Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.42 Информационная безопасность и защита информации

1. Код и наименование направления подготовки/специальности:

09.03.04 Программная инженерия

2. Профиль подготовки/специализация:

Информационные системы и сетевые технологии

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

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:

№7 от 31.08.20

8. Учебный год:

2023-2024

9.Цели и задачи учебной дисциплины:

Изучение теоретических основ информационной безопасности, защиты информации от несанкционированного доступа, обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, вопросов защиты исходных и байт кодов программ; овладение практическими навыками применения методов криптографии, стеганографии, получение профессиональных компетенций в области современных технологий защиты информации.

Основные задачидисциплины:

- 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:

Входит в блок обязательные дисциплины Б1.О.

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):

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-1 Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1 Знает основы математики, физики, вычислительной техники и программирования.	Знать основные теоретические и практические аспекты обеспечения информационной безопасности
ОПК-1 Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.2 Умеет решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.	Уметь применять на практике теоретические знания в области криптографии и стеганографии. Владеть практическими навыками разработки и применения в профессиональной деятельности криптографических и стеганографических алгоритмов.

12. Объем дисциплины в зачетных единицах/час:

4/144

Форма промежуточной аттестации:

Экзамен

13. Виды учебной работы

Вид учебной работы	Семестр 8	Всего
Аудиторные занятия	60	60
Лекционные занятия	48	48
Практические занятия		0
Лабораторные занятия	12	12

Вид учебной работы	Семестр 8	Всего
Самостоятельная работа	48	48
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	144	144

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Основы государственной информационной политики и информационной безопасности Российской Федерации	Лекции по разделу Понятие национальной безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации. Государственная информационная политика. Информационные ресурсы. Проблемы информационной войны. Проблемы информационной безопасности в сфере государственного и муниципального управления.	Создан электронный курс, размещены материалы к лекции.
2	Информационная безопасность автоматизированных систем	Лекции по разделу Современная постановка задачи защиты информации. Организационно-правовое обеспечение, информационной безопасности. Информационные системы. Угрозы информации. Методы и модели оценки уязвимости информации.	Создан электронный курс, размещены материалы к лекции.
3	Методы и модели оценки уязвимости информации	Лекции по разделу Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита».	Создан электронный курс, размещены материалы к лекции.
4	Рекомендации по использованию моделей оценки уязвимости информации	Лекции по разделу Рекомендации по использованию моделей оценки уязвимости информации	Создан электронный курс, размещены материалы к лекции.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
5	Методы определения требований к защите информации	Лекции по разделу Методы определения требований к защите информации	Создан электронный курс, размещены материалы к лекции.
6	Функции и задачи защиты информации	Лекции по разделу Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации	Создан электронный курс, размещены материалы к лекции.
7	Стратегии защиты информации	Лекции по разделу Стратегии защиты информации.	Создан электронный курс, размещены материалы к лекции.
8	Способы и средства защиты информации	Лекции по разделу Способы и средства защиты информации.	Создан электронный курс, размещены материалы к лекции.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
9	Криптографические методы защиты информации	Лекции по разделу Требования к криптосистемам. Основные алгоритмы шифрования. Цифровые подписи. Криптографические хеш-функции. Криптографические генераторы случайных чисел. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Цифровые водяные знаки (ЦВЗ), виды реализации, практические области применения. Лабораторные занятия по разделу 1. Практическое изучение работы алгоритмов блочного симметричного шифрования. 2. Изучение криптографических генераторов случайных чисел. 3. Практическое изучение работы асимметричных алгоритмов шифрования. 4. Изучение частотных характеристик текстовых сообщений. 5. Изучение алгоритмов стеганографического скрытия данных в пространственной и частотной области контейнеров (на примере цифровых изображений). 6. Практическое изучение принципов и методов стегоанализа (на примере визуального и статистического стегоанализа цифровых изображений).	Создан электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ.
10	Архитектура систем защиты информации	Лекции по разделу Требования к архитектуре СЗИ. Построение СЗИ. Ядро системы защиты информации. Ресурсы системы защиты информации.	Создан электронный курс, размещены материалы к лекции.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Основы государственной информационной политики и информационной безопасности Российской Федерации	8			4	12
2	Информационная безопасность автоматизированных систем	4			4	8
3	Методы и модели оценки уязвимости информации	4			4	8
4	Рекомендации по использованию моделей оценки уязвимости информации	2			4	6
5	Методы определения требований к защите информации	2			4	6
6	Функции и задачи защиты информации	4			4	8
7	Стратегии защиты информации	4			4	8
8	Способы и средства защиты информации	4			4	8
9	Криптографические методы защиты информации	12		12	12	36
10	Архитектура систем защиты информации	4			4	8
		48	0	12	48	108

