоколирование и аудит. 2. Стеганографические методы защиты информации. 3. Криптографические методы защиты информации.	
12.	Тема 10. Экранирование	1. Основные понятия. 2. Архитектурные аспекты. 3. Классификация межсетевых экранов. 4. Анализ защищенности.	
13.	Тема 11. Обеспечение высокой доступности. Туннелирование и управление	1. Доступность 2. Туннелирование и управление	
14.	Тема 12. Лицензирование деятельности в области защиты информации	1. Лицензирование деятельности в области защиты государственной тайны	
15.	Тема 13. Аттестация объектов информатизации. Сертификация средств защиты информации	1. Общие вопросы аттестации объектов информатизации. 2. Система сертификации средств защиты информации.	
16.	Тема 14.1. Требования к организации защиты информации, содержащейся в информационной системе	1. Общие положения 2. Формирование требований к защите информации, содержащейся в информационной системе 3. Разработка системы защиты информации информационной системы 4. Внедрение системы защиты информации информационной системы	
17.	Тема 14.2. Аттестация, ввод в действие, обеспечение защиты информации в ходе эксплуатации и при выводе из эксплуатации информа-	1. Аттестация информационной системы и ввод ее в действие. 2. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы. 3. Обеспечение защиты информации при выводе из	

	ционной системы. Требования к мерам защиты информации, содержащейся в информационной системе	эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации. 4. Требования к мерам защиты информации, содержащейся в информационной системе. 5. Определение класса защищенности информационной системы.	
2. Практические занятия			
2.1	Методы и средства защиты информации	1. Функции непосредственной защиты информации. Механизмы защиты, управление механизмами защиты. 2. Методы защиты информации от преднамеренного доступа, методы защиты информации в вычислительных системах. 3. Методы идентификации и установления подлинности субъектов и различных объектов. 4. Технические, программные и организационно-правовые средства защиты информации. 5. Современные средства и способы обеспечения информационной безопасности.	
3. Лабораторные работы			
3.1	нет		

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Сам. работа	Промежуточная аттестация (экзамен)	Всего
1.	Тема 1. Понятие, сущность и актуальность предмет и объект защиты информации. Основные определения и задачи информационной безопасности.	2	2	2		6
2.	Тема 2. Государственная система защиты информации	2	2	2		6
3.	Тема 3.1. Общие положения законодательной и нормативно-правовой базы в области защиты информации	2	2	2		6
4.	Тема 3.2. Анализ методических документов и стандартов в области защиты информации	2	2	2		6
5.	Тема 4.1. Виды угроз и нарушители информационной безопасности	2	2	2		6
6.	Тема 4.2. Виды угроз и нарушители информационной безопасности	2	2	2		6
7.	Тема 5. Модель угроз безопасности информации	2	2	2		6
8.	Тема 6. Общее содержание методологических основ информационной безопасности	2	2	2		6
9.	Тема 7. Методы и технологии защиты информации. Антивирусная защита	2	2	2		6
10.	Тема 8. Системы идентификации и аутентификации. Системы разграничения доступа	2	2	2		6
11.	Тема 9. Протоколирование и аудит. Стеганографические и криптографические методы защиты информации	2	2	4		8

12.	Тема 10. Экранирование	2	2	2		6
13.	Тема 11. Обеспечение высокой доступности. Туннелирование и управление	2	2	2		6
14.	Тема 12. Лицензирование деятельности в области защиты информации	2	2	2		6
15.	Тема 13. Аттестация объектов информатизации. Сертификация средств защиты информации	2	2	2		6
16.	Тема 14.1. Требования к организации защиты информации, содержащейся в информационной системе	2	2	4		8
17.	Тема 14.2. Аттестация, ввод в действие, обеспечение защиты информации в ходе эксплуатации и при выводе из эксплуатации информационной системы. Требования к мерам защиты информации, содержащейся в информационной системе	2	2	4		8
18.	Экзамен				36	36
	Итого:	34	34	40	36	144

14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка знаний основ информационной безопасности.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов

	высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122>.

