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)

Техническая защита информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Для студентов V курса очной формы обучения

Составитель:
к.ф.м.н., доцент _____ Н.А. Семыкина

Тверь 2023

I. Аннотация

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

Техническая защита информации.

2. Цель и задачи дисциплины (или модуля)

Целью дисциплины является: формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий; развитие системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Задачи дисциплины:

- изучение концепции инженерно-технической защиты информации;
- изучение теоретических основ инженерно-технической защиты информации;
- изучение физических основ инженерно-технической защиты информации;
- изучение технических средств добывания и защиты информации;
- изучение организационных основ инженерно-технической защиты информации;
- изучение методического обеспечения инженерно-технической защиты информации.

3. Место дисциплины (или модуля) в структуре ООП

Дисциплина «Техническая защита информации» относится к числу дисциплин базовой части профессионального цикла.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – работа с программными средствами общего назначения;

«Аппаратные средства вычислительной техники» – знание архитектуры основных типов современных компьютерных систем;

«Операционные системы» – знание принципов построения современных операционных систем и особенностей их применения, владение навыками конфигурирования и администрирования операционных систем.

4. Объем дисциплины (или модуля):

3 зачетных единиц, 108 академических часов, **в том числе**

контактная работа: лекции 15 часов, практические занятия 30 часов, самостоятельная работа: 63 часа.

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

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине (или модулю)**
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 анализа информации, навыками использования нормативных документов по противодействию технической разведке. **Уметь:** осуществлять подбор, изучение и обобщение научно-технической информации по способам и средствам технической защиты информации. **Знать:** нормативные документы по противодействию технической разведке.
ПК-9. способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню	**Владеть:** методами и средствами технической защиты информации; методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее. **Уметь:** проводить аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации, пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения. **Знать:** средства и методы предотвращения и

защищенности компьютерной системы	обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации.
ПК-19. способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	**Владеть:** методами и средствами технической защиты информации, методами расчета и инструментального контроля показателей технической защиты информации. **Уметь:** пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения. **Знать:** технические каналы утечки информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации.
ПК-20. способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	**Владеть:** способностью производить проверку технического состояния и профилактические осмотры оборудования по защите информации. **Уметь:** выполнять работы по приему, настройке, регулировке, освоению и восстановлению работоспособности оборудования защиты информации. **Знать:** средства и методы предотвращения и обнаружения вторжений, методы восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций.

6. Форма промежуточной аттестации зачет

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

1. Для студентов очной формы обучения

Учебная	Всего	Контактная работа (час.)	Самостоятельная

программа – наименование разделов и тем	(час.)	Лекции	Практические (лабораторные) занятия	работа (час.)
Концепция инженерно-технической защиты информации	12	2	4	6
Теоретические основы инженерно-технической защиты информации	30	5	10	15
Физические основы защиты информации	18	3	6	9
Технические средства добывания и инженерно-технической защиты информации	18	3	6	9
Организационные основы инженерно-технической защиты информации	12	2	4	6
Методическое обеспечение инженерно-технической защиты информации	18	3	6	9
ИТОГО	108	18	36	54

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

Тема № 1. Концепция инженерно-технической защиты информации

1.1 Системный подход к защите информации

Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации.

1.2 Основные концептуальные положения инженерно-технической защиты информации

Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации.

Тема № 2. Теоретические основы инженерно-технической защиты информации

2.1 Информация как предмет защиты

Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие о текущей и эталонной признаковой структуре.

2.2 Источники опасных сигналов

Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и краткая характеристика основных и вспомогательных технических средств и систем. Образование опасных сигналов в результате побочных электромагнитных излучений и наводок.

2.3. Характеристика технической разведки

Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведки. Классификация технической разведки. Возможности видов технической разведки. Основные направления развития технической разведки.

2.4. Технические каналы утечки информации

Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика и возможности.

2.5 Методы инженерной защиты и технической охраны объектов

Классификация способов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления охраной. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара. Автоматизация процессов охраны.

2.6 Методы скрытия информации и ее носителей.

Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления.

Тема № 3. Физические основы защиты информации

3.1 Физические основы побочных излучений и наводок

Акустоэлектрические преобразования. Источники побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Утечка опасных сигналов по цепям электропитания и заземления.

3.2 Распространение сигналов в технических каналах утечки информации

Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Характеристика среды распространения сигналов различных технических каналов утечки информации.

3.3 Физические процессы при подавлении опасных сигналов

Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

Тема № 4. Технические средства добывания и инженерно-технической защиты информации

4.1 Средства технической разведки

Визуально-оптические приборы. Фотоаппараты. Оптикоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.

4.2 Средства инженерной защиты и технической охраны.

Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

4.3 Средства предотвращения утечки информации по техническим каналам

Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления.

Тема № 5. Организационные основы инженерно-технической защиты информации

5.1 Государственная система защиты информации

Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации.

5.2 Контроль эффективности инженерно-технической защиты информации.

