Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП:
_____ Н.А. Семыкина
«9» 06 2023 г.

Рабочая программа дисциплины (с аннотацией)

Криптографические методы защиты информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов 4 курса очной формы обучения

Уровень высшего образования

СПЕЦИАЛИТЕТ

Составитель:
ст. преподаватель С.А. Желтов.

Тверь 2023

I. Аннотация

1. Наименование дисциплины (модуля) в соответствии с учебным планом

Криптографические методы защиты информации.

2. Цель и задачи дисциплины (модуля)

Целью освоения дисциплины (модуля) является:

формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области использования и проектирования и средств криптографической защиты информации, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины (модуля) являются:

- получение базовых знаний и умений, связанных с основными понятиями средств криптографической защиты информации;
- получение теоретических знаний о роли и назначении различных криптографических систем;
- обучения студентов общим принципам и методам построения криптографических систем;
- получение теоретических знаний и практических навыков о основных прикладных задачах, решаемых с помощью средств криптографической защиты информации;

3. Место дисциплины (модуля) в структуре ООП

Дисциплина входит в базовую часть профессионального цикла дисциплин.

Для освоения дисциплины студент должен владеть основными понятиями, алгебры, теории вероятности, теории информации, информационной безопасности. Необходимы знания, умения и компетенции, полученные студентами на занятиях по дисциплинам Организационное и правовое обеспечение информационной безопасности, языки программирования, алгебра. Знания и практические навыки, полученные из курса, используются студентами при прохождении производственной и преддипломной практики, а также при разработке курсовых и дипломных работ.

4. Объем дисциплины (или модуля):

___7___ зачетных единиц, __252__ академических часов, **в том числе контактная работа:** лекции _66__ часов, практические занятия _18____ часов, лабораторные работы ___48____ часов, **самостоятельная работа:** ___75__ часа, **контроль** 45 часов.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы	**Планируемые результаты обучения по дисциплине (модулю)**

(формируемые компетенции)	
ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации	**Владеть:** навыками определения видов и форм информации, подверженных угрозам, и возможных методов и путей устранения этих угроз. **Уметь:** пользоваться научно-технической литературой в области криптографии. **Знать:** основные задачи и понятия криптографии.
Базовый **ПСК-2.1.** способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации.	**Владеть:** криптографической терминологией; навыками использования типовых криптографических алгоритмов. **Уметь:** корректно применять симметричные и асимметричные криптографические алгоритмы; использовать криптографические методы и средства защиты информации в автоматизированных системах. **Знать:** основные криптографические примитивы и их использование в решении основных задач защиты информации; принципы построения и основные виды симметричных и асимметричных криптографических алгоритмов; основные криптографические методы и алгоритмы защиты информации; криптографические стандарты.
Продвинутый **ПСК-2.1.** способностью разрабатывать вычислительные алгоритмы, реализующие современные	**Владеть:** навыками использования ПЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии. **Уметь:** применять математические методы описания и исследования криптосистем; использовать принципы построения средств криптографической защиты информации. **Знать:** криптографические алгоритмы и особенности

математические методы защиты информации.	их программной реализации; математические модели шифров; частотные характеристики открытых текстов и их применение к анализу простейших симметричных криптосистем; требования к шифрам и основные характеристики шифров.

6. Форма промежуточной аттестации: зачет, экзамен.

7. Язык преподавания русский**.**

II. Содержание дисциплины (или модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Для студентов очной формы обучения