б) дополнительная литература:

№ п/п	Источник
1	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет) *:

№ п/п	Ресурс
1	*ЭБС Лань – Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024)*
2	*ЭБС «Университетская библиотека online» – Контракт №3010-06/23-22 от 30.12.2022*
3	*ЭБС «Консультант студента» – Лицензионный договор №3010-06/22-22 от 30.12.2022 (с дополнительным соглашение №1 от 09.01.2023) (срок предоставления с 12.01.2023 по 11.01.2024)*

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

№ п/п	Источник
1	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используются:

1. ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024),

2. ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024),

3. ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025),

4. Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027),

5. ЭБС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025).

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

1) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры).

2) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6'' FHD Lenovo V155-15API

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

3) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380

Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17'', мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

4) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 290

Учебная аудитория: специализированная мебель, персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27'' (12 шт.), мультимедийный проектор, экран.

Лабораторное оборудование искусственного интеллекта: рабочие места – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); модули АО НПЦ «ЭЛВИС»: процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эмулятор MC-USB-JTAG (9 шт.).

Лабораторное оборудование электроники, электротехники и схемотехники: рабочие ме-ста – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); стенд для практических занятий по электрическим цепям (KL-100); стенд для изучения аналоговых электрических схем (KL-200); стенд для изучения цифровых схем (KL-300).

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Тема 1. Понятие, сущность и актуальность предмет и объект защиты информации. Основные определения и задачи информационной безопасности.	ОПК-1	ОПК-1.1	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
2.	Тема 2. Государственная система защиты информации	ОПК-5	ОПК-5.2	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
3.	Тема 3.1. Общие положения законодательной и нормативно-правовой базы в области защиты информации	ОПК-1 ОПК-5	ОПК-1.2 ОПК-5.2	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 3.2. Анализ методических документов и стандартов в области защиты информации	ОПК-5	ОПК-5.2	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 4.1. Виды угроз и нарушители информационной безопасности	ОПК-1 ОПК-5	ОПК-1.3 ОПК-5.1 ОПК-5.4	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 4.2. Виды угроз и нарушители информационной безопасности	ОПК-1 ОПК-5	ОПК-1.3 ОПК-5.1 ОПК-5.4	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 5. Модель угроз безопасности информа-	ОПК-1 ОПК-5	ОПК-1.3 ОПК-5.1	Письменная работа либо тестирование в электронной образовательной среде на

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	ции		ОПК-5.4	проверку знаний
	Тема 6. Общее содержание методологических основ информационной безопасности	ОПК-1 ОПК-5	ОПК-1.1 ОПК-1.2 ОПК-5.2 ОПК-5.3	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 7. Методы и технологии защиты информации. Антивирусная защита	ОПК-1	ОПК-1.1	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 8. Системы идентификации и аутентификации. Системы разграничения доступа	ОПК-1	ОПК-1.1	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 9. Протоколирование и аудит. Стеганографические и криптографические методы защиты информации	ОПК-1	ОПК-1.1	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 10. Экранирование	ОПК-1	ОПК-1.1	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 11. Обеспечение высокой доступности. Туннелирование и управление	ОПК-1	ОПК-1.1	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 12. Лицензирование деятельности в области защиты информации	ОПК-1 ОПК-5	ОПК-1.2 ОПК-5.2 ОПК-5.3	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 13. Аттестация объектов информатизации. Сертификация средств защиты информации	ОПК-1 ОПК-5	ОПК-1.2 ОПК-5.2 ОПК-5.3	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 14.1. Требования к организации защиты информации, содержащейся в информационной системе	ОПК-1 ОПК-5	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-5.4	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
	Тема 14.2. Аттестация, ввод в действие, обеспечение защиты информации в ходе эксплуатации и при выводе из эксплуатации информационной системы. Требования к мерам защиты информации, содержащейся в информационной системе	ОПК-1 ОПК-5	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-5.4	Письменная работа либо тестирование в электронной образовательной среде на проверку знаний
Промежуточная аттестация форма контроля – экзамен				

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью письменной работы на проверку знаний по разделам дисциплины (модулям).

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей аттестаций. На аттестации используется контрольно-измерительный материал, включающий в себя два-три вопроса.

Оценивание уровня сформированности компетенций осуществляется по содержанию вопросов, приведенных в таблице.

