

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Тверской государственный технический университет»
(ТвГТУ)

УТВЕРЖДАЮ

Проректор по учебной работе
_____ Э.Ю. Майкова

« ____ » _____ 2019 г.

РАБОЧАЯ ПРОГРАММА

дисциплины обязательной части Блока 1 «Дисциплины (модули)»
«Методы и средства защиты информации»

Направление подготовки бакалавров – 09.03.01 Информатика и вычислительная техника

Направленность (профиль) – Вычислительные машины, комплексы, системы и сети

Тип задач профессиональной деятельности – производственно-технологический

Форма обучения – очная и заочная

Факультет информационных технологий

Кафедра электронных вычислительных машин

Тверь 2019

Рабочая программа дисциплины соответствует ОХОП подготовки бакалавров в части требований к результатам обучения по дисциплине и учебному плану.

Разработчик программы: к.т.н., профессор

А.Р. Хабаров

Программа рассмотрена и одобрена на заседании кафедры ЭВМ 29.03.2019 г. протокол № 5.

Заведующий кафедрой ЭВМ

А.Р. Хабаров

Согласовано:

Начальник УМО УМУ

Д.А. Барчуков

Начальник отдела
комплектования
зональной научной
библиотеки

О.Ф. Жмыхова

1. Цель и задачи дисциплины

Основной целью изучения дисциплины «Методы и средства защиты информации» является ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации и аутентификации пользователей, борьбы с вирусами.

Задачи дисциплины: овладение современными методами и средствами защиты компьютерной информации.

2. Место дисциплины в образовательной программе

Дисциплина относится к обязательной части Блока 1 ОП ВО. Для изучения курса требуются знания дисциплин «Высшая математика», «Алгоритмические языки и программирование», «Организация ЭВМ и систем», «Операционные системы».

Курс «Методы и средства защиты информации» является одной из дисциплин, завершающих формирование специалистов по вычислительной технике.

3. Планируемые результаты обучения по дисциплине

3.1. Планируемые результаты обучения по дисциплине

Компетенции, закрепленные за дисциплиной в ОХОП:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности.

Индикатор компетенции, закреплённый за дисциплиной в ОХОП:

ИОПК-3.2. Решает стандартные задачи профессиональной деятельности с использованием сетевых технологий и учетом основных требований информационной безопасности.

Показатели оценивания индикатора достижения компетенции:

ИОПК-3.2.:

Знать:

31: Правовые основы защиты компьютерной информации.

32: Организационные, технические и программные методы и средства обеспечения информационной безопасности компьютерных систем. Стандарты; модели и методы шифрования.

Уметь:

У1: Самостоятельно анализировать и оценивать угрозы информации. Ставить и решать задачи, связанные с построением систем защиты информации.

ОПК-9. Способен осваивать методики использования программных средств для решения практических задач.

Индикаторы компетенции, закреплённые за дисциплиной в ОХОП:

ИОПК-9.1. Знает методики использования программных средств для решения практических задач.

ИОПК-9.2. Использует пакеты прикладных программ для решения задач в различных областях.

Показатели оценивания индикатора достижения компетенции:

ИОПК-9.1.:

Знать:

31: Методы идентификации и аутентификации пользователей; основные инструменты обеспечения многоуровневой безопасности в компьютерных системах.

32: Методы выявления угроз информационной безопасности на предприятии, выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; аудита безопасности информационных систем.

Уметь:

У1: Применять эффективные методы управления безопасностью.

ИОПК-9.2.:

Знать:

31: Методы защиты компьютерной информации в различных предметных областях.

32: Методы шифрования хранимых и передаваемых данных.

Уметь:

У1: Работать с программно-аппаратными средствами защиты компьютерной информации.

У2: Работать с различными операционными системами и их администрирования с целью обеспечения информационной безопасности компьютерных систем.

3.2. Технологии, обеспечивающие формирование компетенций

Проведение лекционных занятий, выполнение лабораторных работ, самостоятельная работа под руководством преподавателя.