Учебная программа – наименование разделов и тем	**Всего (час.)**	**Контактная работа (час.)**		**Самостоятельная работа (час.)**
		Лекции	Практические (лабораторные) занятия	
Раздел 1. Основные понятия криптографии. Простейшие шифры				
Тема 1.1.Предмет криптографии и история развития.	7	2	2	3
Тема 1.2. Основные понятия криптографии	7	2	2	3
Тема 1.3. Простейшие шифры замены и перестановки.	9	4	2	3
Тема 1.4. Общая схема системы с секретным ключом.	11	6	2	3
Тема 1.5. Модели открытых текстов				
Тема 1.6. Модели шифров				
Раздел 2. Симметричные шифры	9	4	2	3
Тема 2.1. Поточные, итерационные и блочные шифры	9	4	2	3
Тема 2.2. Стандарты симметричного шифрования	11	6	2	3
Тема 2.6. Теоретическая стойкость шифров. Совершенные шифры.				
Тема 2.6. Практическая стойкость шифров.				
Раздел 3. Ассиметричные системы				
Тема 3.1. Общая схема системы с открытым ключом.				
Тема 3.2. RSA				

Тема 3.3. Генерация ключей				
Тема 3.4. Хеш-функции и ЭЦП				
Тема 3.4. Стойкость ассиметричных криптосистем				
ИТОГО	**81**	**34**	**18**	**27**

Учебная программа

Раздел 1. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОПРОТОКОЛОВ

Тема 1.1. Предмет криптографии и история развития.

Определение криптографии. Место криптографии в защите информации. Задачи, решаемые с помощью криптографических преобразований. Основные этапы развития криптографии.

Тема 1.2. Основные понятия криптографии. Простейшие шифры.

Определение шифра. Примеры простейших шифров и других основных понятий

Тема 1.3. Простейшие шифры замены и перестановки.

Классификация шифров. Определение шифра замены и перестановки.

Тема 1.4. Общая схема системы с секретным ключом.

Схема передачи закрытой информации по открытому каналу связи, с использованием системы шифрования с секретным ключом.

Тема 1.5. Модели открытых текстов.

Источники и характеристики открытых текстов. Детерминированные модели. Вероятностные модели. Стационарный источник независимых символов и биграмм.

Тема 1.6. Тема 1.6. Модели шифров

Алгебраическая и вероятностные модели шифра.

Раздел 2 СИММЕТРИЧНЫЕ ШИФРЫ

Тема 2.1. Поточные, итерационные и блочные шифры

Определение поточного шифра. Примеры. Определение итерационного шифра. Примеры. Определение блочного шифра. Сеть Фейстеля. Примеры.

Тема 2.4. Стандарты симметричного шифрования

Стандарт ГОСТ 28147-89. DES. Другие стандарты симметричного шифрования.

Тема 2.6. Теоретическая стойкость шифров. Совершенные шифры.

Понятие стойкости шифра. Теоретико-информационный подход к оценке криптостойкости шифров. Определение совершенного шифра. Примеры. Основные требования к шифрам.

Тема 2.6. Практическая стойкость шифров.

Практическая стойкость шифров; имтостойкость и помехоустойчивость шифров.

Раздел 3. АССИМЕТРИЧНЫЕ СИСТЕМЫ

Тема 3.1. Общая схема системы с открытым ключом.

Схема передачи закрытой информации по открытому каналу связи, с использованием системы шифрования с открытым ключом.

Тема 3.2. RSA.

Описание криптосистемы RSA, её функции. Параметры RSA.

Тема 3.3. Генерация ключей.

Протокол генерации ключей Диффи-Хелмана. Управление ключами, жизненный цикл ключей, способы распределения ключей.

Тема 3.4. Хеш-функции и ЭЦП.

Понятие односторонней функции. Свойства хеш-функций. ЭЦП. Отечественные стандарты ЭЦП.

Тема 3.4. Стойкость ассиметричных

Задачи лежащие в основе ассиметричных криптосистем: факторизации и дискретного логарифмирования. Понятие сложности алгоритма.

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (или модулю)

Самостоятельная работа обучающихся направлена на освоение учебного материала и развитие практических умений. Самостоятельная работа включает следующие виды самостоятельной работы студентов: работа с рекомендованной литературой и документацией; выполнение практических заданий; подготовка к контрольным .

Тематика рефератов и методические рекомендации по их написанию.