№	Содержание
1.	Защита информации – это…
2.	Защита информации от утечки – это …
3.	Несанкционированное воздействие на информацию – это …
4.	Безопасность информации – это…
5.	Составляющие информационной безопасности
6.	Предмет и объект защиты информации
7.	Данные – это …
8.	Материальный носитель – это …
9.	Сообщение – это …
10.	Канал связи – это …
11.	Сведения – это …
12.	Особенности информации
13.	Информационная безопасность системы – это
14.	Общая структурная схема ИБ
15.	Основные направления защиты от информационных воздействий.
16.	Сущность состояния защищенности основных интересов личности заключается…
17.	Общая схема обеспечения информационной безопасности.
18.	Под безопасностью автоматизированной информационной системы (ИС) понимается.
19.	Конфиденциальность информации – это …
20.	Целостность программного компонента (или информационного ресурса) системы.
21.	Доступность программного компонента или информационного ресурса системы.
22.	Аутентичность – это …
23.	Апеллируемость (неотрекаемость) – это …
24.	Понятие государственной системы защиты информации.
25.	Структура государственной системы защиты информации.
26.	Состав государственной системы защиты информации.
27.	Основные направления защиты информации.
28.	Основные задачи государственной системы защиты информации.
29.	Основные задачи государственной системы защиты информации.
30.	Частные Нарушение требований по защите информации.цели защиты информации.
31.	Задачи защиты информации.
32.	Какие категории защищенности применяются в отношении программно-технических компонент информационных систем?
33.	Субъекты, требующие различные уровни защиты информационных активов.
34.	Структура системы обеспечения информационной безопасности организации.
35.	Федеральные законы в области защиты информации («Об информации, информационных технологиях и о защите информации», «О государственной тайне», «О персональных данных» «О коммерческой тайне» «О лицензировании отдельных видов деятельности» «Об обеспечении единства измерений» «О стандартизации в Российской Федерации» «О безопасности критической информационной инфраструктуры РФ»), краткая аннотация.
36.	Нормативные правовые акты (Указы) Президента РФ (Доктрина информационной безопасности РФ, Об утверждении перечня сведений, отнесенных к государственной тайне, Вопросы Федеральной службы по техническому и экспортному контролю, Вопросы Федеральной службы безопасности, Вопросы Межведомственной комиссии по защите государственной тайны, О мерах по обеспечению ИБ РФ при использовании информационно-телекоммуникационных сетей международного обмена), краткая аннотация.
37.	Под угрозой безопасности информации понимается …
38.	Источником угрозы безопасности информации является …
39.	Уязвимость информационной системы.

40.	Факторы, воздействующего на защищаемую информацию.
41.	Несанкционированный доступ к информации – это …
42.	Виды угроз безопасности информации.
43.	Источники угроз безопасности информации .
44.	Нарушители безопасности информации.
45.	Виды и цели нарушителей.
46.	Потенциал и возможности нарушителей.
47.	Способы реализации угроз нарушителем.
48.	Назначение модели угроз безопасности информации.
49.	Идентификация угроз безопасности информации и их источников.
50.	Модель нарушителя.
51.	Принцип оценки актуальности угроз.
52.	Оценка возможности реализации угрозы.
53.	Оценка степени ущерба.
54.	Оценка актуальности угрозы.
55.	Модели, стратегии и системы обеспечения информационной безопасности.
56.	Определение и структура научно-методологических основ информационной безопасности.
57.	Система принципов формирования теоретических основ комплексной защиты информации
58.	Системный подход к управлению защитой информации.
59.	Системные принципы создания комплексной защиты информации.
60.	К организационным (административным) методам защиты информации относятся.
61.	К технологическими методам и средствам защиты относится.
62.	Криптографические методы – это …
63.	Правовые методы защиты.
64.	Типовые методы защиты информации.
65.	Политика безопасности – это …
66.	Вирусная угроза, компьютерный вирус.
67.	Фазы существования вируса, классификация компьютерных вирусов по среде обитания.
68.	Типы компьютерных вирусов по особенностям алгоритма и реализации.
69.	Классификация вирусов по деструктивным возможностям, классификация вирусов по способу заражения.
70.	Основные классы вредоносных программ по характеру воздействия на компьютерную систему.
71.	Признаки вирусного заражения.
72.	Защита от вирусной угрозы.
73.	Виды антивирусных программ (краткая характеристика).
74.	Идентификация – это …
75.	Аутентификация – это …
76.	Под безопасностью (стойкостью) системы идентификации и аутентификации понимается …
77.	Разновидности аутентификации. Группы методов аутентификации основаны на …
78.	Показатели точности биометрической системы аутентификации характеризуется…
79.	Парольная система – это…, идентификатор пользователя – это…, пароль пользователя – это …, учетная запись пользователя – …, база данных пользователей – это …
80.	Методы взлома парольных систем и получения значения пароля.
81.	Системы разграничения доступа.
82.	Дискреционное и мандатное управление доступом.
83.	Протоколирование.
84.	Аудит.
85.	Стеганографические методы защиты информации.
86.	Криптографические методы защиты информации (общие сведения).
87.	Криптографические методы защиты информации (методы шифрования).
88.	Криптографические методы защиты информации (контроль целостности).
89.	Цифровые сертификаты.
90.	Экранирование (основные понятия).
91.	Экранирование (архитектурные аспекты).
92.	Экранирование (классификация межсетевых экранов).
93.	Экранирование (анализ защищенности).
94.	Доступность (общие сведения: эффективность услуг, время недоступности, высокая доступность, отказ).
95.	Основы мер обеспечения высокой доступности.
96.	Отказоустойчивость и зона риска.
97.	Обеспечение отказоустойчивости.
98.	Программное обеспечение промежуточного слоя.
99.	Обеспечение обслуживаемости.

