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

УТВЕРЖДАЮ
декан факультета прикладной математики, информатики и механики
А. И. Шашкин
24.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.45 Методы и средства криптографической защиты информации

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Математические методы защиты информации

3. Квалификация (степень) выпускника:

Специалист по защите информации

4. Форма обучения:

очная

5. Кафедра, отвечающая за реализацию дисциплины:

ERP-систем и бизнес-процессов

6. Составители программы:

Степанец Юлия Александровна , к.т.н., доцент кафедры ERP-систем и бизнес-процессов

7. Рекомендована:

научно-методическим советом факультета ПММ от 15.06.2021 протокол № 10

_____

отметки о продлении вносятся вручную)

8. Учебный год: 2021/2022 **Семестр(ы):** 7

9. Цели и задачи учебной дисциплины

Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и средств, а также примеров реализации этих методов на практике.

Задачи дисциплины - дать основы: системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов разработки шифров; математических методов, используемых в криптографии.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК-10.1	Знает основные задачи, решаемые криптографическими методами.	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Владение: навыками использования типовых криптографических алгоритмов; методами анализа безопасности компьютерных систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости информации в компьютерных системах.
		ОПК-10.2	Знает математические модели шифров, подходы к оценке их стойкости.	
		ОПК-10.3	Знает зарубежные и российские криптографические стандарты.	
		ОПК-10.4	Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами.	
		ОПК-10.5	Умеет применять математические методы при исследовании криптографических алгоритмов.	
		ОПК-10.6	Владеет навыками использования типовых криптографических алгоритмов.	

12. Объем дисциплины в зачетных единицах/час— 3/108.

Форма промежуточной аттестации - зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			7			
Аудиторные занятия	64		64			
в том числе: лекции	34		34			
Практические						
Лабораторные	34		34			
Самостоятельная работа	40		40			
Итого:	108		108			
Форма промежуточной аттестации	Зачет с оценкой		Зачет с оценкой			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Основные понятия. Терминология.	Информация, сообщения, сигналы, криптосистемы.	Криптографические методы защиты информации (10.05.01)
1.2	Математические основы криптографии	Теоремы о простых числах. Алгоритм Евклида. Функция Эйлера. Свойства модулярной арифметики. Теорема Эйлера. Вычисление обратных величин. Расширенный алгоритм Евклида	
1.3	Общие вопросы информационной безопасности	Основы классической криптографии. Классификация криптографических методов. Угрозы информации. Атаки на криптосистемы.	
1.4	Особенные системы криптографии.	Классы стойкости. Идеальные криптосистемы.	
1.5	Системы шифрования	Шифр RSA. Шифр Эль Гамаля. Цифровая подпись	
2. Лабораторные работы			
2.1	Работа с криптографическими средствами защиты	ГОСТ Р 34.12-2015, «Магма». ГОСТ Р 34.12-2015, «Кузнечик». Криптосистема Эль Гамаля.	Криптографические методы защиты информации (10.05.01)

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоя-тельная работа	Всего
1.1	Основные понятия. Терминология.	6	0	4	10
1.2	Математические основы криптографии	8	0	12	20
1.3	Общие вопросы информационной безопасности	8	10	8	26
1.4	Особенные системы криптографии	8		4	12
1.5	Системы шифрования	4	4	4	12
2.1	Работа с криптографическими средствами защиты	0	20	8	28
	Итого:	34	34	40	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1	Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111097 (дата обращения: 5.04.2019). — Режим доступа: для авториз. пользователей.
2	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, [б. г.]. — Часть 1 — 2017. — 64 с. — ISBN 978-5-7641-1053-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111765 (дата обращения: 10.02.2020). — Режим доступа: для авториз. пользователей.
3	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2018 — Часть 2 — 2018. — 63 с. — ISBN 978-5-7641-1215-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/138103 (дата обращения: 10.02.2020). — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
4	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. — Самара : ПГУТИ, 2019. — 68 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223319 (дата обращения: 20.01.2020). — Режим доступа: для авториз. пользователей.
5	Салий В. Н. Криптографические методы и средства защиты информации / В. Н. Салий. – 2010. (URL:http://www.sgu.ru/files/nodes/11017/V.N._Saliy._Kriptograficheskie_metody_i_sredstva_zashchity_informacii.doc) (дата обращения: 12.05.2019)

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
6	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
7	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
8	Криптографические методы защиты информации (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению проекта. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Криптографические методы защиты информации», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном. Аудитория для практических занятий должна быть оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном.