1. Марковские модели открытых текстов
2. История криптографии
3. Основные понятия стеганографии
4. Сокрытие информации средствами стеганографии, на примере графических и видео файлов
5. Энигма
6. Шифратор Джефферсона
7. Модификации DES
8. Ранцевые криптоситемы
9. Случайные последовательности в криптографии
10. Генераторы ПСЧ чисел и ПСП
11. Удостоверяющие центры и производители ЭЦП
12. Модели атак на алгоритмы ЭЦП

Вопросы для контрольных тестов и самоконтроля.

1. Дайте определение шифра.

2. Назовите основные модели открытых текстов

3. Назовите основные модели шифров

4. Приведите классификацию шифров по типу используемого преобразования.

5. Дайте определение блочного шифра.

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)

1. Типовые контрольные задания для проверки уровня сформированности компетенций ОПК-3 , ПСК-2.1.

Рассматривается трехкомпонентной структура компетенции: знать, уметь, владеть.

При этом под указанными категориями понимается:

- «знать» – воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;
- «уметь» – решать типичные задачи на основе воспроизведения стандартных алгоритмов решения;
- «владеть» – решать усложненные задачи на основе приобретенных знаний, умений и навыков, в нетипичных ситуациях

Этап формирования компетенции, в котором участвует дисциплина	**Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)**	**Показатели и критерии оценивания компетенции, шкала оценивания**
Базовый		
Базовый владеть	Основными понятиями криптографии	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части описания из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
	Алгоритмами реализующими простейшие шифры замены и перестановки	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за логической ошибки – 1 балл • Решение не дано ИЛИ

		дано неверное решение – 0 баллов
Базовый уметь	Описывать схемы и алгоритмы реализующие простейшие шифры замены и перестановки	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
	Формально описать шифр в терминах алгебраической или вероятностной модели.	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
Базовый знать	Основные симметричные шифры и требования к ним.	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
	Основные операторы и преобразования используемые в блочных шифрах	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
Продвинутый	Основными понятиями	• Факты и примеры в полном

владеть	ассиметричной криптографии	объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
Продвинутый уметь	Формулировать (описывать) алгоритмы схемы реализующие блочные и итерационные шифры	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за алгоритмической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
Продвинутый знать	Стандарты шифрования	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
	Основные способы (методы) криптоанализа	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов

При оценивании результатов освоения дисциплины применяется «рейтинговая» технология (балльно-накопительная) система. Оценка уровня сформированности компетенций осуществляется в процессе следующих форм контроля:

1) **следящего** (проводится оценка выполнения студентами заданий в ходе аудиторных занятий). Дает возможность квалифицировать степень сформированности знаний, умений, навыков, а также их глубину и прочность. Его задача - регулярное управление учебной деятельности студентов и ее корректировка. Он позволяет получать первичную информацию о ходе и качестве усвоения учебного материала, а также стимулировать регулярную, напряженную и целенаправленную работу студентов. Данный контроль позволяет вовремя выявить пробелы в знаниях и оказать им помощь в усвоении программного материала. Данными формами контроля являются: ответы с места и у доски, проверка работ выполненных в тетради.

2) **текущего** (оценивается работа студентов вне аудиторных занятий). Текущими формами контроля являются: проверка выполнения практических работ, ответы у доски, рефераты, доклады, проверка самостоятельной работы студентов.

3) **промежуточного** (рейтинговые точки) позволяет определять качество изучения студентами учебного материала по разделам и темам. Контроль проводится два раз в семестр. С помощью периодического контроля обобщаются и усваиваются целые темы и разделы, выявляется взаимосвязями с другими разделами, предметами. Контроль охватывает студентов и всей группы и проводится в виде теста, письменных практических работ.