100.	Туннелирование.
101.	Управление (основные понятия).
102.	Управление (возможности типичных систем).
103.	Перечень методических документов и стандартов в области защиты информации.
104.	Классы автоматизированных систем.
105.	Лицензирование деятельности в области защиты государственной тайны (общие сведения).
106.	Нормативные документы, определяющие порядок лицензирования.
107.	Лицензируемые виды деятельности, отнесенные к компетенции ФСТЭК России.
108.	Общие требования к соискателям лицензии. Срок действия лицензии.
109.	Заявительные документы для получения лицензии.
110.	Требования к органу по аттестации.
111.	Аттестация объекта информатизации. Общие сведения (определение, виды, что проверяется в ходе аттестации)
112.	Дать понятие сертификации, сертификата соответствия, сертификации СЗИ.
113.	Порядок сертификации СЗИ.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, практические работы). При оценивании используется количественная шкала.

Критерии оценивания приведены таблице.

Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

20.2. Промежуточная аттестация

Контроль успеваемости по дисциплине осуществляется с помощью контрольной работы на проверку знаний по дисциплине и собеседования по ее результатам.

Для оценивания результатов обучения на зачете с оценкой используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование и представление основных теоретических и практических результатов (теорем, алгоритмов, методик) с использованием математических вы-

кладок, блок-схем, структурных схем и стандартных описаний к ним;

3) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и экспериментирования с компьютерными моделями алгоритмов обработки информации в среде Matlab в рамках выполняемых практических заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций):

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на зачете с оценкой используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

В ходе промежуточной аттестации используется контрольно-измерительный материал, включающий в себя два-три вопроса.

Оценивание уровня сформированности компетенций осуществляется по содержанию вопросов, приведенных в таблице.

№	Содержание
1.	Защита информации – это…
2.	Защита информации от утечки – это …
3.	Несанкционированное воздействие на информацию – это …
4.	Безопасность информации – это…
5.	Составляющие информационной безопасности
6.	Предмет и объект защиты информации
7.	Данные – это …
8.	Материальный носитель – это …
9.	Сообщение – это …
10.	Канал связи – это …
11.	Сведения – это …
12.	Особенности информации
13.	Информационная безопасность системы – это
14.	Общая структурная схема ИБ
15.	Основные направления защиты от информационных воздействий.
16.	Сущность состояния защищенности основных интересов личности заключается…
17.	Общая схема обеспечения информационной безопасности.
18.	Под безопасностью автоматизированной информационной системы (ИС) понимается.
19.	Конфиденциальность информации – это …
20.	Целостность программного компонента (или информационного ресурса) системы.
21.	Доступность программного компонента или информационного ресурса системы.
22.	Аутентичность – это …
23.	Апеллируемость (неотрекаемость) – это …
24.	Понятие государственной системы защиты информации.
25.	Структура государственной системы защиты информации.
26.	Состав государственной системы защиты информации.
27.	Основные направления защиты информации.
28.	Основные задачи государственной системы защиты информации.
29.	Основные задачи государственной системы защиты информации.
30.	Частные Нарушение требований по защите информации.цели защиты информации.
31.	Задачи защиты информации.
32.	Какие категории защищенности применяются в отношении программно-технических компонент информационных систем?
33.	Субъекты, требующие различные уровни защиты информационных активов.

