

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

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа и операторных уравнений
наименование кафедры, отвечающей за реализацию дисциплины

ка

Каменский М.И.
подпись, расшифровка подписи
26.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.3.1 Информационная безопасность

Код и наименование дисциплины в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

01.03.01 Математика

2. Профиль подготовки/специализация: _____

3. Квалификация (степень) выпускника: бакалавр

4. Форма обучения: очная

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

6. Составители программы: Завгородний Михаил Григорьевич
(ФИО, ученая степень, ученое звание)

Канд. физ-мат. наук, доцент

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

8. Учебный год: 2018-2019

Семестр(ы): 7

9. Цели и задачи учебной дисциплины:

Цель курса - изучение основных принципов информационной безопасности, 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: (блок Б1, базовая или вариативная часть, к которой относится дисциплина; требования к входным знаниям, умениям и навыкам; дисциплины, для которых данная дисциплина является предшествующей))

Дисциплина входит в вариативную часть (дисциплины по выбору) математического и естественнонаучного цикла. Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Дискретная математика и математическая логика, Теория вероятностей, случайные процессы, Алгоритмы дискретной математики, Технология программирования и работа на 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	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: общие проблемы информационной безопасности, ее роль и место на современном этапе развития общества; правовые основы защиты информации; основные методы криптографической защиты информации; методы защиты информации в вычислительных сетях; технические средства обеспечения безопасности; принципы функционирования компьютерных вирусов и методы борьбы с ними;</p> <p>уметь: использовать полученные знания для организации безопасной работы персональных компьютеров и сетей на их основе; использовать программно-аппаратные средства защиты от несанкционированного доступа и модификации информации; защищать ресурсы персональных компьютеров и сетей на их основе от компьютерных вирусов и их вредного воздействия;</p> <p>владеть (иметь навык(и)): навыками работы со специальной литературой; навыками работы со специализированным программно-аппаратным обеспечением компьютерной безопасности.</p>
ПК-1	способность к определению	знать: общие проблемы

	<p>общих форм и закономерностей отдельной предметной области</p>	<p>информационной безопасности, ее роль и место на современном этапе развития общества; правовые основы защиты информации; основные методы криптографической защиты информации; методы защиты информации в вычислительных сетях; технические средства обеспечения безопасности; принципы функционирования компьютерных вирусов и методы борьбы с ними;</p> <p>уметь: использовать полученные знания для организации безопасной работы персональных компьютеров и сетей на их основе; использовать программно-аппаратные средства защиты от несанкционированного доступа и модификации информации; защищать ресурсы персональных компьютеров и сетей на их основе от компьютерных вирусов и их вредного воздействия;</p> <p>владеть (иметь навык(и)): навыками работы со специальной литературой; навыками работы со специализированным программно-аппаратным обеспечением компьютерной безопасности.</p>
--	--	--

12. Объем дисциплины в зачетных единицах/час.(в соответствии с учебным планом) — 2/72.

Форма промежуточной аттестации(зачет/экзамен) зачет.

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам сем. № 7
Аудиторные занятия	32	32
в том числе: лекции	16	16
практические	-	-
лабораторные	16	16
Самостоятельная работа	40	40
Форма промежуточной аттестации		<i>Зачёт+1 контр. работа</i>
Итого:	72	72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в теорию информационной	Основные понятия и определения. Концептуальные основы информационной безопасности и защиты

	безопасности	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 ассиметричными 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. Темы (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	6	10
3	Угрозы информационной безопасности и их классификация.	2	2	8	12
4	Правовые аспекты защиты информации.	4	4	6	14
5	Организационные мероприятия, направленные на защиту информации.	4	4	6	14
6	Программно-аппаратные средства защиты информации	2	2	6	10
7	Математические методы и модели в задачах защиты информации.	6	6	16	28

8	Эффективность мероприятий по защите информации	2	4	6	12
	Итого	16	16	36	72

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.)

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)

№ 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. : АCADEMIA, 2006 .— 330 с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
2	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.
3	Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.
4	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.

* 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, задачки, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
5	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.
6	Велпури, Рама. Oracle8i : 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.
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>.

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

№ п/п	Источник
-------	----------

1	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 .
---	---

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)

Лекционная аудитория (доска, мел, маркеры), Компьютерный класс (14-15 компьютеров + программное обеспечение) мультимедийный проектор.

19. Фонд оценочных средств:

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.

Промежуточная аттестация проводится в форме и включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков.

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.

При сдаче зачета

оценка «зачтено» - 3-5 баллов

оценка «незачтено» - 0-2 балла

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
<i>Обучающийся в полной мере владеет понятийным аппаратом в области программирования и технологии работы на ЭВМ, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач программирования, СУБД и сетевых технологий.</i>	<i>Повышенный уровень</i>	<i>Отлично</i>
<i>У обучающегося сформированы знания, умения и навыки программирования и технологии работы на ЭВМ; 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>Хорошо</i>
<i>У обучающегося сформированы неполные знания, умения и</i>	<i>Пороговый</i>	<i>Удовлетвори-</i>

навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.	уровень	тельно
Сформированы лишь фрагментарные знания, умения и навыки или знания, умения и навыки отсутствуют	–	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

Пример КИМ № 1

УТВЕРЖДАЮ
Заведующий кафедрой функционального
анализа и операторных уравнений

_____ Каменский М.И.
подпись, расшифровка подписи

Направление подготовки / специальность _____ 01.03.01 математика

Дисциплина _____ Б1.В.ДВ.3.1 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

Пример контрольного задания (вариант задания) Контрольная работа по дисциплине «Информационная безопасность» Вариант № _____

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

