МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института энергетики, информационных технологий и управляющих систем
_____ Белоусов А.В.
«___» _____ 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Методы и средства криптографической защиты информации

направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы:

Безопасность открытых информационных систем

Квалификация

Специалист по защите информации

Форма обучения

очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и автоматизированных систем

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 №1457
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: к.т.н., доцент _____ (Сергиенко Е.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

«14» 05 2021 г., протокол № 8

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем
(наименование кафедры/кафедр)

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

«14» 05 2021 г.

Рабочая программа одобрена методической комиссией института

«20» 05 2021 г., протокол № 9

Председатель к.т.н., доцент _____ (Семернин А.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Общепрофессиональные компетенции	ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	**Знать:** классические шифры, блочные и поточные шифры, симметричные и асимметричные шифры; **Уметь:** использовать симметричные и асимметричные шифры для закрытия информации с гарантированной стойкостью **Владеть:** навыками применения блочных и поточных шифров
		ОПК-10.2 Использует средства криптографической защиты информации при решении задач профессиональной деятельности	**Знать:** стандарты DES, AES, ГОСТ, алгоритмы RSA и Диффи-Хеллмана, принцип действия электронной подписи, криптографический протокол электронных денег. **Уметь:** генерировать ключи, выполнять обмен секретными ключами, использовать электронную подпись; методы ее конструирования. **Владеть:** навыками применения шифров на основе стандартов DES, AES, ГОСТ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Данная компетенция формируется следующими дисциплинами.

№	Наименования дисциплины
1.	Методы и средства криптографической защиты информации
2.	Математика криптографии
3.	Криптографические интерфейсы
4.	Квантовые вычисления и квантовая криптография
5.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.

Форма промежуточной аттестации: экзамен.

Вид учебной работы	Всего часов	Семестр № 6
Общая трудоемкость дисциплины, час	180	180
Контактная работа (аудиторные занятия), в т.ч.:	90	90
лекции	34	34
лабораторные	34	34
практические	17	17
групповые консультации в период теоретического обучения и промежуточной аттестации	5	5
контроль самостоятельной работы	-	-
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	90	90
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	-	-
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	54	54
Экзамен	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем

Курс 3 Семестр 6

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1	**Введение. Основные понятия криптографии**. Классические шифры: моноалфавитные и полиалфавитные шифры; шифры перестановки.	8	3	8	12
2	**Блочные и поточные шифры.** Шифры с симметричным ключом. Стандарты шифрования. Стандарты DES, AES, ГОСТ.	10	4	12	17
3	**Шифры с ассиметричным ключом.** Алгоритм RSA.	6	4	6	11

4	**Практические задачи криптографии.** Генерация ключей. Алгоритм Диффи-Хеллмана. Алгоритмы хеширования. Электронная цифровая подпись; методы ее конструирования. Электронные деньги.	10	6	8	14
	ВСЕГО	34	17	34	54

4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического занятия	К-во часов	К-во часов СРС
семестр № 6				
1	Введение. Основные понятия криптографии	Классические шифры	3	3
2	Блочные и поточные шифры	Шифр Виженера	4	4
3	Шифры с ассиметричным ключом	Стандарт шифрования DES Стандарт шифрования AES Алгоритм шифрования RSA	4	4
4	Практические задачи криптографии	Протокол Диффи–Хеллмана	6	5
		ИТОГО:	17	16
			ВСЕГО:	33

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
1.	Введение. Основные понятия криптографии	Аддитивные и мультипликативные шифры	8	8
		Аффинный шифр		
		Шифр Плейфера		
		Шифр Виженера		
2.	Блочные и поточные шифры	Стандарт шифрования DES. Основная функция DES	12	12
		Стандарт шифрования DES. Генерация ключей раунда		
		Стандарт шифрования DES. Режимы шифрования		
		Стандарт шифрования AES. Структура раунда		
		Стандарт шифрования AES. Расширение ключей		
		Стандарт шифрования AES. Шифрование и дешифрование		
3.	Шифры с ассиметричным ключом	Криптоалгоритм RSA и его применение	6	6
4.	Практические задачи криптографии	Алгоритмы криптографического хеширования	8	8
		Обмен секретными ключами		
		Обмен секретными ключами с тремя и более участниками		
		Криптографический протокол электронных денег		
		ИТОГО:	34	34
			ВСЕГО:	68

