МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный университет»

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«05» июля 2018 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.06 Управление информационной безопасностью

1. Шифр и наименование направления подготовки/специальности:
09.04.02 Информационные системы и технологии

2. Профиль подготовки/специализации:
Безопасность информационных систем

3. Квалификация (степень) выпускника: магистр

4. Форма образования: очная

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

6. Составители программы:
Вялых Сергей Ариевич, к.т.н., доцент

7. Рекомендована:
Научно-методическим советом ФКН, протокол № 6 от 25.06.2018 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2019-2020 **Семестр(-ы):** 3

9. Цели и задачи учебной дисциплины: изучение основ и овладение практическими навыками планирования, развертывания и поддержания комплекса регламентов и процедур, направленных на минимизацию рисков нарушения информационной безопасности при разработке, сопровождении и проектировании информационных систем различного назначения; получение профессиональных компетенций в области современных технологий обработки и защиты информации.

Основные задачи дисциплины:

- освоение студентами положений и требований, современных нормативно-методических документов, регламентирующих меры, обеспечивающие информационную безопасность информационных систем различного назначения;
- формирование представления о системе управления информационной безопасностью в организации;
- овладение практическими навыками разработки системы документов, регламентирующих требования и меры, обеспечивающие информационную безопасность в информационных системах различного назначения, разработки модели угроз, выявления и анализа рисков информационной безопасности;
- формирование представления о процедурах планирования и практической реализации процессов, направленных на минимизацию рисков информационной безопасности и контроля выполнения мер по защите информационных систем, различного назначения.

10. Место учебной дисциплины в структуре ООП: Блок Б1.В относится к профессиональному циклу дисциплин вариативной профильной части.

Для успешного освоения дисциплины необходимы входные знания в области основ информационной безопасности, программно-аппаратных средств защиты информации, криптографических методов защиты информации, организационно и правовом обеспечении информационной безопасности.

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

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-8	Способность проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция	**знать:** базовые понятия, требования нормативных документов, методы анализа информационной безопасности при проектировании и эксплуатации информационных систем; **уметь:** анализировать и разрабатывать модели угроз для различных объектов защиты; **владеть:** практическими навыками формирования требований безопасности информации для различных классов и уровней защищенности информационных систем.
ПК-9	Способность проводить разработку и исследование методик анализа, синтеза, оптимизации и прогнозирования качества процессов функционирования информационных систем и технологий	**знать:** состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы; **уметь**: проводить разработку политики информационной безопасности для различных вариантов построения защищенных информационных систем; **владеть**: навыками комплексного подхода к обеспечению информационной безопасности объекта защиты.

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

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)			
	Всего	По семестрам		
		№ сем. 3	№ сем.	Итого
Аудиторные занятия	50	50		50
в том числе: лекции	16	16		16
практические	-	-		
лабораторные	34	34		34
Самостоятельная работа	58	58		58
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*	36	36		36
Итого:	144	144		144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Система управления информационной безопасностью	1. Система управления информационной безопасностью. Модель разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы управления информационной безопасности.
1.2	Государственная информационная система, классы защищённости информационной системы	2. Государственная информационная система, классы защищённости информационной системы. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.
1.3	Обеспечение безопасности персональных данных при их обработке в информационных системах	3. Понятие категории персональных данных. И её нормативно-правовое регулирование. Основные этапы организации обработки и обеспечения безопасности персональных данных. Определение уровня защищенности персональных данных. 4. Обеспечение защиты персональных данных в ходе эксплуатации и при выводе из эксплуатации информационной системы персональных данных.
1.4	Требования безопасности информации при использовании криптографических средств защиты	5. Криптографические средства защиты информации. Приказ ФСБ № 378 от 10 июля 2014 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
1.5	Модели угроз безопасности информации.	6. Методика определения угроз безопасности информации в информационных системах. Модель нарушителя. Модель угроз безопасности информации.
1.6	Организация обработки персональных данных и обеспечение безопасности информации.	7. Организация обработки персональных данных в органах государственной власти и местного самоуправления.
1.7	Контроль выполнения требований по обеспечению безопасности информации	8. Контроль выполнения требований по обеспечению безопасности информации в государственных информационных системах и информационных системах персональных данных.
2. Практические занятия		
2.1	нет	
3. Лабораторные работы		
3.1	Государственная информационная система, классы защищённости информационной системы	1. Определение класса защищенности государственной информационной системы. 2. Формирование требований к мерам защиты информации для различных классов защищенности в государственных информационных системах.

