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

УТВЕРЖДАЮ

Заведующий кафедрой программного обеспечения
и администрирования информационных систем

Артемов М. А.

08.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.Б.21 Организация защиты информации

1. Шифр и наименование направления подготовки:

09.03.03 Прикладная информатика

2. Профиль подготовки: Прикладная информатика в юриспруденции

3. Квалификация (степень) выпускника: бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

программного обеспечения и администрирования информационных систем

6. Составители программы:
Железняк В.П.., к.т.н., преподаватель

7. Рекомендована: НМС факультета ПММ протокол № 10 от 18.06.2018

8. Учебный год: 2018/2019 **Семестр:** 7-8

9. **Цели и задачи учебной дисциплины:**
Сформировать представление об информационной безопасности, категории доступа к информации, угрозах информационной безопасности, организационных аспектах защиты информации

10. Место учебной дисциплины в структуре ООП: дисциплина относится к Б1.Б. 21.

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	
ОПК-3	способность использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности	знать: порядок классификации государственных информационных систем
ОПК-4	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знать требования к информационной безопасности информационной системы
ПК-11	способность эксплуатировать и сопровождать информационные системы и сервисы	уметь: сопровождать информационные системы и сервисы с учетом требований защиты информации
ПК-13	способность осуществлять инсталляцию и настройку параметров программного обеспечения информационных систем	владеть: навыками определения уровня исходной защищенности информационной системы

12.1. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 3/108.

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)		
	Всего	По семестрам	
		7	8
Аудиторные занятия	82	50	32

в том числе: лекции	66	34	16
лабораторные			
практические	32	16	16
Самостоятельная работа	78	22	56
Итого	180	72	108
Промежуточная аттестация (экзамен)	72	36	36
Итого:	**252**	**108**	**144**

13.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Основные понятия	Понятия информации и обладателя информации. Права обладателя информации. Разделение информации в зависимости от категории доступа к ней. Право на доступ к информации. Ограничение на доступ к информации. Понятия защиты информации и информационной безопасности. Обеспечиваемые характеристики безопасности.
2	Категории информации и классификация информационных систем	Категорирование информации. Существующие категории информации с ограниченным доступом. Понятие и виды объектов информатизации. Понятие, типы и виды информационных систем. Порядок классификации государственных информационных систем.
3	Угрозы безопасности информации	Понятие уровня значимости информации, его определение. Порядок определения уровня защищенности персональных данных при их обработке в информационной системе. Понятие недекларированных возможностей. Типы актуальных угроз безопасности персональных данных. Понятие и типы источников угроз безопасности информации. Источники антропогенных угроз безопасности информации. Преднамеренные угрозы безопасности информации. Способы их реализации. Понятие и виды технических каналов утечки информации.
4	Анализ защищенности информационных систем	Нарушители безопасности информации. Типы и виды нарушителей безопасности информации. Цели (мотивации) реализации нарушителями угроз безопасности информации. Потенциал нарушителя. Возможные способы реализации угроз безопасности информации в информационной системе. Возможные объекты защиты в информационной системе. Структурно-функциональные характеристики информационной системы, влияющие на уровень исходной защищенности информационной системы. Порядок определения уровня исходной защищенности информационной системы
5	Понятие и идентификация угроз безопасности	Понятие угрозы безопасности информации. Цель определения угроз безопасности информации. Идентификация угрозы безопасности информации, ее описание. Нейтрализация идентифицированной угрозы безопасности информации. Оформление процесса определения угроз безопасности

		информации. Структура модели угроз безопасности информации. Актуальность идентифицированных угроз безопасности информации. Показатель актуальности угрозы безопасности информации, его описание. Случаи определения актуальности угроз безопасности информации. Порядок определения актуальности угрозы безопасности информации. Источники исходных данных об угрозах безопасности информации. Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), его содержание. Оценка вероятности (возможности) реализации угрозы безопасности информации.
6	Последствия реализации угрозы безопасности информации	Порядок оценки степени возможного ущерба от реализации угрозы безопасности информации. Определение возможного результата реализации угрозы безопасности информации. Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации. Определение степени возможного ущерба от реализации угрозы безопасности информации. Характеристики степени ущерба. Пересмотр (переоценка) идентифицированных и актуальных угроз безопасности информации.

13.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Основные понятия	8	4		11	23
2	Категории информации и классификация информационных систем	8	4		15	27
3	Угрозы безопасности информации	8	4		15	27
4	Анализ защищенности информационных систем	10	4		15	29
5	Понятие и идентификация угроз безопасности	8	8		11	27
6	Последствия реализации угрозы безопасности информации	8	8		11	27

14. Методические указания для обучающихся по освоению дисциплины

работа с конспектами лекций, презентационным материалом

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

) основная литература:

№ п/п	Источник
1.	*Основы информационной безопасности [Электронный ресурс] : учеб. пособие / Е.Б. Белов [и др.]. — Электрон. дан. — Москва : Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: https://e.lanbook.com/book/5121. — Загл. с экрана.*

б) дополнительная литература:

