МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный университет»

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«31» августа 2020 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.12 Информационная безопасность

1. Шифр и наименование направления подготовки/специальности:
02.03.01 Математика и компьютерные науки

2. Профиль подготовки/специализации: квантовая теория информации, распределенные системы и искусственный интеллект

3. Квалификация (степень) выпускника: бакалавр

4. Форма образования: очная

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

6. Составители программы:
Иванков Александр Юрьевич, к.ф.-м.н. ассистент

7. **Рекомендована:**
Научно-методическим советом ФКН, протокол №7 от 31 августа 2020г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2021-2022 **Семестр(-ы):** 8

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.

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	
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	**знать:** методы и средства защиты конфиденциальности информации, методы контроля целостности и аутентификации данных, принципы организации скрытых каналов передачи информации; **уметь:** разрабатывать и применять на практике специализированные программные средства в интересах обеспечения безопасности, целостности, секретности данных; **владеть:** практическими навыками разработки и применения специализированных программных средств, предназначенных для обеспечения безопасности, целостности и секретности данных.

12. Объем дисциплины в зачетных единицах/час — 3/108.
Форма промежуточной аттестации: *экзамен*.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)			
	Всего	По семестрам		
		№ сем.8	№ сем.	Итого
Аудиторные занятия	54	54		54
в том числе: лекции	36	36		36
практические	-	-		-
лабораторные	18	18		18
Самостоятельная работа	18	18		18
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*	36	36		36
Итого:	108	108		108

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. Криптографические преобразования. Симметричные и ассиметричные криптосистемы. Использование криптографических средств для решения задач идентификация и аутентификация. Электронная подпись (ЭП). Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных. Датчики случайных чисел. Гаммирование. Криптография с использованием эллиптических кривых. Шифрование, обмен ключами, ЭП на основе эллиптических кривых. Квантовая криптография. 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. Цифровые водяные знаки (ЦВЗ). Виды реализации, практические области применения. Перспективные направления развития стеганографических методов. Принципы стегоанализа. Визуальный, статистический, универсальный стегоанализ.
		2. Практические занятия
2.1	нет	
		3. Лабораторные работы
3.1	Криптографические методы защиты информации	1. Практическое изучение работы алгоритмов блочного симметричного шифрования. 2. Практическое изучение алгоритмов хеширования. 3. Практическое изучение работы асимметричных алгоритмов шифрования.
3.2	Стеганографические методы защиты информации	4. Изучение алгоритмов стеганографического скрытия данных в пространственной и частотной области контейнеров (на примере цифровых изображений).

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	12	8	8	28
2	Криптографические методы защиты информации	14	8	8	30
3	Стеганографические методы защиты информации	10	2	2	14
	Итого:	36	18	18	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 проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

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	Рябко, Борис Яковлевич. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов .— 2-е изд. — Москва : Горячая линия - Телеком, 2013 .— 232 с. : ил., табл. — Библиогр.: с.225-229.
2	*Круглов И.А. Введение в теоретико-числовые методы криптографии / И.А. Круглов [и др.]. – СПб: Лань, 2011. – 400 с.*
3	*Дрюченко, Михаил Анатольевич. Методы и алгоритмы стеганографического скрытия и создания цифровых водяных знаков : учебное пособие / М.А. Дрюченко, Е.Ю. Митрофанова ; Воронеж. гос. ун-т .— Воронеж : Издательский дом ВГУ, 2019 .— 144 с. : ил., цв. ил. — ISBN 978-5-9273-2747-8.*

б) дополнительная литература:

№ п/п	Источник
4	*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.*
5	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>.
6	Шифрование. Кодирование. Архивация [Электронный ресурс] : учебно-методическое пособие для вузов : [для студ. 2-го к. днев. отд-ния фак. приклад. математики, информатики и механики ; для специальности 080500.62 -Бизнес-информатика] / Воронеж. гос. ун-т ; сост. Ю.А. Крыжановская .— Электрон. текстовые дан. — Воронеж : Издательско-полиграфический центр Воронежского государственного университета, 2013 .— Загл. с титула экрана .— Свободный доступ из интрасети ВГУ .— Текстовый файл .— Windows 2000; Adobe Acrobat Reader .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m13-218.pdf>.
7	Чмора А.Л. Современная прикладная криптография (учебное пособие для ВУЗов) / А.Л. Чмора. – М.: Гелиос АРВ, 2002 – 244с.

в)информационные электронно-образовательные ресурсы (официальные ресур-

сы интернет)*:

№ п/п	Ресурсы Интернет
8	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
9	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
10	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	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.

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

Для реализации учебного процесса используется:

ПО Microsoft в рамках подписок «Imagine»,ежегодные сублицензионные договоры № 56035/BPH3739 и № 56036/BPH3739 от 07.10.2016.