4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Не предусмотрено учебным планом

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1. Компетенция ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации	устный опрос, защита лабораторной работы, экзамен
ОПК-10.2 Использует средства криптографической защиты информации при решении задач профессиональной деятельности	собеседование, защита лабораторной работы, экзамен

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Введение. Основные понятия криптографии (ОПК-10.1)	Определите три цели безопасности Систематизация атак на конкретную информацию Услуги и механизмы информационной безопасности Математическая модель шифра. Примеры шифров. Принцип Керкхоффа. Основы криптоанализа. Традиционные шифры. Шифры подстановки (моноалфавитные шифры). Аддитивные, мультипликативные и аффинные шифры. Многоалфавитные шифры. Шифр Плейфера. Шифр Виженера. Шифр Хилла. Шифроблокнот. Шифры перестановки.
2.	Блочные и поточные шифры (ОПК-10.2)	Шифры потока и блочные шифры. Современные блочные шифры с симметричным ключом. Компоненты современного блочного шифра. Стандарт шифрования DES. Его свойства. Многократное применение DES. Стандарт шифрования AES. Его версии. Криптоанализ стандартов DES и AES. Режимы работы DES и AES. Шифры потока RC4 и A5/1.
3.	Шифры с ассиметричным ключом (ОПК-10.2)	Криптография с асимметричным ключом. Односторонние функции. Криптосистема RSA. Атаки на RSA. Криптосистемы Рабина и Эль-Гамаля Криптографические хеш-функции Алгоритмы SHA хеширования.

4.	Практические задачи криптографии (ОПК-10.2)	Проверка целостности сообщения. Установление подлинности сообщения. Понятие цифровой подписи. Схемы цифровой подписи. Установление подлинности объекта. Управление ключами. Протоколы Диффи-Хеллмана. Криптографический протокол электронных денег.

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Текущий контроль осуществляется в течение семестра в форме собеседования и устного опроса.

Собеседования и устные опросы направлены на проверку степени усвоения материала и понимания теоретических сведений, используемых в процессе выполнения работы. Примерные перечень вопросов для контроля знаний приведен в таблице:

№ п/п	Наименование раздела дисциплины	Контрольные вопросы
1	Введение. Основные понятия криптографии (ОПК-10.1)	1. Определите три цели безопасности 2. Систематизация атак на конкретную информацию 3. Услуги и механизмы информационной безопасности 4. Математическая модель шифра. Примеры шифров. Принцип Керкхоффа. Основы криптоанализа. 5. Традиционные шифры. Шифры подстановки (моноалфавитные шифры). Аддитивные, мультипликативные и аффинные шифры. 6. Многоалфавитные шифры. Шифр Плейфера. Шифр Виженера. Шифр Хилла. Шифроблокнот. 7. Шифры перестановки.
2	Блочные и поточные шифры (ОПК-10.2)	1. Шифры потока и блочные шифры. 2. Современные блочные шифры с симметричным ключом. 3. Компоненты современного блочного шифра. 4. Стандарт шифрования DES. Его свойства. 5. Многократное применение DES. 6. Стандарт шифрования AES. Его версии. 7. Криптоанализ стандартов DES и AES. 8. Режимы работы DES и AES. 9. Шифры потока RC4 и A5/1.
3	Шифры с ассиметричным ключом (ОПК-10.2)	1. Криптография с асимметричным ключом. Односторонние функции. 2. Криптосистема RSA. Атаки на RSA. 3. Криптосистемы Рабина и Эль-Гамаля 4. Криптографические хеш-функции 5. Алгоритмы SHA хеширования.
4	Практические задачи криптографии (ОПК-10.2)	1. Проверка целостности сообщения. 2. Установление подлинности сообщения. 3. Понятие цифровой подписи. 4. Схемы цифровой подписи. 5. Установление подлинности объекта. 6. Управление ключами. Протоколы Диффи-Хеллмана. 7. Криптографический протокол электронных денег.