Программное обеспечение:
- ОС Windows 8 (10),
- интернет-браузер (Goolge Chrome, Mozilla Firefox).
- ПО Adobe Reader;
- пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, МойОфис, LibreOffice);
- ПО Maple или аналогичная среда визуального программирования.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.1	Основные понятия. Терминология.	ОПК-10	ОПК-10.1-3	Контрольная работа
1.2	Математические основы криптографии	ОПК-10	ОПК-10.1-3	Контрольная работа
1.3	Общие вопросы информационной безопасности	ОПК-10	ОПК-10.1-3	Контрольная работа
1.4	Особенные системы криптографии	ОПК-10	ОПК-10.1-3	Контрольная работа
1.5	Системы шифрования	ОПК-10	ОПК-10.2, 5	Контрольная работа
2.1	Работа с криптографическими средствами защиты	ОПК-10	ОПК-10.4-6	Лабораторные работы
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- контрольная работа,
- лабораторные работы.

Перечень контрольных работ

1. Протоколы и их классификация.
2. Обмен ключами средствами симметричной криптографии.
3. Протоколы открытого распределения ключей.
4. Протоколы передачи секретного ключа по открытому каналу.
5. Аутентификация при входе в систему.
6. Вручение битов на хранение.
7. Бросание монеты по телефону.
8. Доказательство с нулевым разглашением.
9. Схемы аутентификации.
10. Методы разделения секрета.
11. Скрытый канал связи.
12. Мысленный покер.
13. Мысленный покер с тремя игроками.

Технология проведения

Студент выбирает вариант задания, ориентируясь на номер зачетки. Студент выполняет предложенное преподавателем задание, представляет его в письменном виде, при необходимости, комментирует выполненные действия, анализирует и интерпретирует результаты. В курсе предусмотрена одна контрольная работа (одна тема из списка).

Критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Все задания контрольной работы выполнены, арифметических и логических ошибок нет, показано владение терминологией.	Повышенный уровень	Отлично
Все задания контрольной работы выполнены, но имеют место быть незначительные ошибки (арифметические, логические, в терминологии).	Базовый уровень	Хорошо
Не все задания контрольной работы выполнены и имеют место быть несущественные ошибки (арифметические, логические, в терминологии).	Пороговый уровень	Удовлетвори-тельно
Задания контрольной работы не выполнены или имеют место быть существенные ошибки (арифметические, логические, в терминологии).	–	Неудовлетво-рительно

Перечень лабораторных работ

Лабораторная работа №1 Тема: ГОСТ Р 34.12-2015, «Магма»

Теоретические сведения
1. Схема Фейстеля.
2. Операции по модулю.
3. Нелинейное преобразование.
4. Преобразование ключа.

Практическая часть
Обучение на основе компьютерной программы

Лабораторная работа №2 Тема: ГОСТ Р 34.12-2015, «Кузнечик».
Теоретические сведения
1. Простые и расширенные поля Галуа.
2. Преобразование ключа..
3. SP-сети.

Практическая часть
1. Реализация и исследование стандарта.
2. Подготовка и защита отчёта по лабораторной работе.

Лабораторная работа №3 Тема: Криптосистема Эль Гамаля.
Теоретические сведения
1. Понятие дискретного алгоритма.
2. Криптостойкость.
3. Сравнение с RSA.

Практическая часть
1. Обучение на основе компьютерной программы.
2. Подготовка и защита отчёта по лабораторной работе.

Технология проведения
Все лабораторные работы обязательны для выполнения. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания
- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания и они правильные, даны пояснения);

- оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету.

Перечень вопросов к зачету (КИМ №1)

1. Что такое информационная безопасность?
2. В чем заключаются постулаты информационной безопасности?
3. Чем достигается обеспечение безопасности?
4. Что такое способы защиты информации?
5. В чем проявляются угрозы информации?
6. Что такое инженерно-техническая защита информации?
7. Что такое цена и ценность информации?
8. В чем состоят цели защиты информации?
9. Что подразумевается под эффективностью защиты информации?
10. Что такое система безопасности?
11. Охарактеризуйте физические системы защиты информации.
12. На какие классы разделяются инженерно-технические средства защиты информации?
13. Что такое криптология, криптограмма, криптография, криптоанализ?
14. Дайте определение криптосистемы (шифра).
15. В чем состоит основная идея шифрования данных?
16. В чем различие и в чем сходство шифрования и кодирования?
17. В чем различие терминов "дешифрование" и "расшифрование"?
18. Для решения каких задач используется кодирование информации?
19. Охарактеризуйте методы симметричного шифрования данных.
20. Опишите схему симметричного шифрования информации.
21. Приведите упрощённую схему алгоритма шифрования/расшифрования DES?
22. Что такое криптостойкость?
23. Каковы количественные характеристики криптостойкости?
24. Каким образом классифицируется инженерно-техническая защита информации?
25. Перечислите возможные виды утечек информации.
26. Сформулируйте основные законы модулярной арифметики.
27. Что представляет собой функция Эйлера?
28. В чем состоит теорема Эйлера?
29. Охарактеризуйте основные способы нахождения обратных по модулю величин.
30. Что такое криптосистема Эль Гамаля?