34.	Структура системы обеспечения информационной безопасности организации.
35.	Федеральные законы в области защиты информации («Об информации, информационных технологиях и о защите информации», «О государственной тайне», «О персональных данных» «О коммерческой тайне» «О лицензировании отдельных видов деятельности» «Об обеспечении единства измерений» «О стандартизации в Российской Федерации» «О безопасности критической информационной инфраструктуры РФ»), краткая аннотация.
36.	Нормативные правовые акты (Указы) Президента РФ (Доктрина информационной безопасности РФ, Об утверждении перечня сведений, отнесенных к государственной тайне, Вопросы Федеральной службы по техническому и экспортному контролю, Вопросы Федеральной службы безопасности, Вопросы Межведомственной комиссии по защите государственной тайны, О мерах по обеспечению ИБ РФ при использовании информационно-телекоммуникационных сетей международного обмена), краткая аннотация.
37.	Под угрозой безопасности информации понимается …
38.	Источником угрозы безопасности информации является …
39.	Уязвимость информационной системы.
40.	Факторы, воздействующего на защищаемую информацию.
41.	Несанкционированный доступ к информации – это …
42.	Виды угроз безопасности информации.
43.	Источники угроз безопасности информации.
44.	Нарушители безопасности информации.
45.	Виды и цели нарушителей.
46.	Потенциал и возможности нарушителей.
47.	Способы реализации угроз нарушителем.
48.	Назначение модели угроз безопасности информации.
49.	Идентификация угроз безопасности информации и их источников.
50.	Модель нарушителя.
51.	Принцип оценки актуальности угроз.
52.	Оценка возможности реализации угрозы.
53.	Оценка степени ущерба.
54.	Оценка актуальности угрозы.
55.	Модели, стратегии и системы обеспечения информационной безопасности.
56.	Определение и структура научно-методологических основ информационной безопасности.
57.	Система принципов формирования теоретических основ комплексной защиты информации
58.	Системный подход к управлению защитой информации.
59.	Системные принципы создания комплексной защиты информации.
60.	К организационным (административным) методам защиты информации относятся.
61.	К технологическими методам и средствам защиты относится.
62.	Криптографические методы – это …
63.	Правовые методы защиты.
64.	Типовые методы защиты информации.
65.	Политика безопасности – это …
66.	Вирусная угроза, компьютерный вирус.
67.	Фазы существования вируса, классификация компьютерных вирусов по среде обитания.
68.	Типы компьютерных вирусов по особенностям алгоритма и реализации.
69.	Классификация вирусов по деструктивным возможностям, классификация вирусов по способу заражения.
70.	Основные классы вредоносных программ по характеру воздействия на компьютерную систему.
71.	Признаки вирусного заражения.
72.	Защита от вирусной угрозы.
73.	Виды антивирусных программ (краткая характеристика).
74.	Идентификация – это …
75.	Аутентификация – это …
76.	Под безопасностью (стойкостью) системы идентификации и аутентификации понимается …
77.	Разновидности аутентификации. Группы методов аутентификации основаны на …
78.	Показатели точности биометрической системы аутентификации характеризуется…
79.	Парольная система – это…, идентификатор пользователя – это…, пароль пользователя – это …, учетная запись пользователя – …, база данных пользователей – это …
80.	Методы взлома парольных систем и получения значения пароля.
81.	Системы разграничения доступа.
82.	Дискреционное и мандатное управление доступом.
83.	Протоколирование.
84.	Аудит.
85.	Стеганографические методы защиты информации.