4) **итогового** (зачёт). Максимальная сумма рейтинговых баллов по дисциплине составляет 100 баллов. Студенту, набравшему 50 баллов и выше по итогам работе в семестре, в экзаменационной ведомости и зачетной книжке выставляется оценка «зачтено». Студент, набравший от 20 до 49 баллов включительно, сдаёт зачет в последнюю неделю семестра по данной дисциплине. Баллы, полученные на зачете проставляются в ведомости. Студенту, набравшему меньше 20 баллов, в экзаменационной ведомости выставляется оценка «незачтено». Данному студенту разрешается пересдача зачета по направлению деканата на последней неделе семестра.

Формы контроля

Занятия для студентов очной формы обучения проводятся в 1-м и во 2-м семестрах 4 курса и заканчиваются в первом семестре зачётом и во втором – экзаменом. Период времени, отведенный на обучение по данной дисциплине, планируется разделить на 4 модуля, каждый из которых заканчивается контрольной точкой. За текущую работу в первом семестре, включая контрольные точки, студент может заработать 100 баллов, во втором – 60 баллов, и 40 баллов составляет максимальная оценка за экзаменационный ответ. Количество баллов за текущую работу выставляется в соответствии со сложностью темы и количеством заданий, выносимых для практических работ в аудитории и самостоятельных занятий.

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.

Для оценки уровня теоретических и практических знаний используется тест или контрольная работа письменный опрос. Перечень некоторых вопросов теста и практических заданий представлен ниже.

Приводится два варианта из имеющихся двадцати различных вариантов по каждой из рассматриваемых тем.

Вариант 1

1.Опишете алгебраическую модель шифра Цезаря

2. Расшифровать фразу, зашифрованную столбцовой перестановкой "ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО"

Вариант 2

1. Опишете алгебраическую модель шифра гаммирования

2. Расшифровать фразу, зашифрованную столбцовой перестановкой "ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК "

ВОПРОСЫ К ЗАЧЕТУ 7 СЕМЕСТР

1. Предмет криптографии, основные понятия. Общая схема симметричного шифрования.
2. История криптографии (Шифратор Джеферсона, Шифр Виженера, Диск Альберти, Шифры Порта, Шифры Кардано, Книжный шифр, Квадрат Полибия).
3. История русской криптографии.
4. Определение шифра, простейшие примеры. Шифры замены, основные понятия.
5. Алгебраические модели шифров.
6. Вероятностные модели шифров.
7. Понятие блочного и итерированного шифров.
8. Шифр Фейстеля, определение и свойства.
9. Алгоритм DES.
10. Режимы DES.
11. Теоретическая стойкость шифров.
12. Практическая стойкость.
13. ГОСТ 28147-89.

ВОПРОСЫ К ЭКЗАМЕНУ 8 СЕМЕСТР

1. Предмет криптографии, основные понятия. Общая схема симметричного шифрования.
2. История криптографии (Шифратор Джеферсона, Шифр Виженера, Диск Альберти, Шифры Порта, Шифры Кардано, Книжный шифр, Квадрат Полибия).

3. История русской криптографии.
4. Определение шифра, простейшие примеры. Шифры замены, основные понятия.
5. Алгебраические модели шифров.
6. Вероятностные модели шифров.
7. Понятие блочного и итерированного шифров.
8. Шифр Фейстеля, определение и свойства.
9. Алгоритм DES.
10. Режимы и модификации DES.
11. Операторы, используемые при построении блочных шифров.
12. Требования к шифрам.
13. Теоретическая стойкость шифров.
14. Практическая стойкость.
15. Частотный криптоанализ.
16. Дифференциальный криптоанализ.
17. ГОСТ 28147-89.
18. CAST-256.
19. Rijndael.
20. RC5.
21. Blowfish.
22. Совершенные шифры.
23. Криптосистемы с открытым ключом.
24. Стойкость криптосистем с открытым ключом.
25. Крипто система RSA.
26. Параметры RSA.
27. Протокол Диффи-Хелмана и его модификации.
28. ЭЦП ГОСТ Р 34.10-2001.
29. Бесключ. Система Месси-Омуры.
30. Вероят. Шифр. СОК Блюма-Голдвассера.
31. Ранцевые криптоситемы.
32. схема подписи Эль-Гамаля.
33. DSA.
34. ГОСТ Р 34.10-94.

