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

УТВЕРЖДАЮ

Заведующий кафедрой
ТО и ЗИ


А.А. Сирота

03.05.2023г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.39 Основы информационной безопасности

1. Шифр и наименование направления подготовки/специальности:
10.03.01 Информационная безопасность

2. Профиль подготовки/специализации: безопасность компьютерных систем

3. Квалификация (степень) выпускника: бакалавр

4. Форма образования: очная

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

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

7. Рекомендована:
Научно-методическим советом ФКН, протокол № 7 от 03.05.2023 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2024-2025 **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 понятия информации и информационной безопасности;	**знать:** сущность и понятие информационной безопасности, характеристику ее составляющих; **уметь:** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; **владеть:** навыками определения основных угроз безопасности информации.
		ОПК-1.2	знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики;	**знать:** место информационной безопасности в системе национальной безопасности страны; источники угроз информационной безопасности и меры по их предотвращению; **уметь**: определять основные угрозы национальной безопасности, связанные с информационной безопасностью; **владеть**: основами государственной информационной политики
		ОПК-1.3	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-1.4	умеет классифицировать и оценивать угрозы информационной безопасности.	**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 — 3/108.
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		54	54		54
в том числе:	лекции	18	18		18
	практические	36	36		36
	лабораторные	-	-		-
Самостоятельная работа		54	54		54
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*		-	-		-
Итого:		108	108		108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Общие проблемы безопасности. Роль и место информационном безопасности	1. Предметная область информационной безопасности. Исторические сведения и этапы развития проблем и технологий обеспечения информационной безопасности. 2. Математические основы обеспечения информационной безопасности.	
1.2	Методы и средства защиты информации	3. Функции непосредственной защиты информации. Механизмы защиты, управление механизмами защиты. 4. Методы защиты информации от преднамеренного доступа, методы защиты информации в вычислительных системах. 5. Методы идентификации и установления подлинности субъектов и различных объектов. 6. Технические, программные и организационно-правовые средства защиты информации. 7. Современные средства и способы обеспечения информационной безопасности.	
1.3	Перспективы развития информационной безопасности	8. Методы и средства развития информационной безопасности и методов и средств ведения информационных противоборств	
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	Всего
1	Общие проблемы безопасности. Роль и место информационном безопасности	6	12	18	36
2	Методы и средства защиты информации	6	12	18	36
3	Перспективы развития информационной безопасности	6	12	18	36
	Итого:	18	36	54	108

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 он-лайн и проведения лабораторно- 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 (срок предоставления с 12.01.2023 по 11.01.2024)*
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) ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.

2) ОС Windows v.7, 8, 10; LibreOffice v.5-7; Foxit PDF Reader; MATLAB “Total Academic Headcount – 25”; Windows Server v. 2008-2019

3) LibreOffice v.5-7.

4) Foxit PDF Reader.

5) При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

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 ви-деоконференций 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 – персональ-ные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); модули АО НПЦ «ЭЛ-ВИС»: процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эму-лятор 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 анало-говых 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.	Общие проблемы безопасности. роль и место информационном безопасности	ОПК-1	ОПК-1.1	Письменная работа на проверку знаний понятия информации и информационной безопасности
2.	Методы и средства защиты информации		ОПК-1.2 ОПК-1.3	Письменная работа на проверку знаний места и роли информационной безопасности в системе национальной безопасности Российской Федерации, основ государственной информационной политики
3.	Перспективы развития информационной безопасности		ОПК-1.4	Письменная работа на проверку: знаний источников и классификации угроз информационной безопасности; умений классифицировать и оценивать угрозы информационной безопасности
Промежуточная аттестация форма контроля – Контрольная работа				