После изучения каждой темы раздела для закрепления изученного материала проводится **тестирование**. Тестирование проходит с использованием системы MyTest. Задание теста включает 10 вопросов. Время выполнения заданий теста составляет 10 минут.

Тестовые задание по темам

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Введение. Основные понятия криптографии (ОПК-10.1)	**Задание 1** Главные составляющие информационной безопасности *Выберите один из 3 вариантов ответа:* 1) конфиденциальность, целостность, доступность. 2) конфиденциальность, достоверность, доступность. 3) конфиденциальность, подлинность, отказоустойчивость. **Задание 2** Формальные группы способов обеспечения информационной безопасности *Выберите один из 3 вариантов ответа:* 1) физические, аппаратные, программные, специфические 2) физические, аппаратные, программные, законодательные 3) организационные, аппаратные, программные, законодательные Задание 3 К базовым атакам на криптосистему относятся *Выберите один из 3 вариантов ответа:* 1) брутфорс, частотный анализ, интерполяция, понижение и кросс-протоколы 2) брутфорс, частотный анализ, интерполяция, статистическое смещение 3) частотный анализ, интерполяция, статистическое смещение, брутфорс, числовое решето **Задание 4** Принцип Керкхоффа при разработке криптографических систем *Выберите один из 3 вариантов ответа:* 1) в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым 2) ключ должен содержать не менее двух взаимно независимых полей 3) простота шифра может быть компенсирована длиной ключа **Задание 5** Шифры подстановки предполагают выполнение *Выберите один из 3 вариантов ответа:* 1) замены символов исходного сообщения на другие, выбранные по определенному алгоритму 2) смещения символов исходного сообщения относительно базового алфавита 3) совместное выполнение пунктов 1 и 2 **Задание 6** Принцип работы шифра Виженера заключается в том, что *Выберите один из 3 вариантов ответа:* 1) каждая буква в исходном шифруемом тексте сдвигается по алфавиту на переменное количество символов в соответствии с ключом

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		2) каждая буква в исходном шифруемом тексте сдвигается по алфавиту на переменное количество символов в зависимости от ее начальной позиции в алфавите и от ключа 3) текст разбивается на блоки, каждый из которых вписывается в таблицу с последующей сменой строк и столбцов **Задание 7** Шифр Вернама относится к *Выберите один из 3 вариантов ответа:* 1) достаточно стойким 2) абсолютно стойким 3) относительно стойким **Задание 8** Какое утверждение верно *Выберите один из 3 вариантов ответа:* 1) в асиметричной криптосистеме закрытый ключ получается путем преобразования открытого 2) в асиметричной криптосистеме закрытый ключ не может быть получен путем преобразования открытого 3) в асиметричной криптосистеме закрытый ключ может формироваться исключительно путем нелинейного преобразования открытого **Задание 9** Вероятностная модель шифра содержит *Выберите один из 3 вариантов ответа:* 1) алгебраическую модель, дополненную вероятностными распределениями для открытого текста и ключей 2) пространства открытых текстов, криптограмм и ключей 3) алгебраическую модель, дополненную вероятностными распределениями для открытого текста, криптограмм и ключей **Задание 10** Какой тип атаки может быть реализован при отсутствии механизмов аутентификации *Выберите один из 3 вариантов ответа:* 1) человек посредине 2) Downgrade Attack 3) статистическое смещение
2	Блочные и поточные шифры (ОПК-10.2)	**Задание 1** Современный блочный шифр содержит в себе *Выберите один из 3 вариантов ответа:* 1) блоки перестановки (P-блоки) и блоки подстановки (S-блоки) 2) блоки перестановки (P-блоки) 3 типов (прямые, расширения и сжатия), и блоки подстановки (S-блоки) с равным числом входов и выходов 3) блоки перестановки (P-блоки) 3 типов (прямые, расширения и сжатия), и блоки подстановки (S-блоки) с разным числом входов и выходов **Задание 2** Современный блочный шифр содержит в себе *Выберите один из 3 вариантов ответа:* 1) блоки перестановки (P-блоки) и блоки подстановки (S-блоки) 2) блоки перестановки (P-блоки) 3 типов (прямые, расширения и сжатия), и блоки подстановки (S-блоки) с равным числом входов и выходов 3) блоки перестановки (P-блоки) 3 типов (прямые, расширения и сжатия), и блоки подстановки (S-блоки) с разным числом входов и выходов