№ п/п	Источник
2.	*Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс] : учеб. пособие / Н.С. Кармановский, О.В. Михайличенко, Н.Н. Прохожев. — Электрон. дан. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Режим доступа: https://e.lanbook.com/book/91449. — Загл. с экрана.* *Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : учеб. пособие — Электрон. дан. — Санкт-Петербург : НИУ ИТМО, 2014. — 173 с. — Режим доступа: https://e.lanbook.com/book/70952. — Загл. с экрана.* *Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.* *Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс] : учеб. — Электрон. дан. — Москва : ФЛИНТА, 2014. — 448 с. — Режим доступа: https://e.lanbook.com/book/48368. — Загл. с экрана.* *Кожуханов, Н.М. Правовые основы информационной безопасности: учебное пособие [Электронный ресурс] : учеб. пособие / Н.М. Кожуханов, Е.С. Недосекова. — Электрон. дан. — Москва : РТА, 2013. — 88 с. — Режим доступа: https://e.lanbook.com/book/74237. — Загл. с экрана.*

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
3.	*Электронный каталог Научной библиотеки Воронежского государственного университета. – http://www.lib.vsu.ru/*

16. Материально-техническое обеспечение дисциплины:

Лабораторный класс с проектором (ауд 214): компьютеры (мониторы SyncMaster SA 200, системные блоки Intel Pentium CPU G620@ 2.60 GHz, ОЗУ 4 Гб) (16 шт.), мультимедиа-проектор BENQ, экран настенный для проектора, принтер HP Laser Jet Pro 400 M401dn, аудио колонки Creative A60, коммутатор

17. Фонд оценочных средств:

17.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	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)
ОПК-3 способность использовать основные законы естественнонаучных дисциплин и	знать: порядок классификации государственных информационных систем	Разделы 1-2	Комплект КИМ,

современные информационно-коммуникационные технологии в профессиональной деятельности			
ОПК-4 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знать требования к информационной безопасности информационной системы	Все разделы	Комплект КИМ, практические задания
ПК-11 способность эксплуатировать и сопровождать информационные системы и сервисы	уметь: сопровождать информационные системы и сервисы с учетом требований защиты информации	Разделы 3-6	Комплект КИМ, практические задания
ПК-13 способность осуществлять инсталляцию и настройку параметров программного обеспечения информационных систем	владеть: навыками определения уровня исходной защищенности информационной системы	Разделы 3-6	Комплект КИМ, практические задания
Промежуточная аттестация			опрос

17. 2 Список вопросов к экзамену

7 семестр.

1. Понятия информации и обладателя информации. Права обладателя информации. Разделение информации в зависимости от категории доступа к ней.
2. Право на доступ к информации. Ограничение на доступ к информации.
3. Понятия защиты информации и информационной безопасности. Обеспечиваемые характеристики безопасности.
4. Категорирование информации. Существующие категории информации с ограниченным доступом.
5. Понятие и виды объектов информатизации.
6. Понятие, типы и виды информационных систем.
7. Порядок классификации государственных информационных систем.
8. Понятие уровня значимости информации, его определение.
9. Порядок определения уровня защищенности персональных данных при их обработке в информационной системе.
10. Понятие недекларированных возможностей. Типы актуальных угроз безопасности персональных данных.
11. Понятие и типы источников угроз безопасности информации.
12. Источники антропогенных угроз безопасности информации.
13. Преднамеренные угрозы безопасности информации. Способы их реализации.
14. Понятие и виды технических каналов утечки информации.
15. Нарушители безопасности информации. Типы и виды нарушителей безопасности информации.
16. Цели (мотивации) реализации нарушителями угроз безопасности информации. Потенциал нарушителя.
17. Возможные способы реализации угроз безопасности информации в информационной системе.
18. Возможные объекты защиты в информационной системе.
19. Структурно-функциональные характеристики информационной системы, влияющие на уровень исходной защищенности информационной системы.
20. Порядок определения уровня исходной защищенности информационной системы.

8 семестр.

1. Понятие угрозы безопасности информации. Цель определения угроз безопасности информации.
2. Идентификация угрозы безопасности информации, ее описание. Нейтрализация идентифицированной угрозы безопасности информации.
3. Оформление процесса определения угроз безопасности информации. Структура модели угроз безопасности информации.
4. Актуальность идентифицированных угроз безопасности информации. Показатель актуальности угрозы безопасности информации, его описание. Случаи определения актуальности угроз безопасности информации.
5. Порядок определения актуальности угрозы безопасности информации.
6. Источники исходных данных об угрозах безопасности информации. Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), его содержание.
7. Оценка вероятности (возможности) реализации угрозы безопасности информации.

8. Порядок оценки степени возможного ущерба от реализации угрозы безопасности информации.

9. Определение возможного результата реализации угрозы безопасности информации.

10. Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации.

11. Определение степени возможного ущерба от реализации угрозы безопасности информации. Характеристики степени ущерба.

12. Пересмотр (переоценка) идентифицированных и актуальных угроз безопасности информации.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
свободно владеет материалом, отвечает на вопросы; умеет рассуждать; в случае незнания небольшой части материала способен выстроить собственную логическую цепочку рассуждений и получить ответ	*Повышенный уровень*	*Отлично*
знает материал, допускает неточности, не полностью отвечает на вопросы;	*Базовый уровень*	*Хорошо*
знание минимально допустимого объема материала; нежелание рассуждать;	*Пороговый уровень*	*Удовлетвори-тельно*
незнание материала	–	*Неудовлетвори-тельно*