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.05 Информационная безопасность

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

2. Профиль подготовки/специализации: информатика как вторая компетенция

3. Квалификация (степень) выпускника: магистр

4. Форма образования: очная

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

6. Составители программы:
Митрофанова Елена Юрьевна, доцент, к.т.н.

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

(отметки о продлении вносятся вручную)

8. Учебный год: 2018/2019 **Семестр(-ы):** 2

9. Цели и задачи учебной дисциплины: изучение основ информационной безопасности, вопросов криптографии, стеганографии, защиты информации от несанкционированного доступа, обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, вопросов защиты исходных и байт кодов программ; получение профессиональных компетенций в области современных технологий защиты информации.

Основные задачи дисциплины:

- обучение студентов теоретическим и практическим аспектам обеспечения информационной безопасности;
- обучение студентов базовым принципам защиты конфиденциальной информации, методам идентификации, аутентификации пользователей информационной системы, принципам организации скрытых каналов передачи информации, принципам защиты авторских прав на объекты цифровой интеллектуальной собственности;

овладение практическими навыками применения теоретических знаний для шифрования конфиденциальной информации, стеганографического скрытия информации, контроля за целостностью информации, решения задач идентификации и аутентификации.

10. Место учебной дисциплины в структуре ООП: учебная дисциплина «Информационная безопасность» относится к блоку обязательные дисциплины вариативной части.

Для успешного освоения дисциплины необходимы входные знания в области устройства ЭВМ и операционных систем, принципах их работы, сетевых технологий, криптографии, информатики.

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	
ОК-6	Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности	**знать:** современные достижения науки, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности; **уметь:** самостоятельно приобретать и использовать в практической деятельности новые знания и умения; расширять и углублять свое научное мировоззрение; **владеть:** информационными технологиями
ПК-8	Умение проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информационных систем, управление технологическими процессами, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство, транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая	**знать:** теоретические основы моделей объектов различной профессиональной деятельности; **уметь:** проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности; **владеть:** навыками разработки и исследования теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информацион-

	промышленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоинформационные системы, лесной комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества	ных систем, управление технологическими процессами, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство, транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая промышленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоинформационные системы, лесной комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества.
ПК-10	Умение осуществлять моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований	**знать:** основы моделирования процессов и объектов; **уметь:** осуществлять моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований; **владеть:** навыками моделирования процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований.

12. Объем дисциплины в зачетных единицах/час — 2/72.
Форма промежуточной аттестации: *зачет*.

13 Виды учебной работы:

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 2	№ семестра	Итого
Аудиторные занятия	32	32		32
в том числе: лекции	16	16		16
практические	-	-		-
лабораторные	16	16		16
Самостоятельная работа	40	40		40
Форма промежуточной аттестации *(зачет – __ час. / экзамен – 0 час.)*	-	-		-
Итого:	72	72		72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
	1. Лекции	
1.1	Основные теоретические аспекты информационной безопасности	Понятие информационной безопасности и защищенной системы. Цели, задачи, практические аспекты защиты информационных систем и телекоммуникаций. Угрозы информационной безопасности, модели нарушителей. Общие требования к построению надежной системы защиты. Общие меры по обеспечению информационной безопасности.
1.2	Криптографические методы защиты информации	Предметная область криптографии. Исторические сведения и этапы развития криптографии. Криптографические преоб-

		разования. Симметричные и ассиметричные криптосистемы. Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП). Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных. Моделирование случайных величин с заданным законом распределения. Датчики случайных чисел. Гаммирование. Криптография с использованием эллиптических кривых. Шифрование, обмен ключами, ЭЦП на основе эллиптических кривых. Квантовая криптография. Криптоанализ. Виды криптоанализа. Принципы работы криптоаналитических алгоритмов.
1.3	Стеганографические методы защиты информации	Предметная область стеганографии. Стеганографические преобразования. Базовые методы цифровой стеганографии. Принципы сжатия изображений. Алгоритмы стеганографического скрытия информации в текстовые файлы, изображения, звуковые файлы, видео файлы, исполняемые файлы. Статистические и структурные методы скрытия информации. Использование аппарата искусственных нейронных сетей для реализации скрывающий и восстанавливающих информацию преобразований. Цифровые водяные знаки (ЦВЗ). Виды реализации, практические области применения. Перспективные направления развития стеганографических методов. Принципы стегоанализа. Визуальный, статистический, универсальный стегоанализ.
1.4	Защита программного обеспечения	Вредоносное ПО. Программные средства противодействия вирусам, антивирусы. Приемы защиты исходных кодов программ. Обфускация кода. Противодействие анализу двоичного кода программ.
2. Практические занятия		
2.1	нет	
3. Лабораторные работы		
3.1	1) Алгоритмы стеганографического скрытия данных в пространственной области контейнера 2) Алгоритмы стеганографического скрытия данных в частотной области	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Основные теоретические аспекты информационной безопасности	4	4	10	16
2	Криптографические методы защиты информации	4	4	10	16
3	Стеганографические методы защиты информации	4	4	10	16
4	Защита программного обеспечения	4	4	10	16
	Итого:	16	16	40	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.)