14. Методические указания для обучающихся по освоению дисциплины

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 переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

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

№ п/п	Источник
1	Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499170
2	Баранова, Елена Константиновна. Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330.

б) дополнительная литература:

№ п/п	Источник
1	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>.
2	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>.
3	Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.
4	*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	Источник
1	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).*
2	*Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)*
3	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

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Основы информационной безопасности [Электронный ресурс] : учеб. пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов .— М. : Горячая линия – Телеком, 2011 .— 559 с. : ил. — ISBN 5-93517-292-5 .— ISBN 978-5-93517-292-5 .— Режим доступа: https://rucont.ru/efd/202786.

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 подписки "Imagine/Azure Dev Tools for Teaching",
договор №3010-16/96-18 от 29 декабря 2018г.
2. ПО MATLAB Classroom ver. 7.0, 10 конкурентных бессрочных лицензий на каждый,
компоненты: Matlab, Simulink, Stateflow, 1 тулбокс, N 21127/VRN3 от 30.09.2011 (за счет проекта ЕК TEMPUS/ERAMIS).
3. ПО Матлаб в рамках подписки "Университетская лицензия на программный
комплекс для ЭВМ - MathWorks, Headcount – 25 ": лицензия до 31.01.2022,
сублицензионный контракт 3010-07/01-19 от 09.01.19.
4.При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

18. Материально-техническое обеспечение дисциплины:

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. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.	ОПК-1	ОПК-1.1	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
2	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.	ОПК-1	ОПК-1.2	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

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.

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- Устный опрос на практических занятиях
- Контрольная работа по теоретической части курса
- Лабораторные работы

Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос на практических занятиях	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 20.2
3	Лабораторная работа	Содержит 5 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.

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.

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

$$C = 31499911228106520536170634151732198749109866 7$$

Примеры контрольных вопросов:

1. На чем основывается надежность алгоритма RSA?

2. Какие преобразования лежат в основе криптосистем с открытым ключом?

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.
Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице ниже.
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.
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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	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. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2020

Направление подготовки / специальность 09.03.04 Программная инженерия

Дисциплина Б1.О.42 Информационная безопасность и защита информации

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 _____ А.Ю. Иванков

Примерный перечень вопросов к экзамену

№	Содержание
1	Основы государственной информационной политики и информационной безопасности Российской Федерации
2	Угрозы информационной безопасности, модели нарушителей
3	Методы и модели оценки уязвимости информации
4	Рекомендации по использованию моделей оценки уязвимости информации
5	Функции и задачи защиты информации
6	Предметная область криптографии
7	Алгоритмы симметричного шифрования, сеть Фейстеля
8	Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
9	Криптосистемы с открытым ключом, однонаправленные функции
10	Однонаправленные хэш-функции
11	Электронная подпись
12	Программные датчики ПСП чисел
13	Принципы работы криптоаналитических алгоритмов.
14	Предметная область стеганографии
15	Стеганографическое скрытие данных в пространственной области контейнера
16	Стеганографическое скрытие данных в частотной области контейнера, методы кодирования с расширением спектра
17	Статистические и структурные методы скрытия информации
18	Цифровые водяные знаки
19	Стегоанализ. Визуальный, статистический, универсальный стегоанализ.
20	Архитектура систем защиты информации
21	Общие требования к построению надежной системы защиты