86.	Криптографические методы защиты информации (общие сведения).
87.	Криптографические методы защиты информации (методы шифрования).
88.	Криптографические методы защиты информации (контроль целостности).
89.	Цифровые сертификаты.
90.	Экранирование (основные понятия).
91.	Экранирование (архитектурные аспекты).
92.	Экранирование (классификация межсетевых экранов).
93.	Экранирование (анализ защищенности).
94.	Доступность (общие сведения: эффективность услуг, время недоступности, высокая доступность, отказ).
95.	Основы мер обеспечения высокой доступности.
96.	Отказоустойчивость и зона риска.
97.	Обеспечение отказоустойчивости.
98.	Программное обеспечение промежуточного слоя.
99.	Обеспечение обслуживаемости.
100.	Туннелирование.
101.	Управление (основные понятия).
102.	Управление (возможности типичных систем).
103.	Перечень методических документов и стандартов в области защиты информации.
104.	Классы автоматизированных систем.
105.	Лицензирование деятельности в области защиты государственной тайны (общие сведения).
106.	Нормативные документы, определяющие порядок лицензирования.
107.	Лицензируемые виды деятельности, отнесенные к компетенции ФСТЭК России.
108.	Общие требования к соискателям лицензии. Срок действия лицензии.
109.	Заявительные документы для получения лицензии.
110.	Требования к органу по аттестации.
111.	Аттестация объекта информатизации. Общие сведения (определение, виды, что проверяется в ходе аттестации)
112.	Дать понятие сертификации, сертификата соответствия, сертификации СЗИ.
113.	Порядок сертификации СЗИ.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете с оценкой представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2024

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.О.39 Основы информационной безопасности

Форма обучения Очное

Вид контроля Зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Понятие, сущность и актуальность предмет и объект защиты информации.
2. Основные определения и задачи информационной безопасности.

Преподаватель _____ А.С. Мальцев

Тестовые задания

1

Что такое защита информации?			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства		*0*
B.	Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность		*0*
C.	Деятельность, направленная на предотвращение НСД к информации		*0*
D.	Деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию		*100*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

2

Замысел защиты информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации		*100*
B.	деятельность по обеспечению защиты информации не криптографическими методами от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию		*0*
C.	совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация		*0*
D.	реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

3

Технический канал утечки информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	совокупность объекта разведки, средства разведки, среды распространения сигнала		*100*
B.	возможность доступа к информации с нарушением правил разграничения доступа		*0*
C.	совокупность ресурсов автоматизированной системы и человека		*0*
D.	возможность доступа к информации с помощью штатных средств автоматизированной системы		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

4

Несанкционированный доступ (НСД) к информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)		*100*
B.	доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств		*0*
C.	копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа		*0*
D.	совокупность объекта разведки, средства разведки, среды распространения сигнала		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

5

Безопасность информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)		*0*
B.	состояние защищенности информации (данных) при котором обеспечивается ее (их) конфиденциальность, доступность и целостность		*100*
C.	реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность		*0*
D.	деятельность, направленная на предотвращение НСД к информации		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

6

Техническая защита информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств		*100*
B.	защита информации с помощью ее криптографического преобразования		*0*
C.	защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты		*0*
D.	защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

7

Физическая защита информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств		*0*
B.	защита информации с помощью ее криптографического преобразования		*0*
C.	защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты		*100*
D.	защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

8

Правовая защита информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств		*0*
B.	защита информации с помощью ее криптографического преобразования		*0*
C.	защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты		*0*
D.	защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением		*100*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

9

Криптографическая защита информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств		*0*
B.	защита информации с помощью ее криптографического преобразования		*100*
C.	защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты		*0*
D.	защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением		*0*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