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		Задание 3 Ключевые требования с современным блочным шифрам согласно Шенону *Выберите один из 3 вариантов ответа:* 1) рассеивание и перемешивание информации 2) рассеивание, расширение и перемешивание информации 3) рассеивание, сужение и перемешивание информации **Задание 4** Размеры ключей, используемых в AES *Выберите один из 3 вариантов ответа:* 1) 128, 192 и 256 бит 2) 256, 512 и 1024 бита 3) 64, 128 и 512 бит **Задание 5** Максимальное количество раундов шифрования в AES *Выберите один из 3 вариантов ответа:* 1) 10 2) 14 3) 32 **Задание 6** Укажите верную очередность технологических операций в ходе раунда шифрования AES *Выберите один из 3 вариантов ответа:* 1) AddRoundKey, SubBytes, ShiftRows, MixColumn 2) SubBytes, ShiftRows, MixColumn, AddRoundKey 3) AddRoundKey, MixColumn, SubBytes, ShiftRows **Задание 7** Какие недостатки являются характерными для шифросистемы DES *Выберите несколько из 4 вариантов ответа:* 1) небольшой раз мер ключа 2) битовые операции в узлах замены неэффективно реализуются программным путем 3) возможность реализации атаки сторонними каналами 4) низкая скорость работы алгоритма **Задание 8** Размер слова в алгоритме шифрования RC4 по умолчанию составляет *Выберите один из 3 вариантов ответа:* 1) 16 бит 2) 8 бит 3) 64 бита **Задание 9** Какой из вариантов многократного шифрования DES не используется *Выберите один из 3 вариантов ответа:* 1) 2DES 2) 3DES с двумя ключами 3) 3DES с одним ключом **Задание 10** Сеть Фейстеля использует *Выберите один из 3 вариантов ответа:* 1) многораундовое шифрование с половинным делением входных блоков 2) многораундовое шифрование с перестановочно-перестановочной обработкой каждого блока 3) однораудновое шифрование с применением гамирования
3	Шифры с ассиметричным	**Задание 1** Модуль RSA определяется на основе

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
	ключом (ОПК-10.2)	*Выберите один из 3 вариантов ответа:* 1) функции Эйлера 2) произведения двух взаимно простых чисел 3) формулы Ферма для простых чисел **Задание 2** Секретный ключ RSA содержит *Выберите один из 3 вариантов ответа:* 1) секретную экспоненту и модуль 2) модуль и сеансовый ключ 3) секретную экспоненту в неявном виде **Задание 3** Закрытый ключ может быт получен злоумышленником если *Выберите один из 3 вариантов ответа:* 1) величина секретной экспоненты меньше корня 4-й степени из модуля 2) он владеет открытым ключом 3) слагаемые, взятые для вычисления модуля, не являются независимыми **Задание 4** Сколько слов содержит блок исходного сообщения в ходе обработки по схеме SHA-2 хеширования *Выберите один из 3 вариантов ответа:* 1) 32 2) 16 3) 4 **Задание 5** К снижению стойкости RSA-шифра приводит *Выберите несколько из 4 вариантов ответа:* 1) выбор слагаемых модуля малых величин 2) табличный выбор слагаемых модуля 3) неиспользование сеансовых ключей 4) выбор большой открытой экспоненты **Задание 6** Недостатком асимметричного шифрования является *Выберите один из 3 вариантов ответа:* 1) низкое быстродействие 2) неустойчивость к атаке Винера 3) зависимость стойкости шифра от исходного сообщения **Задание 7** Сеансовые ключи, как правило, шифруются *Выберите один из 3 вариантов ответа:* 1) симметричными алгоритмами 2) асимметричными алгоритмами 3) как симметричными, так и асимметричными алгоритмами **Задание 8** В схеме Эль-Гамаля длина шифротекста и сообщения соотносятся как: *Выберите один из 3 вариантов ответа:* 1) 1:1 2) 2:1 3) 1:2 **Задание 9** Ключевыми недостатками криптосистемы Рабина является *Выберите несколько из 4 вариантов ответа:* 1) необходимость выбора истинного сообщения из 4-х возможных 2) возможность восстановить закрытый ключ при малых величинах открытого 3) низкое быстродействие