4. Трудоемкость дисциплины и виды учебной работы

Таблица 1а. Распределение трудоемкости дисциплины по видам учебной работы

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	Зачетные единицы	Академические часы
Общая трудоемкость дисциплины	2	72
Аудиторные занятия (всего)		52
В том числе:		
Лекции		26
Практические занятия (ПЗ)		не предусмотрены
Лабораторные работы (ЛР)		26
Самостоятельная работа обучающихся (всего)		20
В том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Реферат		не предусмотрен
Другие виды самостоятельной работы: - подготовка к защите лабораторных работ		10
Текущий контроль успеваемости и промежуточная аттестация (зачёт)		10
Практическая подготовка при реализации дисциплины (всего)		0

Таблица 1б. Распределение трудоемкости дисциплины по видам учебной работы

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	Зачетные единицы	Академические часы
Общая трудоемкость дисциплины	2	72
Аудиторные занятия (всего)		8
В том числе:		
Лекции		4
Практические занятия (ПЗ)		не предусмотрены
Лабораторные работы (ЛР)		4
Самостоятельная работа обучающихся (всего)		64
В том числе:		
Курсовая работа		не предусмотрена
Курсовой проект		не предусмотрен
Расчетно-графические работы		не предусмотрены
Реферат		не предусмотрен
Другие виды самостоятельной работы: - изучение теоретической части дисциплины;		55
- подготовка к защите лабораторных работ		5

Текущий контроль успеваемости и промежуточная аттестация (зачёт)		4
Практическая подготовка при реализации дисциплины (всего)		0

5. Структура и содержание дисциплины

5.1. Структура дисциплины

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2а. Модули (разделы) дисциплины, трудоемкость в часах и виды учебной работы

№	Наименование модуля	Труд-ть часы	Лекции	Практ. занятия	Лаб. работы	Сам. работа
1	Основные понятия защиты информации. Основы информационной безопасности	10	4	-	4	2
2	Программно-аппаратная защита информации	12	6	-	4	2
3	Криптографические методы защиты информации	32	12	-	12	8
4	Организационное и правовое обеспечение информационной безопасности	18	4	-	6	8
Всего на дисциплину		72	26	-	26	20

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2б. Модули (разделы) дисциплины, трудоемкость в часах и виды учебной работы

№	Наименование модуля	Труд-ть часы	Лекции	Практ. занятия	Лаб. работы	Сам. работа
1	Основные понятия защиты информации. Основы информационной безопасности	13	0.5	-	0.5	12
2	Программно-аппаратная защита информации	18	1	-	1	16
3	Криптографические методы защиты информации	24	2	-	2	20
4	Организационное и правовое обеспечение информационной безопасности	17	0.5	-	0.5	16
Всего на дисциплину		72	4	-	4	64

5.2. Содержание дисциплины

МОДУЛЬ 1

Цель и задачи дисциплины, ее роль и место в общей системе подготовки специалиста. Понятие «защита информации». Функции и задачи защиты информации. Методы и средства защиты информации. Внешние и внутренние источники угроз. Стандарты информационной безопасности. Предмет и объекты защиты информации в автоматизированных системах обработки данных. Модель угроз, модель нарушителя. Информационная война. Перспективные направления развития средств и методов защиты информации.

МОДУЛЬ 2

Идентификация и аутентификация. Управление доступом, аутентификация, аудит. Виды угроз. Политики безопасности. Защита программного обеспечения от несанкционированного использования. Антивирусная защита компьютерных систем. Пакетные фильтры и межсетевые экраны, их классификация и особенности применения. Биометрическая аутентификация пользователей.

МОДУЛЬ 3

Основные задачи и понятия криптографии. Симметричное и асимметричное шифрование в задачах защиты информации. Классификация шифров. Модели шифров. Основные требования к шифрам. Криптографическая стойкость шифров. Алгоритмы идентификации. Электронно-цифровая подпись. Криптоключи. Криптоанализ.

МОДУЛЬ 4

Категории информации по условиям доступа к ней и распространения. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативно-правовых актов, регулирующих обеспечение информационной безопасности в РФ. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна. Интеллектуальная собственность и авторское право. Методы обеспечения физической безопасности. Организация режима секретности. Инженерно-техническая защита информации.