Критерии оценки ответов на вопросы зачета

Для оценивания результатов обучения на зачете используется – 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.

Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле:

$$Q_{пром\_ат} = 0{,}4Q_{КР} + 0{,}6Q_{зач}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

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-7 Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Владеть навыками работы с программными средствами общего и специального назначения	Раздел 16. Работа с криптографическими средствами защиты	Лабораторные работы
ПК-2 Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищённости информации в компьютерных системах, составлятъ научные отчёты, обзоры по результатам выполнения исследований.	Знать принципы оценки защищённости информации в компьютерных системах	Раздел 1. Информация, сообщения, сигналы, криптосистемы.	Устный опрос.
	Уметь составлять научные отчёты и обзоры по результатам выполнения исследований.	Раздел 8. Основы классической криптографии.	Отчёты по лабораторным работам.
	Владеть методами оценки защищённости информации в компьютерных системах.	Раздел 10 Атаки на криптосистемы. Раздел 11 Угрозы информации.	Устный опрос, защита лабораторных работ.
ПК-3 Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.	Знать методы анализа безопасности компьютерных систем.	Раздел 1. Информация, сообщения, сигналы, криптосистемы.	Устный опрос.
	Уметь анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.	Раздел 8. Основы классической криптографии.	Отчёты по лабораторным работам.
	Владеть методами анализа безопасности компьютерных систем.	Раздел 10 Атаки на криптосистемы. Раздел 11 Угрозы информации.	Устный опрос, защита лабораторных работ.
ПК-10 Способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищённые операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной	Знать методы реализации систем защиты информации и действующих политик безопасности в компьютерных системах.	Раздел 1. Информация, сообщения, сигналы, криптосистемы.	Устный опрос.
	Уметь оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах.	Раздел 8. Основы классической криптографии.	Отчёты по лабораторным работам.

защиты, средства криптографической защиты информации.	Владеть методиками оценки эффективности реализации систем защиты информации.	Раздел 10 Атаки на криптосистемы. Раздел 11 Угрозы информации. Раздел 14 Идеальные криптосистемы	Устный опрос, защита лабораторных работ.
Промежуточная аттестация			Комплект 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.

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и результаты выполнения лабораторных работ, позволяющие оценить степень сформированности умений и навыков.

Для оценивания результатов обучения на экзамене используется шкала из таблицы ниже.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Компетенция	Показатель сформированности компетенции	Шкала и критерии оценивания уровня освоения компетенции			
		5	4	3	2
ОПК-7 Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения	Владеть навыками работы с программными средствами общего и специального назначения	Сформированные навыки	Успешные навыки, но содержащие отдельные пробелы	Успешные, но не системные навыки	Фрагментарные навыки или отсутствие навыков
ПК-2. способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищённости информации в компьютерных системах, составлятъ научные отчёты, обзоры по результатам выполнения исследований.	Знать принципы оценки защищённости информации в компьютерных системах	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Уметь составлять научные отчёты и обзоры по результатам выполнения исследований.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеть методами оценки защищённости информации в компьютерных системах.	Сформированные навыки	Успешные навыки, но содержащие отдельные пробелы	Успешные, но не системные навыки	Фрагментарные навыки или отсутствие навыков
ПК-3. способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.	Знать методы анализа безопасности компьютерных систем.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Уметь анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений

	компьютерной безопасности.				
	Владеть методами анализа безопасности компьютерных систем.	Сформированные навыки	Успешные навыки, но содержащие отдельные пробелы	Успешные, но не системные навыки	Фрагментарные навыки или отсутствие навыков
ПК-10. способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищённые операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.	Знать методы реализации систем защиты информации и действующих политик безопасности в компьютерных системах.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Уметь оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеть методиками оценки эффективности реализации систем защиты информации.	Сформированные навыки	Успешные навыки, но содержащие отдельные пробелы	Успешные, но не системные навыки	Фрагментарные навыки или отсутствие навыков

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 Примеры контрольных вопросов и заданий:

14. Перечислите режимы работы обучающей программы DES Tutorial.
15. Какова длина ключа алгоритма DES?
16. Что означает выражение "конкатенация битовых строк ассоциативна"?
17. Что представляет собой операция по модулю два?
18. Что такое криптология, криптограмма, криптография, криптоанализ?
19. В чем состоит основная идея шифрования данных?
20. В чем различие и в чем сходство шифрования и кодирования?
21. В чем различие терминов "дешифрование" и "расшифрование"?
22. Для решения каких задач используется кодирование информации?
23. Приведите алгоритм перехода от двоичной системы счисления к десятичной и наоборот.
24. Приведите алгоритм перехода от шестнадцатеричной системы счисления к десятичной и наоборот.
25. Опишите схему симметричного шифрования информации.
26. Что является аргументом функции шифрования F?
27. Приведите упрощённую схему алгоритма шифрования DES?
28. Приведите упрощённую схему алгоритма расшифрования DES?
29. Приведите схему реализации функции шифрования F.

