

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

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа
и операторных уравнений

Каменский М.И.

подпись, расшифровка подписи

26.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.32 Информационная безопасность

1. Шифр и наименование направления подготовки / специальности: 01.05.01

Фундаментальные математика и механика

2. Профиль подготовки / специализации:

3. Квалификация (степень) выпускника: специалист

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины: функционального анализа
и операторных уравнений

6. Исполнители программы: Сидельникова Софья Юрьевна, математический факультет, кафедра функционального анализа и операторных уравнений

7. Рекомендована: НМС математического факультета, протокол №0500-07 от 03.07.2018 г.

8. Учебный год: 2018-2019

Семестр(ы): 8

9. Цели и задачи учебной дисциплины:

Цель курса - изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Основными задачами изучения дисциплины являются:

- изучение характеристик основных угроз информационной безопасности, каналов утечки информации и методов компьютерного шпионажа;

- получение представлений о существующих правовых, организационных методах и технических средствах защиты информации от несанкционированного доступа и от модификации и удаления;
- освоение критериев эффективности мер по защите информации.

10. Место учебной дисциплины в структуре ООП: Дисциплина входит в базовую часть математического и естественнонаучного цикла. Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Теория графов и математическая логика, Теория вероятностей, математическая статистика и теория случайных процессов, Алгоритмы дискретной математики, Операционные системы и сети, Программные аппаратные средства информатики, Программирование для ЭВМ. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области защиты информации.

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	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p>знать: как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p> <p>уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p> <p>владеть (иметь навык(и)): методами решений стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>
ОПК-4	способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	<p>Знать: как находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем.</p> <p>Уметь: находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем.</p> <p>Владеть: навыками, позволяющими находить, ана-</p>

		лизировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем
--	--	---

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 2/72

Форма промежуточной аттестации: зачет

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		сем. № 8
Аудиторные занятия	32	32
в том числе: лекции	16	16
практические	-	-
лабораторные	16	16
Самостоятельная работа	40	40
Форма промежуточной аттестации		1 контрольная работа, зачет
Итого:	72	72

13.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в теорию информационной безопасности	Основные понятия и определения. Концептуальные основы информационной безопасности и защиты информации
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	Понятие об информационных ресурсах. Понятия интеллектуальной собственности и коммерческой тайны, их структура. Персональные данные. Принципы информационной безопасности.
3	Угрозы информационной безопасности и их классификация.	Угрозы информационным ресурсам: угрозы несанкционированного доступа, модификации и удаления информации; угрозы криминогенного характера, природного и техногенного характера, угрозы, связанные с неквалифицированным использованием информационными ресурсами. Компьютерный шпионаж, его цели и методы. Внутренние и внешние факторы, способствующие компьютерному шпионажу. Характеристика каналов утечки информации. Активный и пассивный доступ к информационным ресурсам.
4	Правовые аспекты защиты информации.	Понятие о правовых средствах защиты информации. Законы, регулирующие деятельность по защите информации. Охрана объектов интеллектуальной собственности. Проблемы, возникающие при реализации правовых мер защиты информации.
5	Организационные мероприятия, направленные на защиту информации.	Ограничение и разграничение доступа к информации. Дублирование важной информации на разнотипных носителях. Многоуровневая система защиты информации.
6	Программно-аппаратные средства защиты информации	Пароли и системы с многоуровневым доступом. «Защита от дурака» в компьютерных программах. Защита программ и электронных баз данных. Антивирусные программы. Защита каналов связи. Повреждение информации в каналах связи и

		средства борьбы с ним.
7	Математические методы и модели в задачах защиты информации.	Методы сжатия информации. Криптографические методы защиты информации. Шифрование с симметричными и асимметричными ключами.
8	Эффективность мероприятий по защите информации	Частный функциональный критерий информационной безопасности и его формула для мероприятий по предотвращению несанкционированного доступа. Структура понесенного и предотвращенного ущерба от несанкционированного доступа к информации. Структура затрат на защиту информации.