5.3. Лабораторные работы

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3а. Тематика, форма лабораторных работ (ЛР) и их трудоемкость

№ пп.	Порядковый номер модуля. Цели лабораторных работ	Наименование лабораторных работ	Трудоемкость в часах
1.	Модуль 1. Цель: Изучение нормативно-правовой базы. Ознакомление с методикой	Лабораторная работа № 1. Нормативно-методическое обеспечение КСЗИ	2
		Лабораторная работа № 2. Оценочный расчет защищенности помещений от утечки речевых	2

	расчета защищенности помещений	сообщений по акустическому каналу	
2	Модуль 2. Цель: Использование парольной аутентификации для разграничения полномочий пользователей компьютерных систем	Лабораторная работа № 3. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации	4
3	Модуль 3. Цель: Изучение и практическая реализация методов криптографической защиты информации	Лабораторная работа № 4. Дешифровка сообщений методом полного перебора всех возможных значений ключа шифрования	2
		Лабораторная работа № 5. Использование статистических характеристик распределения букв русского алфавита при дешифровке текста	2
		Лабораторная работа № 6. Разработка крипто-системы на основе алгоритма RSA	6
		Лабораторная работа № 7. Выработка общего-секретного ключа по алгоритму Диффи–Хэлла	2
4	Модуль 4. Цель: Проведение анализа угроз информационной безопасности, выработка практических рекомендаций по повышению показателей защищенности информации	Лабораторная работа № 8. Использование функций криптографического интерфейса <i>Windows</i> для защиты информации	2
		Лабораторная работа № 9. Определение показателей защищенности информации при несанкционированном доступе	4

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3б. Тематика, форма лабораторных работ (ЛР) и их трудоемкость

№ пп.	Порядковый номер модуля. Цели лабораторных работ	Наименование лабораторных работ	Трудоемкость в часах
1	Модуль 1. Цель: Изучение нормативно-правовой базы. Ознакомление с методикой расчета защищенности помещений	Лабораторная работа № 1. Оценочный расчет защищенности помещений от утечки речевых сообщений по акустическому каналу	0.5
2	Модуль 2. Цель: Использование парольной аутентификации для разграничения полномочий пользователей компьютерных систем	Лабораторная работа № 2. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации	0.5
3	Модуль 3. Цель: Изучение и практическая реализация мето-	Лабораторная работа №3. Дешифровка сообщений методом полного перебора всех возможных значений ключа шифрования	0.5

	дов криптографической защиты информации	Лабораторная работа № 4. Использование статистических характеристик распределения букв русского алфавита при дешифровке текста	0.5
		Лабораторная работа № 5. Разработка крипто-системы на основе алгоритма RSA	1.5
4	Модуль 4. Цель: Проведение анализа угроз информационной безопасности, выработка практических рекомендаций по повышению показателей защищенности информации	Лабораторная работа № 6. Определение показателей защищенности информации при несанкционированном доступе	0.5

5.4. Практические занятия

Учебным планом практические занятия не предусмотрены.

6. Самостоятельная работа обучающихся и текущий контроль успеваемости

6.1. Цели самостоятельной работы

Формирование способностей к самостоятельному познанию и обучению, поиску литературы, обобщению, оформлению и представлению полученных результатов, их критическому анализу, поиску новых и неординарных решений, аргументированному отстаиванию своих предложений, умений подготовки выступлений и ведения дискуссий.

6.2. Организация и содержание самостоятельной работы

Самостоятельная работа заключается в изучении отдельных тем курса по заданию преподавателя по рекомендуемой им учебной литературе, в подготовке к лабораторным занятиям, текущему контролю успеваемости, зачёту.

В рамках дисциплины выполняется 9 лабораторных работ по очной форме обучения и 6 лабораторных работ по заочной форме обучения

При защите лабораторной работы студент показывает отчёт о выполненной работе. Докладывает и аргументировано защищает результаты выполненной работы, отвечая при этом на вопросы преподавателя, убеждая его в том, что работа выполнена верно, цели работы полностью достигнуты.

В случае пропуска занятия студент должен взять тематику занятия и задание на лабораторную работу у преподавателя, изучить и отработать материал в часы самостоятельной работы: написать конспект пропущенной лекции и выполнить лабораторную работу.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература по дисциплине

1. Краковский, Ю.М. Методы защиты информации : учебное пособие для вузов / Ю.М. Краковский. - 3-е изд. - Санкт-Петербург [и др.] : Лань, 2021. - ЭБС Лань. - Текст : электронный. - ISBN 978-5-8114-5632-1. - URL: <https://e.lanbook.com/book/156401>. - (ID=145974-0).
2. Казарин, О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О.В. Казарин, А.С. Забабурин. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - ISBN 978-5-9916-9043-0. - URL: <https://urait.ru/bcode/491249>. - (ID=145962-0).
3. Зенков, А.В. Информационная безопасность и защита информации : учебное пособие для вузов / А.В. Зенков. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - ISBN 978-5-534-14590-8. - URL: <https://urait.ru/bcode/497002>. - (ID=140920-0).