Виды контроля эффективности инженерно-технической защиты информации. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

Тема № 6. Методическое обеспечение инженерно-технической защиты информации

6.1 Моделирование инженерно-технической защиты информации.

Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты.

6.2 Принципы оценки эффективности инженерно-технической защиты информации.

Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в помещении.

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

Типовые контрольные задания для проверки уровня сформированности компетенций ОПК 3, ПК – 9, 19, 20.

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 **Владеть**	1. В структуру системы технической разведки входят А – объекты разведки, органы добывания и органы сбора и обработки В – потребители информации, органы планирования и управления, органы добывания С - органы планирования и управления, органы добывания и органы сбора и обработки 2. Чем отличается технический канал утечки информации от канала связи? А – средой распространения сигнала В – типом получателя информации С – видом помехи в канале Д - все ответы верны 2. Лицензирование деятельности в области технической защиты информации и сертификацию средств защиты осуществляет А – ФСБ В – СВР С – ФСТЭК Д – МО	*Правильный ответ – 1балл.* *Дан неверный ответ – 0 баллов*
Базовый **Уметь**	1. По способу формирования электрического сигнала активные акустоэлектрические преобразователи могут быть А – индуктивными, электродинамическими и пьезоэлектрическими В – емкостными, электродинамическими и электромагнитными С - электродинамическими, электромагнитными и пьезоэлектрическими Д – индуктивными,	*Правильный ответ – 1балл.* *Дан неверный ответ – 0 баллов*

	емкостными и резистивными 2. Какие способы перехвата речевой информации требуют проникновения в выделенное помещение А) Перехват акустических колебаний, возникающих при ведении разговоров, закладными устройствами с датчиками микрофонного типа. Б) Перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, закладными устройствами с датчиками контактного типа. В) Перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, электронными стетоскопами. Г) Перехват информативных электрических сигналов, возникающих вследствие акустоэлектрических преобразований акустических сигналов элементами ВТСС, техническими средствами, построенными на базе низкочастотных усилителей, подключаемыми к соединительных линий ВТСС. Д) Перехват акустической (речевой) информации методом «высокочастотного облучения» ВТСС, имеющих в своем составе акустоэлектрические преобразователи	
Базовый **Знать**	1. Причины, вызывающие появление опасных сигналов в цепях электропитания А – наведение в цепях ЭДС полями НЧ и ВЧ побочных излучений ОТСС В – модуляция тока электропитания токами радиоэлектронного средства С – попадание опасного сигнала в цепи электропитания через паразитные связи элементов схемы и блоков питания Д – наличие в радиоэлектронном средстве импульсного блока питания Е – все ответы верны 2. К техническим средствам добывания информации относятся А – средства обнаружения, распознавания и локализации В – средства наблюдения и	*Правильный ответ – 1балл.* *Дан неверный ответ – 0 баллов*

	средства подслушивания С – средства перехвата и физико-химического анализа веществ Д – варианты А и С Е – варианты В и С	

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

а) Основная литература

Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю. Н. Сычев; Российский экономический университет им. Г.В. Плеханова. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 201 с. - (Высшее образование: Магистратура). - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=420080

Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / О. В. Прохорова. - 5-е изд., стер. - Санкт-Петербург : Лань, 2023. - 124 с. - Книга из коллекции Лань - Информатика. – Режим доступа: https://e.lanbook.com/book/293009

Игнатьев Е. Б. Защита информации: криптоалгоритмы хеширования [Электронный ресурс] : учебное пособие для вузов / Е. Б. Игнатьев. - Санкт-Петербург : Лань, 2023. - 264 с. - Книга из коллекции Лань - Информатика. – Режим доступа: https://e.lanbook.com/book/311792

б) Дополнительная литература:

Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ В.В. Креопалов.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 278 с.— Режим доступа: http://www.iprbookshop.ru/10871.html

Титов, А.А. Инженерно-техническая защита информации: учебное пособие / А.А. Титов. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с.; [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208567

Закон Российской Федерации « Об информации, информатизации и защите информации». [Электронный ресурс]. - URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

Иванов А.В. Защита речевой информации от утечки по акустоэлектрическим каналам [Электронный ресурс]: учебное пособие/ А.В. Иванов, В.А Трушин.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2012.— 43 с.— Режим доступа: http://www.iprbookshop.ru/44919.html

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.

VII. Методические указания для обучающихся по освоению дисциплины

Примерный перечень вопросов для опросов на практических занятиях и темы рефератов:

1. Характеристика инженерно-технической защиты информации.
2. Основные проблемы инженерно-технической защиты информации.
3. Представление сил и средств защиты информации в виде системы.
4. Основные параметры систем защиты информации.
5. Цели и задачи защиты информации.
6. Ресурсы, выделяемые на защиту информации.
7. Принципы защиты информации техническими средствами.
8. Основные направления инженерно-технической защиты информации.
9. Показатели эффективности инженерно-технической защиты информации.
10. Виды, источники и носители защищаемой информации.
11. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
12. Понятие о текущей и эталонной признаковой структуре.
13. Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов.
14. Состав и краткая характеристика основные и вспомогательные технические средства и системы.
15. Образование опасных сигналов в результате побочных электромагнитных излучений и наводок.
16. Основные задачи и органы технической разведки. Принципы технической разведки.
17. Основные этапы и процессы добывания информации технической разведки. Классификация технической разведки.
18. Возможности видов технической разведки. Основные направления развития технической разведки..
19. Понятие и особенности утечки информации.
20. Структура, классификация и основные характеристики технических каналов утечки информации.
21. Классификация способов инженерной защиты и технической охраны объектов.

22. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления охраной.
23. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара. Автоматизация процессов охраны.
24. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения.
25. Методы технического закрытия речевых сигналов.
26. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях.
27. Распространение оптических сигналов в атмосфере и в светопроводах.
28. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.
29. Характеристика среды распространения сигналов различных технических каналов утечки информации.
30. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация полей.
31. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.
32. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.
33. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей.
34. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз.
35. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.
36. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения.
37. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления.
38. Основные задачи, структура и характеристика государственной системы противодействия технической разведке.
39. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.
40. Основные организационные и технические меры по защите информации.
41. Виды контроля эффективности инженерно-технической защиты информации.
42. Методы технического контроля.
43. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

44. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.

45. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации.

46. Методические рекомендации по выбору рациональных вариантов защиты.

47. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в помещении.

Требования к рейтинг-контролю.

Модули.	Виды контроля.	Максимальное количество баллов.	Формы контрольных испытаний.
Модуль I.	Текущий.	25	1) контроль посещения занятий, 2) устный опрос, 3) контроль за выполнением индивидуальных заданий.
	Рубежный.	25	1) устный опрос, 2) контрольная работа.
Модуль II.	Текущий.	25	1) контроль посещения занятий, 2) устный опрос, 3) контроль за выполнением индивидуальных заданий.
	Рубежный.	25	1) устный опрос, 2) контрольная работа.

Перечень вопросов для зачета

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.

2. Принципы защиты информации техническими средствами.

3. Основные направления инженерно-технической защиты информации.

4. Показатели эффективности инженерно-технической защиты информации.

5. Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты.

6. Семантическая информация, циркулирующая в человеческом обществе. Профессиональные языки.

7. Признаковая информация. Информация о видовых признаках, о признаках сигналов, о признаках веществ.

8. Структурирование информации.

9. Классификация демаскирующих признаков.

10. Опознавательные признаки и признаки деятельности.

11. Видовые демаскирующие признаки.

12. Демаскирующие признаки сигналов.

13. Демаскирующие признаки веществ. Именные, прямые и косвенные демаскирующие признаки.

14. Виды источников и носителей информации.

15. Прямые и косвенные источники семантической информации.

16. Принципы записи и съема информации с её носителя.

17. Источники функциональных сигналов. Понятие модуляции, манипуляции, демодуляции.

18. Побочные электромагнитные излучения и наводки Угрозы утечки информации. Угрозы преднамеренных воздействий. Угрозы случайных воздействий.

19. Технические каналы утечки информации: наблюдение, подслушивание, перехват.

20. Источники угроз безопасности информации.

21. Опасные сигналы и их источники.

22. Способы и средства наблюдения в оптическом диапазоне. Обработка информации в оптическом приемнике.

23. Способы и средства наблюдения в радиодиапазоне. Способы и средства перехвата сигналов.

24. Обработка информации в радиоприемнике.

25. Способы и средства подслушивания. Обработка информации в акустическом приемнике.

26. Типовая структура и виды технических каналов утечки информации.

27. Каналы утечки речевой информации.

28. Каналы утечки информации при её передаче по каналам связи.

29. Каналы утечки видовой информации.

30. Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.

31. Каналы утечки информации за счет побочных электромагнитных излучений и наводок.

32. Средства маскировки и дезинформирования в оптическом и радиодиапазонах.

33. Средства звукоизоляции из звукопоглощения.

34. Средства обнаружения, локализации и подавления сигналов закладных устройств.

35. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления.

36. Генераторы линейного и пространственного зашумления.

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

1) лекционные занятия в аудитории, с использованием мультимедийной установки;
2) практические занятия с использованием средств мультимедиа;
3) использование необходимого программного обеспечения

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
GIMP 2.8.20	бесплатно
Google Chrome	бесплатно
Java SE Development Kit 8 Update 45 (64-bit)	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 бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
Microsoft SQL Server 2014 Express LocalDB	бесплатно
Microsoft Visio Professional 2013	Акт на передачу прав №785 от 06.08.2021 г.
Microsoft Visual Studio Ultimate 2013 с обновлением 4	Акт на передачу прав №785 от 06.08.2021 г.
Microsoft Web Deploy 3.5	бесплатно
Microsoft Windows 10 Enterprise	Акт на передачу прав №785 от 06.08.2021 г.
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	бесплатно
Python 3.4.3	бесплатно
Unity Web Player	бесплатно
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски. Класс ПЭВМ класса Intel с установленным программным обеспечением для самостоятельной работы.

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.			
2.			