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		4) возможность взлома с использованием атаки на основе подобранного открытого зашифрованного текста **Задание 10** Криптосистема Эль-Гамаля основана на *Выберите один из 3 вариантов ответа:* 1) вычислительной сложности поиска квадратных корней в кольце остатков по модулю составного числа 2) вычислительной сложности проблемы дискретного логарифмирования 3) вычислительной сложности задачи факторизации больших полупростых чисел
4	Практические задачи криптографии (ОПК-10.2)	**Задание 1** Электронная подпись представляет собой *Выберите несколько из 3 вариантов ответа:* 1) информацию в электронной форме присоединенную к подписываемой информации или иным образом связаную с такой информацией и которая используется для определения лица, подписывающего информацию 2) массив данных, использующийся для подтверждения подлинности иной электронной информации 3) результат вычисления хеш-функции на основе исходного сообщения **Задание 2** Типы электронной подписи *Выберите одино из 3 вариантов ответа:* 1) простая ЭП, усиленная неквалифицированная ЭП, достоверная ЭП 2) простая ЭП, усиленная неквалифицированная ЭП, усиленная квалифицированная ЭП 3) достоверная ЭП, условно-достоверная ЭП **Задание 3** Протокол Диффи-Хеллмана использует *Выберите один из 3 вариантов ответа:* 1) асимметричное шифрование 2) асимметричное и симметричное шифрование 3) симметричное шифрование **Задание 4** Для какой атаки уязвим протокол Диффи-Хеллмана в чистом виде *Выберите один из 3 вариантов ответа:* 1) brut force 2) человек посредине 3) числовое решето **Задание 5** ДК методом установления подлинности объекта относятся *Выберите один из 3 вариантов ответа:* 1) простой пароль, выборка символов пароля 2) простой пароль, биометрическая идентификация, функциональное преобразование, выборка символов пароля 3) простой пароль, функциональное преобразование, выборка символов пароля **Задание 6** Проверка целостности сообщения выполняется *Выберите один из 3 вариантов ответа:* 1) вычислением хеш-функции по заранее установленному алгоритму 2) вычислением контрольной функции (check function) от сообщения - некоего числа небольшой длины 3) путем анализа синтаксических и семантических свойств сообщения **Задание 7**

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		Что требуется для реализации протокола электронных денег *Выберите один из 3 вариантов ответа:* 1) формирование конверта и получение слепой подписи 2) только получение слепой подписи 3) формирование конверта, получение слепой подписи и установление нечеткой зависимовти между ними **Задание 8** Количество конвертов, которое покупатель будет отправлять в банк, считается *Выберите один из 3 вариантов ответа:* 1) маскирующим 2) потенциально возможным 3) достаточным **Задание 9** В ходе перевода денег из фиатной формы в цифровую, клиент выполняет *Выберите один из 3 вариантов ответа:* 1) формирование открытого ключа для взаимодействия с банком 2) генерирацию уникального номера «монеты» m. 3) формирование закрытого ключа для взаимодействия с банком **Задание 10** Для защиты Биткойн использует *Выберите один из 3 вариантов ответа:* 1) симметричное шифрование и хеширование 2) асимметричное шифрование и хеширование . 3) эцп на эллиптических кривых

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме зачета используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминов, определений, понятий
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Умения	Умение анализировать основные положения законодательства в области безопасности информации
	Умение использовать руководящие документы регуляторов в области информационной безопасности
Навыки	Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности

	Качество выполнения исследований объектов профессиональной деятельности
	Самостоятельность выполнения исследований объектов профессиональной деятельности