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

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. № 479), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, микрофон, аудиосистема, специализированная мебель: доски меловые 2 шт., столы 60 шт., лавки 30 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385),ПК-Intel-i3 16 шт., специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 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 (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	**знать:** методы и средства защиты конфиденциальности информации,	Разделы 1-3 Основные теоретические аспекты ин-	Контрольная работа по соответствующим разделам. Тест по

профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	методы контроля целостности и аутентификации данных, принципы организации скрытых каналов передачи информации	формационной безопасности. Криптографические методы защиты информации. Стеганографические методы защиты информации.	разделам дисциплины
	уметь: разрабатывать и применять на практике специализированные программные средства в интересах обеспечения безопасности, целостности, секретности данных	Разделы 2-3 Криптографические методы защиты информации. Стеганографические методы защиты информации.	Лабораторные работы 1-4
	владеть: практическими навыками разработки и применения специализированных программных средств, предназначенных для обеспечения безопасности, целостности и секретности данных	Разделы 2-3 Криптографические методы защиты информации. Стеганографические методы защиты информации.	Лабораторные работы 1-4
Промежуточная аттестация			Комплект 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

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;

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 в рамках выполняемых лабораторных заданий.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	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

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	Шкала оценивания соответствует приведенной в разделе 19.2
3	Лабораторная работа	Содержит 4 лабораторных заданий, предусматривающих разработку и тестирование криптографических и стеганографических алгоритмов .	При успешном выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
4	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 19.2

19.3.2. Примерный перечень вопросов к экзамену

№	Вопросы к экзамену
1	Угрозы информационной безопасности, модели нарушителей
2	Общие требования к построению надежной системы защиты

3	Предметная область криптографии
4	Алгоритмы симметричного шифрования, сеть Фейстеля
5	Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
6	Криптосистемы с открытым ключом, однонаправленные функции
7	Система распределения ключей Диффи-Хеллмана
8	Однонаправленные хэш-функции
9	Электронная подпись
10	Программные датчики ПСП чисел
11	Гаммирование, линейный регистр сдвига с обратной связью
12	Криптография с использованием эллиптических кривых
13	Квантовая криптография
14	Принципы работы криптоаналитических алгоритмов.
15	Предметная область стеганографии
16	Стеганографическое скрытие данных в пространственной области контейнера
17	Стеганографическое скрытие данных в частотной области контейнера, методы кодирования с расширением спектра
18	Статистические и структурные методы скрытия информации
19	Цифровые водяные знаки
20	Стегоанализ. Визуальный, статистический, универсальный стегоанализ.
21	Приемы защиты исходных кодов программ. Обфускация кода.

19.3.3. Пример задания для выполнения лабораторной работы

Лабораторная работа № 3

«Изучение работы асимметричных алгоритмов шифрования»

Цель работы

Изучение работы асимметричных алгоритмов шифрования на примере алгоритма RSA.

Форма контроля

Опрос в устной форме по исходному коду и результатам работы реализованной программы.

Количество отведённых аудиторных часов - 3

Содержание работы

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Провести дешифрование текста, зашифрованного алгоритмом RSA, на основе известного открытого ключа K_p и шифрованного текста C.

$$K_p = \{n=471090785117207;\ e=12377\}$$

$$C = 31499911228106520536170634151732 1987491098667$$

Примеры контрольных вопросов:

1. На чем основывается надежность алгоритма RSA?
2. Какие преобразования лежат в основе криптосистем с открытым ключом?

19.3.4. Пример заданий теста по разделам дисциплины

1	Режим шифрования, сохраняющий статистические особенности открытого текста *а) Cipher block chaining (CBC)* *б) Cipher feed back (CFB)* *в) Electronic code book (ECB)* *г) Counter mode (CTR)*	
2	Какой тип избыточности чаще всего используется в стегоалгоритмах *а) статистическая* *б) психовизуальная* *в) спектральная* *г) временная*	

3	Длительность действия криптографического ключа зависит от *а) длины ключа* *б) частоты использования ключа* *в) объема и характера шифруемой информации* *г) величины потенциального ущерба, связанного с компрометацией ключа* *д) используемого криптоалгоритма*	
4	Установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем *а) идентификация* *б) авторизация* *в) аутентификация* *г) контроль целостности*	
5	Цифровые водяные знаки – это *а) уникальные метки, скрытно встраиваемые в цифровой контейнер с целью контроля его незаконного копирования и тиражирования* *б) метки, скрытно встраиваемые в цифровой контейнер с целью защиты авторских прав и контроля его использования* *в) видимые или невидимые пиктограммы, добавляемые на защищаемые изображения или видео-файлы*	
…	…	

19.3.5. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2020

Направление подготовки / специальность 02.03.01 Математика и компьютерные науки

Дисциплина Б1.В.12 Информационная безопасность

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB).
2. Цифровые водяные знаки.

Преподаватель _____ Иванков А.Ю.

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.