10

Способ защиты информации – это:			*MC*
		Балл по умолчанию:	1
		Случайный порядок ответов	Нет
		Нумеровать варианты ответов?	0
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
#	**Ответы**	**Отзыв**	**Оценка**
A.	основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации		*0*
B.	заранее намеченный результат защиты информации		*0*
C.	совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации		*0*
D.	порядок и правила применения определенных принципов и средств защиты информации		*100*
	Общий отзыв к вопросу:		
	Для любого правильного ответа:	Ваш ответ верный.	
	Для любого неправильного ответа:	Ваш ответ неправильный.	
	Подсказка 1:		
	Показать количество правильных ответов (Подсказка 1):	Нет	
	Удалить некорректные ответы (Подсказка 1):	Нет	
	Теги:		
Позволяет выбирать один или несколько правильных ответов из заданного списка. (MC/MA)			

Задания с коротким ответом

11

Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ – это…?			*SA*
		Балл по умолчанию:	2
		Чувствительность к регистру:	Нет
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
	Ответы	**Отзыв**	**Оценка**
	лицензирование		*100*
	Общий отзыв к вопросу:		
	Подсказка 1:		
	Теги:		
Вам необходимо указать хотя бы один возможный ответ. Пустые ответы не будут использоваться. Символ «» можно использовать в качестве шаблона, соответствующего любым символам. Первый подходящий ответ будет использоваться для определения оценки и отзыва.*			

12

Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ – это…?			*SA*
		Балл по умолчанию:	2
		Чувствительность к регистру:	Нет
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
	Ответы	**Отзыв**	**Оценка**
	лицензирование		*100*
	Общий отзыв к вопросу:		
	Подсказка 1:		
	Теги:		
Вам необходимо указать хотя бы один возможный ответ. Пустые ответы не будут использоваться. Символ «» можно использовать в качестве шаблона, соответствующего любым символам. Первый подходящий ответ будет использоваться для определения оценки и отзыва.*			

13

Форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров – это…? (к объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации)			*SA*
		Балл по умолчанию:	2
		Чувствительность к регистру:	Нет
		Штраф за каждую неправильную попытку:	100
		ID-номер:	
	Ответы	**Отзыв**	**Оценка**
	сертификация		*100*
	Общий отзыв к вопросу:		
	Подсказка 1:		
	Теги:		
Вам необходимо указать хотя бы один возможный ответ. Пустые ответы не будут использоваться. Символ «» можно использовать в качестве шаблона, соответствующего любым символам. Первый подходящий ответ будет использоваться для определения оценки и отзыва.*			

Задания с развернутым ответом

14

<table>
<tr><td colspan="3">Охарактеризуйте термины «защита информации», «безопасность информации» и их взаимосвязь</td><td>ES</td></tr>
<tr><td colspan="3" align="right">Балл по умолчанию:</td><td>3</td></tr>
<tr><td colspan="3" align="right">Формат ответа:</td><td>HTML-редактор</td></tr>
<tr><td colspan="3" align="right">Требовать текст:</td><td>Да</td></tr>
<tr><td colspan="3" align="right">Размер поля:</td><td>15</td></tr>
<tr><td colspan="3" align="right">Разрешить вложения:</td><td>0</td></tr>
<tr><td colspan="3" align="right">Требуемое число вложений:</td><td>0</td></tr>
<tr><td colspan="3" align="right">Разрешенные типы файлов:</td><td></td></tr>
<tr><td colspan="3" align="right">ID-номер:</td><td></td></tr>
<tr><td></td><td>Шаблон ответа</td><td>Информация для оценивающих</td><td></td></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Критерии оценивания</td><td>Шкала оценок</td></tr>
<tr><td>Обучающийся приводит полное и безошибочное определение терминов, умеет объяснить их взаимосвязь.</td><td>Отлично (90-100 баллов)</td></tr>
<tr><td>Обучающийся приводит полное и безошибочное определение терминов, не умеет объяснить их взаимосвязь.</td><td>Хорошо (70-80 баллов)</td></tr>
<tr><td>Обучающийся приводит неполное определение терминов, не умеет объяснить их взаимосвязь.</td><td>Удовлетворительно (50-70 баллов)</td></tr>
<tr><td>Обучающийся не приводит определение терминов, не умеет объяснить их взаимосвязь.</td><td>Неудовлетворительно (менее 50 баллов)</td></tr>
</table>
</td><td></td></tr>
<tr><td></td><td>Общий отзыв к вопросу:</td><td></td><td></td></tr>
<tr><td></td><td>Теги:</td><td></td><td></td></tr>
<tr><td colspan="3">Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.</td><td></td></tr>
</table>