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений, понятий	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, их интерпретирует и использует	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательности	Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5

Умение анализировать основные криптографическ ие методы обеспечения информационной безопасности	Не умеет анализировать основные криптографическ ие методы обеспечения информационной безопасности	Допускает неточности в анализе основных криптографическ их методов обеспечения информационно й безопасности	Умеет анализировать основные криптографиче ские методы обеспечения информационн ой безопасности	Умеет анализировать основные криптографические методы обеспечения информационной безопасности и делать обобщающие выводы
Умение использовать криптографичес кие средства обеспечения безопасности информации	Не умеет использовать криптографичес кие средства обеспечения безопасности информации	Использование криптографиче ских средств обеспечения безопасности информации вызывает затруднения	Умеет использовать криптографич еские средства обеспечения безопасности информации	Умело использует криптографическ ие средства обеспечения безопасности информации

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками теоретического и экспериментальн ого исследования объектов профессионально й деятельности	Не владеет навыками теоретического и экспериментально го исследования объектов профессионально й деятельности	Не достаточно хорошо владеет навыками теоретического и экспериментальн ого исследования объектов профессиональн ой деятельности	Владеет навыками теоретического и экспериментальн ого исследования объектов профессиональ ной деятельности	Профессионально владеет навыками теоретического и экспериментальног о исследования объектов профессиональной деятельности
Качество выполнения исследований объектов профессионально й деятельности	Не качественно выполняет исследования объектов профессионально й деятельности, допускает грубые ошибки	Не достаточно качественно выполняет исследования объектов профессиональн ой деятельности, допускает и исправляет ошибки с посторонней помощью	Не достаточно качественно выполняет исследования объектов профессиональн ой деятельности, допускает и исправляет ошибки самостоятельно	Качественно выполняет исследования объектов профессиональной деятельности
Самостоятельнос ть выполнения исследований объектов профессионально й деятельности	Не может самостоятельно выполнять исследования объектов профессионально й деятельности	Выполняет исследования объектов профессиональн ой деятельности с посторонней помощью	При выполнении исследования объектов профессиональн ой деятельности иногда требуется посторонняя помощь	Самостоятельно выполняет исследования объектов профессиональной деятельности

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения практических занятий	Специализированная мебель. Компьютеры на базе процессоров Intel или AMD.
3.	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду.

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
2	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
3	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4	Среды программирования Free Pascal, Dev C++ или CodeBlocks	Свободно распространяемое ПО согласно условиям лицензионного соглашения

6.3. Перечень учебных изданий и учебно-методических материалов

1. Алексеев В.А. Методы и средства криптографической защиты информации методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации»: Методические указания – Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2009. Эл.ресурс: http://www.iprbookshop.ru/17710
2. Алферов А.П. Основы криптографии : учеб. пособие / сост. : А. П. Алферов [и др.]. - Москва : Гелиос АРВ, 2001. - 480 с.
3. Баричев, С.Г. Основы современной криптографии: учеб. курс. / С.Г. Баричев, В. В. Гончаров, Р. Е. Серов. – 2-е изд., перераб. и доп. – М.: Горячая линия. – Телеком, 2002. – 175 с.
4. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. - Москва : МЦНМО, 2003. - 325 с.
5. Гашков, С.Б. Криптографические методы защиты информации: учеб. пособие. / С. Б. Гашков, С. Б. Применко, М. А. Черепнев. – М.: Академия, 2010. – 298 с.
6. Грибунин В.Г., И.Н. Оков, И.В. Туринцев Цифровая стеганография: учебное пособие – М.: СОЛОН-ПРЕС, 2009. Эл.ресурс: http://www.iprbookshop.ru/8642
7. Зензин, О.С. Стандарт криптографической защиты – AES. Конечные поля. / О. С. Зензин, М.А. Иванов. – М.: Кудиц – Образ, 2002. – 174 с.
8. Кукина Е.Г. Введение в криптографию [Электронный ресурс] : сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. — 91 с. — 978-5-7779-1588-7. — Режим доступа: http://www.iprbookshop.ru/24876.html
9. Рябко Б.Я. Основы современной криптографии для специалистов в информационных технологиях / Б. Я. Рябко, А. Н. Фионов. - Москва : Научный мир, 2004. - 172 с.
10. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии : Монография – М.: Горячая линия – Телеком, 2010. Эл.ресурс: http://www.iprbookshop.ru/12018
11. Столлингс В. Криптография и защита сетей: принципы и практика / В. Столлингс. - 2-е изд. - Москва : Вильямс, 2001. - 669 с.
12. Масленников М.Е. Практическая криптография / М. Е. Масленников. - Санкт-Петербург : БХВ-Петербург, 2003. - 458 с. + 1 CD-ROM.
13. Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии: Учебное пособие – СПб.: Российский государственный гидрометеорологический университет, 2010. Эл.ресурс: http://www.iprbookshop.ru/17925
14. Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс] : учебное пособие / П.П. Бескид, Т.М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 104 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17926.html Аграновский А.В., Хади Р.А. Практическая криптография. Алгоритмы и их программирование: Учебное пособие – М.: СОЛОН-ПРЕС, 2009. Эл.ресурс: http://www.iprbookshop.ru/8641