13.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Введение в теорию информационной безопасности	2	2	4	8
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	2	2	4	8
3	Угрозы информационной безопасности и их классификация.	2	2	6	10
4	Правовые аспекты защиты информации.	2	2	6	10
5	Организационные мероприятия, направленные на защиту информации.	2	2	4	8
6	Программно-аппаратные средства защиты информации	2	2	6	10
7	Математические методы и модели в задачах защиты информации.	2	2	6	10
8	Эффективность мероприятий по защите информации	2	2	4	8
	Итого	16	16	40	72

14. Методические указания для обучающихся по освоению дисциплины

Преподавание дисциплины заключается в чтении лекций и проведении лабораторных занятий. На лекциях рассказывается теоретический материал, на лабораторных занятиях решаются примеры по теоретическому материалу, прочитанному на лекциях. При изучении курса «Информационная безопасность» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения обучающимся рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения, разобрать примеры, решенные на лекции. Перед следующей лекцией обязательно повторить материал предыдущей лекции.

2. Перед лабораторным занятием обязательно повторить лекционный материал. После лабораторного занятия еще раз разобрать решенные на этом занятии примеры, после приступить к выполнению домашнего задания. Если при решении примеров, заданных на дом, возникают вопросы, обязательно задать на следующем лабораторном занятии или в присутствующий час преподавателю.

3. При подготовке к лабораторным занятиям повторить основные понятия по темам, изучить примеры. Решая задачи, предварительно понять, какой теоретический мате-

риал нужно использовать. Наметить план решения, попробовать на его основе решить лабораторные задачи.

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

а) основная литература:

№ п/п	Источник
1	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
2	Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.

б) дополнительная литература:

№ п/п	Источник
3	Скоромников, Кир Серафимович. Компьютерное право Российской Федерации : Учебник / К.С.Скоромников;Междунар.независим. эколого-политол.ун-т .— М. : Изд-во МНЭПУ, 2000 .— 220,[1] с. — ISBN 5-7383-0105-6.
4	Чубукова, Светлана Георгиевна. Основы правовой информатики (юридические и математические вопросы информатики) : учебное пособие для студ. / С.Г. Чубукова, В.Д. Элькин ; Моск. гос. юрид. акад.; под ред. М.М. Рассолова .— М. : Контракт, 2004 .— 247 с. : ил. — На обл. авт. не указан .— Библиогр. в конце глав .— ISBN 5-900785-84-Х.программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил.
5	Велпури, Рама. Огаслеѝ : Резервное копирование и восстановление / Р. Велпури, А. Адколи ; Пер.с англ. И. Афанасьева; Науч. ред. А. Головки; Авт. предислов. Я. Текер .— М. : Лори, 2002 .— 572 с. : ил .— Парал. тит. л. англ. — ISBN 5-85582-166-8.
6	Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.
7	Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин .— Екатеринбург : Изд-во Уральского ун-та, 2003 .— 327 с. : ил .— Библиогр.:с.317-322 .— Алф.-предм. указ.: с.306-316 .— ISBN 5-86037-024-5.
8	Голуб, Владимир Александрович. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — ISBN 5-86026-020-2 : 37.00 .— <URL: http://www.lib.vsu.ru/elib/books/b102829.djvu >.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
9	www.fstec.ru , www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1.	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
2.	Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.
3.	Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.

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

Лекция с применением современных компьютерных технологий (лекция-презентация).

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория (доска, мел, маркеры), компьютерные классы для проведения лабораторных работ, программное обеспечение, мультимедийный проектор.

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 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p>знать: как решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>	<p>Введение в теорию информационной безопасности</p>	<p>Текущая аттестация – контрольная работа. Контрольно-измерительный материал к контрольной работе. Промежуточная аттестация – зачет. Контрольно-измерительные материалы к зачету</p>
	<p>уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>	<p>Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.</p>	
	<p>владеть (иметь навык(и)): методами решений стандартных задач профессиональной деятельности на основе информационной и</p>	<p>Угрозы информационной безопасности и их классификация.</p> <p>Правовые аспекты защиты информации.</p>	

	библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Организационные мероприятия, направленные на защиту информации.	
ОПК-4 способность находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	Знать: как находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем.	Программно-аппаратные средства защиты информации	Текущая аттестация – контрольная работ. Контрольно-измерительный материал к контрольной работе. Промежуточная аттестация –зачет. Контрольно-измерительные материалы к зачету
	Уметь: находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем.	Математические методы и модели в задачах защиты информации.	
	Владеть: навыками, позволяющими находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	Эффективность мероприятий по защите информации	
Промежуточная аттестация			КИМ

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

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

Текущая аттестация проводится в форме лабораторных работ и контрольной работы.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.