35.Генераторы ПСП и ПСЧ и их применение в криптографии.

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

а) Основная литература

Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 c. — ISBN 978-5-4488-0091-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87998.html

Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. -
URL: http://biblioclub.ru/index.php?page=book&id=429092

б) Дополнительная литература:

Донгак, Ш. М. Криптография: Практикум : учебное пособие / Ш. М. Донгак. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163935

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (или модуля)

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.
2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.
3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.
6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. Репозитарий ТвГУ http://eprints.tversu.ru

VII. Методические указания для обучающихся по освоению дисциплины (или модуля)

Материал дисциплины распределен по главным разделам (темам). В результате изучения дисциплины у студентов должно сформироваться научное представление о криптографических системах. Необходимо выработать системный подход к пониманию процессов преобразования входных данных в приложениях защиты информации. В процессе обучения студенты, наряду с текстами лекций и учебными пособиями, должны пользоваться дополнительными научными изданиями, академическими периодическими изданиями. После каждой лекционной темы рекомендуется проработать вопросы для повторения и самоконтроля. В аспекте самостоятельной работы рекомендуется составлять конспект. Рекомендуется использовать справочники и руководства.

Для успешного освоения дисциплины важно соблюсти следующие рекомендации: На первой лекции важно обратить внимание на конкретные требования

к прохождению и сдаче курса. Активная работа на занятиях, выполнение творческих заданий сформирует о Вас дополнительное положительное представление как об активном участнике познавательного процесса. На данном курсе практические занятия являются самым важным компонентом обучающего процесса. На занятиях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, настоятельно рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам в библиотеках и системе «Интернет». Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить: без самостоятельной работы невозможно серьезное освоение любого курса. Надо быть готовым к тому, что по времени, затраченном на дисциплину, самостоятельная работа будет превалировать над иными видами работы. Важно продумать стиль фиксации нового и важного материала. Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (или модулю), включая перечень программного обеспечения и информационных справочных систем (по необходимости)

Процесс изучения дисциплины включает лекции, практические занятия и самостоятельную работу студента. Во время обучения применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении занятий применяется имитационный подход (метод деловой игры, анализ конкретных ситуаций), когда преподавателем разбирается на конкретном примере проблемная ситуация, все шаги решения задачи студентам демонстрируются при помощи мультимедийной техники. Затем студенты самостоятельно решают аналогичные задания. Так же при проведении занятий применяется частично-поисковый метод: студенты осуществляют поиск решения поставленной проблемы (задачи). При этом постановочные задачи опираются на уже имеющиеся у студентов знания и умения, полученные в предшествующих темах. На занятиях практикуется выполнение заданий в малых группах, письменные работы, работа с раздаточным материалом, привлекаются ресурсы сети Интернет. Курс предусматривает выполнение тестов, контрольных и самостоятельных работ, письменных домашних заданий. В качестве форм контроля используются различные варианты взаимопроверки и взаимоконтроля.

Программное обеспечение

Adobe Acrobat Reader DC - Russian	бесплатно
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
Git version 2.5.2.2	бесплатно
Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011;
MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012;
Многофункциональный редактор ONLYOFFICE	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
Microsoft Web Deploy 3.5	бесплатно
MiKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
MySQL Workbench 6.3 CE	бесплатно
NetBeans IDE 8.0.2	бесплатно
Notepad++	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»;
PostgreSQL 9.6	бесплатно
Python 3.4.3	бесплатно
Visual Studio 2010 Prerequisites - English	Акт на передачу прав №785 от 06.08.2021 г.
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно
WinPcap 4.1.3	бесплатно
Wireshark 2.0.0 (64-bit)	бесплатно
R studio	бесплатно

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (или модулю)

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски. Класс ПЭВМ.

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.	I - X	14.05.2017 Корректировка всех разделов в соответствии с новым стандартом	
2.			

3.			