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 обработка информации, излагаемых в рамках лекций.

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	Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2.
2	Элементы теории чисел и критозащита : учебное пособие / Воронеж. гос. ун-т; сост. : Б.Н. Воронеков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 87 с. : ил .— Библиогр.: с.87 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-95.pdf>.
3	Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>.

б) дополнительная литература:

№ п/п	Источник
4	Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.
5	Теоретические основы компьютерной безопасности (учебное пособие для ВУЗов) / П.Н. Девянин [и др.]. – М.: Радио и связь, 2000 – 192с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Ресурс
6	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
7	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
8	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012

* 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	Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>.

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

Для реализации учебного процесса используются:

1) ПО Microsoft в рамках подписок «Imagine»,ежегодные сублицензионные договоры № 56035/ВРН3739 и № 56036/ВРН3739 от 07.10.2016.

2) ПО в виде произвольной среды разработки на языке С++.

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) Мультимедийная лекционная аудитория (корп.1а, ауд. № 380) - ПК-Intel-G3420, рабочее место преподавателя: проектор, видеокоммутатор, специализированная мебель: доска меловая 1 шт., столы 31 шт., стулья 64 шт.; выход в Интернет, доступ к фондам учебно-методической документации и электронным изданиям.

2) Компьютерный класс (один из корп. 1а, ауд. № 291, 293, 295, 387, 381) - ПК-Intel-Core2/i3 14 шт., специализированная мебель: доска маркерная 1 шт., столы 14 шт., стулья 28 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)
ОК-6 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности	**знать:** современные достижения науки, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности;	Разделы 1-3	Устный опрос
	уметь: самостоятельно приобретать и использовать в практической деятельности новые знания и умения; расширять и углублять свое научное мировоззрение;	Разделы 1-4	Лабораторная работа 1-2
	владеть: информационными технологиями	Разделы 1-4	Лабораторная работа 1-2
ПК-8 Умение проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информационных систем, управление технологическими процессами, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство, транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая промыш-	**знать** теоретические основы моделей объектов различной профессиональной деятельности	Разделы 3-4	Контрольная работа по разделам дисциплины
	уметь проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности	Разделы 3-4	Лабораторная работа 1-2
	владеть навыками разработки и исследования теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информационных систем, управление технологическими процессами, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство,	Разделы 3-4	Контрольная работа по соответствующим разделам или тест

ленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоиформационные системы, лесной комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества	транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая промышленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоиформационные системы, лесной комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества		
ПК-10 Умение осуществлять моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований	**знать:** основы моделирования процессов и объектов	Разделы 1-4	Контрольная работа по разделам дисциплины
	уметь: осуществлять моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований	Разделы 1-4	Контрольная работа по разделам дисциплины
	владеть: навыками моделирования процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований	Разделы 1-4	Лабораторная работа 1-2
Промежуточная аттестация			Комплект КИМ

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 теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование и представление основных теоретических и практических результатов (теорем, алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3) умение связывать теорию 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 экспериментирования с компьютерными моделями алгоритмов обработки информации в среде Matlab в рамках выполняемых лабораторных заданий;

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

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 (нужное выбрать)

«зачтено» - 3-5 баллов

«не зачтено» - 2 балла.

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	Теоретические вопросы по темам/разделам дисциплины	Шкалы оценивания соответствует приведенной в разделе 3
4	Лабораторная работа	Содержит 3 лабораторных заданий	При успешно выполнении работы ставится оценка зачтено, в противном случае ставится оценка не зачтено.
5	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 3

19.3.2. Примерный перечень вопросов к зачету

№	Вопросы к итоговой аттестации (зачет – 2 семестр)
1	Алгоритмы симметричного шифрования, сеть Фейстеля
2	Криптосистемы с открытым ключом, однонаправленные функции
3	Система распределения ключей Диффи-Хеллмана
4	Электронная цифровая подпись
5	Однонаправленные хэш-функции
6	Программные датчики ПСП чисел
7	Гаммирование, линейный регистр сдвига с обратной связью
8	Частотный, дифференциальный, линейный криптоанализ
9	Криптография с использованием эллиптических кривых

10	Квантовая криптография
11	Базовые отображения стеганографического преобразования данных, методы цифровой стеганографии
12	Стеганографическое скрытие данных в частотной области контейнера, методы кодирования с расширением спектра
13	Цифровые водяные знаки
14	Противодействие изучению исходного кода, методы обфускации
15	Средства отладки и взлома программ; уязвимости распространенных методов защиты ПО

19.3.3. Пример задания для выполнения лабораторной работы

Лабораторная работа №2
«**Алгоритмы стеганографического скрытия данных в частотной области**»

Цель работы:
Исследовать алгоритмы стеганографического скрытия данных в частотной области.

Форма контроля: отчёт в электронном виде
Количество отведённых аудиторных часов: 4

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.06 Информационная безопасность

Форма обучения Очное

Вид контроля Зачёт

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Алгоритмы симметричного шифрования, сеть Фейстеля
2. Алгоритмы стеганографического скрытия данных в пространственной области контейнера

Преподаватель _____ Е.Ю. Митрофанова

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.