Для оценивания результатов обучения на зачете используется – зачтено, не зачтено
Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
<i>Обучающийся в полной мере владеет понятийным аппаратом в области программирования и технологии работы на ЭВМ, информационной безопасности, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач программирования в области информационной безопасности.</i>	<i>Повышенный уровень</i>	<i>Зачтено</i>
<i>У обучающегося сформированы знания, умения и навыки программирования и технологии работы на ЭВМ в области информационной безопасности; он способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач; но допускает отдельные несущественные пробелы в своих знаниях, допускает ошибки при выполнении практических задач.</i>	<i>Базовый уровень</i>	
<i>У обучающегося сформированы неполные знания, умения и навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.</i>	<i>Пороговый уровень</i>	
<i>Ответ на контрольно-измерительный материал не соответствует четырем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки.</i>	–	<i>Незачтено</i>

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 Задания для зачета:

Пример КИМ № 1

УТВЕРЖДАЮ
Заведующий кафедрой функционального
анализа и операторных уравнений

_____ Каменский М.И.
подпись, расшифровка подписи

_____._____._____

Направление подготовки / специальность 01.05.01 Фундаментальные математика и механика

Дисциплина Б1.Б.32 Информационная безопасность

Форма обучения очная
очное, очно-заочное, заочное

Вид контроля зачет
экзамен, зачет

Вид аттестации промежуточная
текущая, промежуточная

Контрольно-измерительный материал № _____1. Угрозы информационной безопасности.2. Методы и средства инженерной защиты объектов информатизации

Преподаватель _____
подпись расшифровка подписи

19.3.2 Задания для контрольной работы:

Пример контрольного задания (вариант задания)

Контрольная работа**Вариант 1.****Задание 1.** Угрозы информационной безопасности.

Задание 2. В результате шифрования методом Вижинера был получен следующий шифртекст: «СПЦСЗЗЮУГИВЕБЪБТЖЩИОБ». Прочитайте этот шифртекст, если известно, что шифрующая последовательность содержит только символы А, Б и В.

Вариант 2.

Задание 1. Методы и средства инженерной защиты объектов информатизации.

Задание 2. В результате шифрования методом Вижинера был получен следующий шифртекст: «СПЦСЗЗЮУГИВЕБЬБТЖЦИОБ». Прочитайте этот шифртекст, если известно, что шифрующая последовательность содержит только символы А, Б и В.

19.3.2 Примерные темы рефератов:

1. Структура Государственной системы обеспечения информационной безопасности Российской Федерации.
2. Иерархия законодательства Российской Федерации в области информационной безопасности.
3. Основные положения федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
4. Доктрина информационной безопасности Российской Федерации
5. Основные положения федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями от 25 ноября, 27 декабря 2009 г.)
6. Основные положения федерального Российской Федерации «Об электронной подписи» от 6 апреля 2011 г. N 63-ФЗ.
7. Основные положения федерального закона от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (с изменениями от 2 февраля, 18 декабря 2006 г., 24 июля 2007 г.)
8. Основные положения постановления Правительства РФ от 17 ноября 2007 г. N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
9. Основные положения приказа Министерства информационных технологий и связи РФ от 9 января 2008 г. N 1 «Об утверждении требований по

защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации»

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, проверку домашних заданий, лабораторные работы, контрольные работы. Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины «Информационная безопасность» 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 профессиональных компетенций. На зачете оценивается практический уровень освоения дисциплины и степень сформированности компетенций оценками «зачтено», «не зачтено». 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.