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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа

А.Д. Баев
(подпись)
03.07.2018

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.08.01 Информационная безопасность

Код и наименование дисциплины в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

02.03.01 Математика и компьютерные науки

2. Профиль подготовки/специализация: Математические методы в экономике и финансах

3. Квалификация (степень) выпускника: Бакалавр

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: Кафедра математического анализа

6. Составители программы:
Шабров Сергей Александрович, канд. Физ.-мат. наук, доцент

7. Рекомендована: Научно-методическим советом математического факультета. протокол №0500-07 от 03.07.2018г.

(наименование рекомендующей структуры, дата, номер протокола,

отметки о продлении вносятся вручную)

8. Учебный год:2018-2019 Семестр(ы):7

9. Цели и задачи учебной дисциплины:

Цели изучения дисциплины:

предоставление обучаемым знаний основных типов и способов защиты информации; приобретение студентами умения проектировать системы защиты информации;

Задачи дисциплины:

овладение современными программными и аппаратными средствами защиты информации.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к математическому и естественнонаучному циклу ФГОС ВПО в структуре ООП бакавриата. Для изучения дисциплины слушатели должны владеть базовыми знаниями школьного курса «Информатика» в области алгоритмизации и программирования.

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-2		Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.
ОПК-3		Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.
ОПК-4		Знать: основные понятия информационной

		безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **— 1** /32.

Форма промежуточной аттестации*(зачет/экзамен) зачет* **.**

13. Виды учебной работы

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра	№ семестра	7
Аудиторные занятия	32			32
в том числе: лекции	16			16
практические				
лабораторные	16			16
Самостоятельная работа				
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*				
Итого:	32			32

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		1. Лекции
1.1	Общие вопросы информационной безопасности	Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.

1.2	Государственная система информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
1.3	Угрозы безопасности	Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
1.4	Теоретические основы методов защиты информационных систем	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.
1.5	Методы защиты средств вычислительной техники	Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.
3. Лабораторные работы		
3.1	Общие вопросы информационной безопасности	Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
3.2	Государственная система информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности

		Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
3.3	Угрозы безопасности	Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
3.4	Теоретические основы методов защиты информационных систем	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.
3.5	Методы защиты средств вычислительной техники	Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Общие вопросы информационной безопасности	2		2		4
02	Государственная система информационной безопасности	4		4		8
03	Угрозы безопасности	2		2		4
04	Теоретические основы методов защиты информационных систем	4		4		8
05	Методы защиты средств вычислительной техники	4		4		8
	Итого	16		16		32

14. Методические указания для обучающихся по освоению дисциплины
работа с конспектами лекций

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

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	Голуб, Владимир Александрович. Информационная безопасность СМИ: криптографическая защита информации : учебное пособие / В.А. Голуб ; Воронеж. гос. ун-т, Фак. журналистики .— Воронеж : Факультет журналистики ВГУ, 2010 .— 99 с.

б) дополнительная литература:

№ п/п	Источник
2	Мещеряков Р. В. Информационная безопасность: Учеб. пособие – Томск.: Изд-во Том. политехн. Ун-т, 2004 – 168 с.
3	Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информационной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.
4	Мещеряков Р. В., Шелупанов А. А., Белов Е. Б., Лось В. П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 540 с.
5	Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994.
6	Герасименко В. А., Малюк А. А. Основы защиты информации. – М.: «Инкомбук», 1997. – 540 с.

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

№ п/п	Ресурс
1.	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
2.	*Google, Yandex, Rambler*

* 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 Р. В. Информационная безопасность: Учеб. пособие – Томск.: Изд-во Том. политехн. Ун-т, 2004 – 168 с.
2	Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информационной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.

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

---

18. Материально-техническое обеспечение дисциплины: компьютерный класс

---

19. Фонд оценочных средств:

19.1. 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 - 2	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем.	Все разделы	Опрос
	Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации.	Все разделы	Опрос
	Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.	Все разделы	Опрос
ОПК -3	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем.	Все разделы	Опрос
	Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта	Все разделы	Опрос

	информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации.		
	Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.	Все разделы	Опрос
ОПК -4	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем.	Все разделы	Опрос
	Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации.	Все разделы	Опрос
	Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.	Все разделы	Опрос
Промежуточная аттестация			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

1) знание учебного материала и владение понятийным аппаратом;
2) умение связывать теорию с практикой;
3) умение иллюстрировать ответ примерами, фактами, данными научных исследований;
4) умение применять полученные знания на практике;
5) владение понятийным аппаратом данной области науки (теоретическими основами дисциплины), способность иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения практических задач.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения практических задач в области…	*Повышенный уровень*	*зачет*
Обучающийся владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), допускает не значительные ошибки при ответе.	*Базовый уровень*	*зачет*
Обучающийся владеет частично теоретическими основами дисциплины, фрагментарно способен дать ответ .	*Пороговый уровень*	*зачет*
Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки,	–	*Незачет*

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 Перечень вопросов к экзамену (зачету): (нужное выбрать)

1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность.
2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
3. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена.
4. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации.
5. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
6. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
7. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности.
8. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации.
9. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
10. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения.
11. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз.
12. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
13. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение.
14. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы.
15. Ролевая политика безопасности. Ограничения на области применения формальных моделей.
16. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы.

17. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

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

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на занятиях.

К основным формам текущего контроля можно отнести устный опрос.

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины в форме зачета.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение как отдельной дисциплины, так и ее разделов. Промежуточная аттестация помогает оценить более крупные совокупности знаний и умений, в некоторых случаях даже формирование определенных компетенций.

На зачете оценивается практический уровень освоения дисциплины и степень сформированности компетенций оценками «зачет» и «не зачет».

Задания текущего контроля и проведение промежуточной аттестации должны быть направлены на оценивание уровня освоения теоретических и практических понятий, научных основ профессиональной деятельности; степени готовности обучающегося применять теоретические и практические знания и практически значимую информацию; приобретение умений профессионально значимых для профессиональной деятельности.