30. Опишите алгоритм реализации "функций преобразования S(i).
31. Что означает фраза "процесс расшифрования данных является инверсным по отношению к процессу шифрования"?
32. Какие преобразования используются при реализации функции шифрования F(R,K)?
33. Какие биты ключа не влияют на шифрование? Для каких целей могут использоваться эти биты?
34. Расшифруйте сокращение "DES".
35. Почему (и какие?) программа добавляет символы к строкам, размеры которых не кратны восьми?
36. Для какой цели была разработана программа "DES Tutorial"?
37. Что такое криптостойкость? Каковы количественные характеристики криптостойкости?
38. Опишите алгоритм получения 48-битовых ключей K(i).
39. Докажите, что таблица 2 ("конечная перестановка") является обратной по отношению к таблице 1 ("начальная перестановка").
40. Опишите упрощённую схему асимметричного шифрования.
41. Какова максимальная длина открытого текста в программе DES? Подтвердите экспериментально.
42. В чем разница между закрытой, секретной и конфиденциальной информацией?
43. Что такое цена и ценность информации?
44. Что подразумевается под эффективностью защиты информации?
45. Что такое система безопасности?
46. В чем заключаются постулаты безопасности?
47. Чем достигается обеспечение безопасности?
48. Что такое способы защиты информации?
49. Что такое пространственное, временное, структурное и энергетическое скрытие информации?
50. В чем состоят цели защиты информации?
51. Охарактеризуйте физические системы защиты информации.
52. На какие классы разделяются инженерно-технические средства защиты информации?
53. В чем проявляются угрозы информации?
54. Что такое инженерно-техническая защита информации?
55. Каким образом классифицируется инженерно-техническая защита информации?
56. Что такое информационная безопасность?
57. Что такое защита информации?
58. Перечислите возможные виды утечек информации.
59. Охарактеризуйте методы симметричного шифрования данных.
60. Что такое отношение сравнимости?
61. Что называется полным набором вычетов по модулю n (n – целое число)?
62. Сформулируйте основные законы модулярной арифметики.
63. Что представляет собой функция Эйлера?
64. В чем состоит теорема Эйлера?
65. Сформулируйте малую теорему Ферма.
66. Как найти функцию Эйлера $\varphi(\prod_{i=1}^{n} p_i^{r_i})$, где p_i – простые числа, n и r_i - натуральные числа?
67. Дайте определение величины, обратной целому числу a по модулю n.
68. Охарактеризуйте основные способы нахождения обратных по модулю величин.
69. Что такое дискретный логарифм? В чем заключается проблема дискретного логарифмирования?
70. Дайте определение криптосистемы (шифра).
71. Что такое криптосистема Эль Гамаля?

19.3.2 Перечень заданий для контрольных работ

ГОСТ Р 34.12-2015, «Магма», «Кузнечик»; криптосистема Эль Гамаля.

19.3.3 Перечень лабораторных работ

Лабораторная работа №1 Тема: ГОСТ Р 34.12-2015, «Магма»

Теоретические сведения
1. Схема Фейстеля.
2. Операции по модулю.
3. Нелинейное преобразование.
4. Преобразование ключа.

Практическая часть
Обучение на основе компьютерной программы

Лабораторная работа №2 Тема: ГОСТ Р 34.12-2015, «Кузнечик».
Теоретические сведения
4. Простые и расширенные поля Галуа.
5. Преобразование ключа..
6. SP-сети.

Практическая часть
1. Реализация и исследование стандарта.
2. Подготовка и защита отчёта по лабораторной работе.

Лабораторная работа №3 Тема: Криптосистема Эль Гамаля.
Теоретические сведения
1. Понятие дискретного алгоритма.
2. Криптостойкость.
3. Сравнение с RSA.

Практическая часть
3. Обучение на основе компьютерной программы.
4. Подготовка и защита отчёта по лабораторной работе.

19.3.5. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
заведующий кафедрой
ERP-систем и бизнес-процессов
_____ Й. Беккер
подпись, расшифровка подписи
_03.06.2020

Направление подготовки / специальность ___10.05.01_Компьютерная безопасность
шифр, наименование
Дисциплина_Криптографические методы защиты информации

Вид контроля зачет с оценкой

Контрольно-измерительный материал №_1_

1. Расширенный алгоритм Эвклида.
2. Теорема Эйлера.
3. SP-сети в стандарте ГОСТ Р 34.12-2015

Преподаватель _____ .____
подпись *расшифровка подписи*

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; лабораторные работы; тестирования. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков по вопросам компьютерной безопасности.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.