7.2. Дополнительная литература по дисциплине

1. Фот, Ю.Д. Методы защиты информации: учебное пособие по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» / Ю.Д. Фот, Н.П. Мошуров; Оренбургский государственный университет. - Оренбург : Оренбургский государственный университет, 2019. - ЭБС Лань. - Текст : электронный. - ISBN 978-5-7410-2296-2. - URL: <https://e.lanbook.com/book/159977>. - (ID=145964-0).
2. Мельников, Ю.Н. Методы и средства защиты информации : учеб. пособие : в составе учебно-методического комплекса / Ю.Н. Мельников. - [Б. м.], [б. г.]. - (УМК-У). - Сервер. - Текст: электронный. - 0-00. - URL: <http://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/97215>. - (ID=97215-1).
3. Внуков, А.А. Защита информации: учебное пособие для вузов / А.А. Внуков. - 3-е изд. - Москва : Юрайт, 2022. - (Высшее образование). - Образовательная платформа Юрайт. - Текст : электронный. - ISBN 978-5-534-07248-8. - URL: <https://urait.ru/bcode/490277>. - (ID=135647-0).
4. Прохорова, О.В. Информационная безопасность и защита информации : учебник для вузов / О.В. Прохорова. - 3-е изд. - Санкт-Петербург [и др.] : Лань, 2021. - ЭБС Лань. - Текст : электронный. - ISBN 978-5-8114-7970-2. - URL: <https://e.lanbook.com/book/169817>. - (ID=145977-0).
5. Леонтьев, А.С. Защита информации: учебное пособие / А.С. Леонтьев; МИРЭА - Российский технологический университет. - Москва : МИРЭА - Российский технологический университет, 2021. - ЭБС Лань. - Текст : электронный. - URL: <https://e.lanbook.com/book/182491>. - (ID=145965-0).
6. Каширская, Е.Н. Защита информации в информационно-управляющих системах : учебное пособие / Е.Н. Каширская, М.А. Макаров; МИРЭА - Российский технологический университет. - Москва : МИРЭА - Российский технологический университет, 2021. - ЭБС Лань. - Текст : электронный. - URL: <https://e.lanbook.com/book/182491>. - (ID=145965-0).

университет, 2020. - ЭБС Лань. - Текст: электронный. - URL: <https://e.lanbook.com/book/167621>. - (ID=145978-0).

7. Пугин, В.В. Защита информации в компьютерных информационных системах : учебное пособие / В.В. Пугин, Е.Ю. Голубничая, С.А. Лабада; Поволжский государственный университет телекоммуникаций и информатики. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2018. - ЭБС Лань. - Текст : электронный. - URL: <https://e.lanbook.com/book/182299>. - (ID=145967-0).

8. Киздермишов, А.А. Актуальные вопросы защиты информации : учебное пособие по направлениям подготовки 09.03.01 «Информатика и вычислительная техника» 27.03.04 «Управление в технических системах» / А.А. Киздермишов, А.В. Шопин; Адыгейский государственный университет. - Майкоп: Адыгейский государственный университет, 2018. - ЭБС Лань. - Текст: электронный. - URL: <https://e.lanbook.com/book/146128>. - (ID=145349-0).

9. Исаева, М.Ф. Техническая защита информации: учебное пособие для вузов / М.Ф. Исаева; Петербургский государственный университет путей сообщения Императора Александра I. - Санкт-Петербург : Петербургский государственный университет путей сообщения Императора Александра I, 2017. - ЭБС Лань. - Текст : электронный. - ISBN 978-5-7641-1008-0. - URL: <https://e.lanbook.com/book/101600>. - (ID=145976-0).

10. Введение в информационную безопасность и защиту информации : учебное пособие / В.А. Трушин [и др.]; Новосибирский государственный технический университет. - Новосибирск: Новосибирский государственный технический университет, 2017. - ЭБС Лань. - Текст : электронный. - ISBN 978-5-7782-3233-4. - URL: <https://e.lanbook.com/book/118219>. - (ID=145942-0).