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	Виды национальной безопасности и их краткая характеристика
2	Средства обеспечения информационной безопасности
3	Системные связи информационной безопасности с другими видами национальной безопасности
4	Аппаратные средства обеспечения информационной безопасности
5	Информационные уязвимости объектов
6	Программные средства обеспечения информационной безопасности
7	Антропогенные информационные уязвимости
8	Криптографические средства обеспечения информационной безопасности
9	Техногенные информационные уязвимости
10	Стеганографические средства обеспечения информационной безопасности
11	Организационно-правовые информационные уязвимости
12	Организационно-правовые средства обеспечения информационной безопасности
13	Комбинированные информационные уязвимости
14	Государственная политика в области информационной безопасности
15	Угрозы информационной безопасности и их источники
16	Государственные органы обеспечения информационной безопасности
17	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация
18	Приоритетные направления обеспечения информационной безопасности в условиях информационного общества
19	Эндогенные и экзогенные, угрозы информационной безопасности, их классификация
20	Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества
21	Антропогенные и техногенные угрозы информационной безопасности, их классификация
22	Технические каналы утечки конфиденциальной информации. Основные методы защиты
23	Системная классификация угроз информационной безопасности
24	Пассивные средства противодействия техническим разведкам
25	Угрозы конфиденциальности, целостности и доступности информации
26	Активные средства противодействия техническим разведкам
27	Информационная война как высшая форма угрозы информационной безопасности
28	Базовые стратегии организации защиты информации
29	Категорирование информации
30	Полное множество функций защиты информации

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 выкладок, 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	Виды национальной безопасности и их краткая характеристика

2	Средства обеспечения информационной безопасности
3	Системные связи информационной безопасности с другими видами национальной безопасности
4	Аппаратные средства обеспечения информационной безопасности
5	Информационные уязвимости объектов
6	Программные средства обеспечения информационной безопасности
7	Антропогенные информационные уязвимости
8	Криптографические средства обеспечения информационной безопасности
9	Техногенные информационные уязвимости
10	Стеганографические средства обеспечения информационной безопасности
11	Организационно-правовые информационные уязвимости
12	Организационно-правовые средства обеспечения информационной безопасности
13	Комбинированные информационные уязвимости
14	Государственная политика в области информационной безопасности
15	Угрозы информационной безопасности и их источники
16	Государственные органы обеспечения информационной безопасности
17	Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация
18	Приоритетные направления обеспечения информационной безопасности в условиях информационного общества
19	Эндогенные и экзогенные, угрозы информационной безопасности, их классификация
20	Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества
21	Антропогенные и техногенные угрозы информационной безопасности, их классификация
22	Технические каналы утечки конфиденциальной информации. Основные методы защиты
23	Системная классификация угроз информационной безопасности
24	Пассивные средства противодействия техническим разведкам
25	Угрозы конфиденциальности, целостности и доступности информации
26	Активные средства противодействия техническим разведкам
27	Информационная война как высшая форма угрозы информационной безопасности
28	Базовые стратегии организации защиты информации
29	Категорирование информации
30	Полное множество функций защиты информации

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. Обуча-	–	Неудовлетворительно

ющийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки		

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2023

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.О.39 Основы информационной безопасности

Форма обучения Очное

Вид контроля Зачет с оценкой

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Виды национальной безопасности и их краткая характеристика
2. Средства обеспечения 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)			

10

Концептуальная комплексность включает:			*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.	обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы		*0*
B.	обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла		*0*
C.	защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства		*0*
D.	комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода		*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)			

11

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 неправиль-ный.	
	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)			

12

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 неправиль-ный.	
	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)			

13

Правовая защита информации – это:			*МС*
		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 неправиль-ный.	
	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. (МС/МА)			

14

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)			

15

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 неправиль-ный.	
	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

Какие из перечисленных угроз относятся к случайным угрозам компьютерной 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.	несанкционированный доступ к информации, вредительские программы, ошибки при разработке компьютерной системы		*0*
B.	электромагнитные излучения и наводки, несанкционированная модификация структур компьютерной системы		*0*
C.	стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала		*100*
D.	технические каналы утечки 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)			

3

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)			

4

Технический канал утечки информации – это:			*МС*
		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. (МС/МА)			

5

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)			

6

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)			

7

Структурная комплексность включает:			*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.	обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы		*0*
B.	обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла		*0*
C.	защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства		*100*
D.	комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода		*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

Временная комплексность включает:			*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.	обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы		*0*
B.	обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла		*100*
C.	защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства		*0*
D.	комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода		*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)			

9

Целевая комплексность включает:			*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.	обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы		*100*
B.	обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла		*0*
C.	защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства		*0*
D.	комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода		*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)			

Задания с коротким ответом

16

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.*			

17

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.*			

18

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

19

<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>

20

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

21

<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>