15. Фороузан, Б.А. Криптография и безопасность сетей: Учебное пособие. / Б.А. Фороузан; пер. с англ. под ред. А.Н. Берлина. – М.: Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2014. – 784 с.
16. Гашков С. Б., Применко Э.А., Черепнѐв М.А. Криптографические методы защиты информации: учеб. пособие: Допущено УМО. М.: Изд. центр «Академия», 2010.
17. Хорев, Б.П. Методы и средства защиты информации в компьютерных системах: учеб. пособие. / П.Б. Хорев. – 4-е изд. стер. – М.: Академия, 2008. – 256 с.
18. Чмора, А.Л. Современная прикладная криптография : учеб. пособие / А. Л. Чмора. - Москва : "Гелиос АРВ", 2001. - 244 с.
19. Сергиенко Е.Н. Криптографические методы защиты информации: методические указания к выполнению лабораторных работ и индивидуальных домашних заданий для студентов специальности 090303.65 – Информационная безопасность автоматизированных систем / сост. Е.Н. Сергиенко, Д.О. Давыденко, И.М. Идеменко, А.А. Хохлов. – Белгород: Изд-во БГТУ, 2014. – 82 с.
20. Бабаш, А.В. Криптография: учебная пособие. / А.В. Бабаш, Г.П. Шанкин. – М.: Солон – Р, 2002. – 511 с.
21. Зубов, А.Ю. Криптографические методы защиты информации. Современные шифры: учеб. пособие. / А.Ю. Зубов. – М.: Гелиос АРВ, 2005. – 190 с.
22. Мао, В. Современная криптография: теория и практика. – М.: Вильямс, 2005. – 768 с.
23. Молдовян, Н.А. Практикум по криптосистемам с открытым ключом. / Н.А. Молдовян. – СПб.: БХВ – Петербург, 2007. – 304 с.
24. Нечаев, В.И. Элементы криптографии. Основы теории защиты информации: учеб. пособие. / В.И. Нечаев. – М.: Высш. шк., 1999. – 109 с.
25. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006.
26. Рябко, Б.Я. Криптографические методы защиты информации. / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая линия – Телеком, 2005. – 229 с.
27. Смарт, Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 255 с.
28. Столлингс, В. Криптография и защита сетей: принципы и практика. / В. Столлингс – 2 издание. – М.: Вильямс – Р, 2001. – 381 с.
29.

6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. Электронная библиотека (на базе ЭБС «БиблиоТех») — Режим доступа: http://ntb.bstu.ru
2. Электронно-библиотечная система IPRbooks — Режим доступа: http://www.iprbookshop.ru
3. Электронно-библиотечная система «Университетская библиотека ONLINE» — Режим доступа: http://www.biblioclub.ru/

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 202__/202__ учебный год без изменений / с изменениями, дополнениями

Протокол № _____ заседания кафедры от «____»_____ 202_ г.

Заведующий кафедрой_____
подпись, ФИО

Директор института _____
подпись, ФИО