3.2	Обеспечение безопасности персональных данных при их обработке в информационных системах	3. Определение уровня защищенности информационной системы обрабатывающей персональные данные. 4. Формирование требований к мерам защиты информации для различных уровней защищенности в информационных системах обрабатывающих персональные данные.
3.3	Требования безопасности информации при использовании криптографических средств защиты	5. Формирование состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты.
3.4	Модели угроз безопасности информации	6. Определение источников угроз безопасности информации. 7. Оценка возможностей нарушителей по реализации угроз безопасности информации (разработка модели нарушителя). 8. Оценка возможных способов реализации угроз безопасности информации. 9. Оценка проектной защищенности информационной системы. 10. Оценка возможного ущерба от реализации угрозы безопасности. 11. Определение актуальных угроз безопасности информации в информационной системе. 12. Определение угроз безопасности информации при использовании средств криптографической защиты. 13. Разработка модели угроз безопасности информации в информационной системе.
3.5	Организация обработки персональных данных и обеспечение безопасности информации.	14. Разработка комплекса организационных и технических мер обеспечения защиты информации в информационной системе с использованием сертифицированных средств защиты информации.
3.6	Контроль выполнения требований по обеспечению безопасности информации	15. Контроль выполнения требований по обеспечению безопасности информации в государственных информационных системах. 16. Контроль выполнения требований по обеспечению безопасности информации в информационных системах обрабатывающих персональные данные. 17. Контроль выполнения требований по обеспечению безопасности информации в информационных системах использующих средства криптозащиты.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Система управления информационной безопасностью.	2	-	6	8
2	Государственная информационная система, классы защищённости информационной системы	2	4	8	14
3	Обеспечение безопасности персональных данных при их обработке в информационных системах.	4	4	8	16
4	Требования безопасности информации при использовании криптографических средств защиты.	2	2	8	12
5	Модели угроз безопасности информации	2	16	8	26
6	Организация обработки персональных данных и обеспечение безопасности информации	2	2	8	12
7	Контроль выполнения требований по обеспечению безопасности	2	6	12	20

	информации.				
	Итого:	16	34	58	108

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

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 лабораторно-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 лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

В ходе самостоятельной работы необходимо уделить основное внимание работе с текстом конспекта лекции, изучению рекомендованной литературы, изучению нормативных документов по информационной безопасности.

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	Основы управления информационной безопасностью : [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.] .— 2-е изд., испр. — Москва : Горячая линия-Телеком, 2014 .— 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
2	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
3	Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5-91134-336-1.

б) дополнительная литература:

№ п/п	Источник
4	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
5	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451
6	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст)

7	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
8	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
9	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
10	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
11	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
12	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.

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

№ п/п	Ресурс
13	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
14	Методический документ. Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., http://fstec.ru/component/attachments/download/812.
15	Банк данных угроз безопасности информации, ФСТЭК России, март 2015 г., http://bdu.fstec.ru/

* 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	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
2	Методический документ. Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., http://fstec.ru/component/attachments/download/812.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Для реализации учебного процесса используется установленная версия пакета среды виртуализации VMware, образы операционных систем семейства Windows, доступ в сеть 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) Лекционная аудитория, рабочее место преподавателя: ПК-Intel-i3, проектор, специализированная мебель: доска меловая 1 шт., столы 16 шт., стулья 33 шт.; доступ к

фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.
2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385),ПК-Intel-i3 16 шт., специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-8 способность проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция	**знать:** базовые понятия, требования нормативных документов, методы анализа информационной безопасности при проектировании и эксплуатации информационных систем.	Разделы 1-4. Система управления информационной безопасностью. Классы и уровни защищенности информационных систем. Криптографические средства защиты.	Устный опрос. Лабораторные работы 1-5,
	уметь: анализировать и разрабатывать модели угроз для различных объектов защиты.	Разделы 5 Методика определения угроз безопасности информации в информационных системах	Устный опрос. Лабораторные работы 6-13
	владеть: практическими навыками формирования требований безопасности информации для различных классов и уровней защищенности информационных систем.	Разделы 2-4 Организационные и технические меры обеспечения защиты информации в информационной системе с использованием сертифицированных средств защиты информации	Устный опрос. Лабораторные работы 1-5
ПК-9 способность проводить разработку и исследование методик анализа, синтеза, оптимизации и прогнозирования качества процессов функционирования информационных систем и технологий	**знать:** состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы.	Разделы 2-4 Требования по обеспечению безопасности информации в государственных информационных системах и информационных системах персональных данных.	Устный опрос. Лабораторные работы 1-5. Контрольная работа по соответствующим разделам или тест
	уметь: проводить разработку политики информационной безопасности для различных вариантов построения защищенных информационных систем.	Разделы 2-4 Требования по обеспечению безопасности информации в государственных информационных системах и информационных системах персональных данных.	Устный опрос. Лабораторные работы 1-5. Контрольная работа по соответствующим разделам или тест
	владеть: навыками комплексного подхода к обеспечению информационной безопасности объекта защиты.	Разделы 1-7 Требования по обеспечению безопасности информации в государственных информационных системах и информационных систе-	Устный опрос. Лабораторные работы 1-17. Контрольная работа по соответствующим разде-

		мах персональных данных.	лам или тест
Промежуточная аттестация			Комплект КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

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

1) знание нормативных документов, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование требований нормативных документов и практических мер их реализующих с использованием с использованием сертифицированных средств защиты информации;

3) умение связывать требования нормативных документов 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 администрирования компьютерных систем и средств защиты в рамках выполняемых лабораторных заданий;

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

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

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

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

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 зна-	Пороговый уровень	Удовлетвори-

ний, 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.		тельно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2
3	Лабораторная работа	Содержит 15 лабораторных заданий, предусматривающие разработку требований по уровням и классам защищенности различных информационных систем, разработки и внедрения их систем защиты, а также контроля ее эффективности.	При успешно выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

19.3.2. Примерный перечень вопросов к экзамену

№	Содержание
1	Система управления информационной безопасностью. Модель разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы управления информационной безопасности.
2	Государственная информационная система, классы защищённости информационной системы.
3	Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.
4	Понятие категории персональных данных. И её нормативно-правовое регулирование.
5	Основные этапы организации обработки и обеспечения безопасности персональных данных.
6	Определение уровня защищенности персональных данных и классификация информационных систем персональных данных
7	Формирование политики в отношении обработки персональных данных.
8	Формирование облика и внедрение системы защиты персональных данных.
9	Обеспечение защиты персональных данных в ходе эксплуатации и при выводе из эксплуатации информационной системы персональных данных

10	Требования безопасности информации при использовании криптографических средств защиты.
11	Модель угроз безопасности информации.
12	Модель нарушителя безопасности информации.
13	Банк данных угроз безопасности информации.
14	Возможные способы реализации угроз безопасности информации.
15	Виды ущерба безопасности информации и методы его оценки.
16	Контроль выполнения требований по обеспечению безопасности информации в государственных информационных системах.
17	Оценка эффективности принимаемых мер защиты персональных данных в информационных системах персональных данных.

19.3.3. Пример задания для выполнения лабораторной работы

Лабораторная работа №15

Контроль выполнения требований по обеспечению безопасности информации в государственных информационных системах. «Управление информационной безопасностью в операционной системе Windows 7 с использованием локальных политик безопасности»

Цель работы: практическое изучение методов управления информационной безопасностью в современных информационных системах.
Вариант №1. Настройка правил парольной защиты входа в информационную систему в соответствии с требованиями нормативных документов и контроль их выполнения.

19.3.4. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2018

Направление подготовки / специальность 09.04.02 Информационные системы и технологии

Дисциплина Б1.В.07 Управление информационной безопасностью

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Государственная информационная система, классы защищённости государственной информационной системы.
2. Базовые организационные и технические меры защиты информации, реализуемые в государственной информационной системе в рамках ее системы защиты.

Преподаватель _____ С.А. Вялых

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

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, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 19.2.