15

<table>
<tr><td colspan="3">Охарактеризуйте термины «несанкционированный доступ к информации», «технический канал утечки информации» и определите их принципиальное различие</td><td>ES</td></tr>
<tr><td colspan="3" align="right">Балл по умолчанию:</td><td>3</td></tr>
<tr><td colspan="3" align="right">Формат ответа:</td><td>HTML-редактор</td></tr>
<tr><td colspan="3" align="right">Требовать текст:</td><td>Да</td></tr>
<tr><td colspan="3" align="right">Размер поля:</td><td>15</td></tr>
<tr><td colspan="3" align="right">Разрешить вложения:</td><td>0</td></tr>
<tr><td colspan="3" align="right">Требуемое число вложений:</td><td>0</td></tr>
<tr><td colspan="3" align="right">Разрешенные типы файлов:</td><td></td></tr>
<tr><td colspan="3" align="right">ID-номер:</td><td></td></tr>
<tr><td></td><td>Шаблон ответа</td><td>Информация для оценивающих</td><td></td></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Критерии оценивания</td><td>Шкала оценок</td></tr>
<tr><td>Обучающийся приводит полное и безошибочное определение терминов, умеет объяснить их различие.</td><td>Отлично (90-100 баллов)</td></tr>
<tr><td>Обучающийся приводит полное и безошибочное определение терминов, не умеет объяснить их различие.</td><td>Хорошо (70-80 баллов)</td></tr>
<tr><td>Обучающийся приводит неполное определение терминов, не умеет объяснить их различие.</td><td>Удовлетворительно (50-70 баллов)</td></tr>
<tr><td>Обучающийся не приводит определение терминов, не умеет объяснить их различие.</td><td>Неудовлетворительно (менее 50 баллов)</td></tr>
</table>
</td><td></td></tr>
<tr><td></td><td>Общий отзыв к вопросу:</td><td></td><td></td></tr>
<tr><td></td><td>Теги:</td><td></td><td></td></tr>
<tr><td colspan="3">Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.</td><td></td></tr>
</table>

16

<table>
<tr><td colspan="3">Раскройте суть физической защиты информации, приведите примеры ее реализации</td><td>ES</td></tr>
<tr><td colspan="3" align="right">Балл по умолчанию:</td><td>3</td></tr>
<tr><td colspan="3" align="right">Формат ответа:</td><td>HTML-редактор</td></tr>
<tr><td colspan="3" align="right">Требовать текст:</td><td>Да</td></tr>
<tr><td colspan="3" align="right">Размер поля:</td><td>15</td></tr>
<tr><td colspan="3" align="right">Разрешить вложения:</td><td>0</td></tr>
<tr><td colspan="3" align="right">Требуемое число вложений:</td><td>0</td></tr>
<tr><td colspan="3" align="right">Разрешенные типы файлов:</td><td></td></tr>
<tr><td colspan="3" align="right">ID-номер:</td><td></td></tr>
<tr><td></td><td>Шаблон ответа</td><td>Информация для оценивающих</td><td></td></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Критерии оценивания</td><td>Шкала оценок</td></tr>
<tr><td>Обучающийся раскрывает суть термина, приводит не менее трех примеров.</td><td>Отлично (90-100 баллов)</td></tr>
<tr><td>Обучающийся раскрывает суть термина, приводит менее трех примеров.</td><td>Хорошо (70-80 баллов)</td></tr>
<tr><td>Обучающийся раскрывает суть термина, не приводит примеров.</td><td>Удовлетворительно (50-70 баллов)</td></tr>
<tr><td>Обучающийся не раскрывает суть термина, не приводит примеров.</td><td>Неудовлетворительно (менее 50 баллов)</td></tr>
</table>
</td><td></td></tr>
<tr><td></td><td>Общий отзыв к вопросу:</td><td></td><td></td></tr>
<tr><td></td><td>Теги:</td><td></td><td></td></tr>
<tr><td colspan="3">Допускает в ответе загрузить файл и/или ввести текст. Ответ должен быть оценен преподавателем вручную.</td><td></td></tr>
</table>