11. Современные методы обеспечения защиты информации : учебное пособие / В.Г. Дмитриев [и др.]; Башкирский государственный педагогический университет имени М. Акмуллы. - Уфа : Башкирский государственный педагогический университет имени М. Акмуллы, 2016. - ЭБС Лань. - Текст : электронный. - URL: <https://e.lanbook.com/book/90965>. - (ID=145350-0).

12. Васильев, В.И. Интеллектуальные системы защиты информации : учеб. пособие для вузов по специализациям спец. «Комплексное обеспечение информационной безопасности автоматизированных систем» / В.И. Васильев. - 2-е изд. ; испр. - Москва : Машиностроение, 2013. - ЭБС Лань. - Текст : электронный. - ISBN 978-5-94275-667-3. - URL: http://e.lanbook.com/books/element.php?pl1_id=5792. - (ID=110306-0).

13. Разработка системы технической защиты информации: учебное пособие / В.И. Аверченков [и др.]. - Брянск : Брянский государственный технический университет, 2012. - ил. - ЦОР IPR SMART. - Текст : электронный. - ISBN 5-89838-358-1. - URL: <https://www.iprbookshop.ru/7005.html>. - (ID=145818-0).

14. Методы и средства инженерно-технической защиты информации : учебное пособие / В.И. Аверченков [и др.]. - Брянск : Брянский государственный технический университет, 2012. - ил. - ЦОР IPR SMART. - Текст : электронный. - ISBN 5-89838-357-3. - URL: <https://www.iprbookshop.ru/7000.html>. - (ID=145819-0).

15. Пушкарев, В.В. Защита информационных процессов в компьютерных системах: учебное пособие / В.В. Пушкарев, В.П. Пушкарев; Томский государственный университет систем управления и радиоэлектроники. - Москва: Томский государственный университет систем управления и радиоэлектроники, 2012. - ЭБС Лань. - Текст : электронный. - URL: <https://e.lanbook.com/book/4925>. - (ID=145966-0).

16. Сердюк, В.А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк; Государственный университет - Высшая Школа Экономики. - Москва: Государственный университет - Высшая Школа Экономики, 2011. - 571, [2] с. : ил. - Текст : непосредственный. - ISBN 978-5-7598-0698-1 : 299 p. - (ID=85474-30).

7.3 Методические материалы

1. Методические указания к курсовой работе по дисциплине «Методы и средства защиты информации». Направление подготовки бакалавров - 09.03.01 Информатика и вычислительная техника. Профиль - Вычислительные машины, комплексы, системы и сети: в составе учебно-методического комплекса / Каф. Электронно-вычислительные машины; сост. А.Р. Хабаров. - Тверь : ТвГТУ, 2017. - (УМК-М). - Сервер. - Текст: электронный. - (ID=124349-0).

2. Вопросы к зачету по дисциплине «Методы и средства защиты информации». Направление подготовки бакалавров - 09.03.01 Информатика и вычислительная техника. Профиль - Вычислительные машины, комплексы, системы и сети: в составе учебно-методического комплекса / каф. Электронно-вычислительные машины; сост. А.Р. Хабаров. - Тверь: ТвГТУ, 2017. - (УМК-В). - Сервер. - Текст: электронный. - (ID=124348-0).

3. Фомин, Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: методические указания / Д.В. Фомин; Амурский государственный университет. - Благовещенск: Амурский государственный университет, 2017. - ЭБС Лань. - Текст : электронный. - URL: <https://e.lanbook.com/book/156494>. - (ID=145950-0).

4. Титова, Л.Н. Информационная безопасность и защита информации : учебно-методическое пособие / Л.Н. Титова; Башкирский государственный педагогический университет имени М. Акмуллы. - Уфа : Башкирский государственный педагогический университет имени М. Акмуллы, 2013. - ЭБС Лань. - Текст : электронный. - URL: <https://e.lanbook.com/book/56704>. - (ID=145947-0).

7.4 Программное обеспечение

1. Операционная система Microsoft Windows: лицензии № ICM-176609 и № ICM-176613 (Azure Dev Tools for Teaching).

2. Microsoft Office 2019 Russian Academic: OPEN No Level: лицензия № 41902814.

7.5. Специализированные базы данных, справочные системы, электронно-библиотечные системы, профессиональные порталы в Интернет

ЭБС и лицензионные ресурсы ТвГТУ размещены:

1. Ресурсы: <https://lib.tstu.tver.ru/header/obr-res>
2. ЭКТвГТУ: <https://elib.tstu.tver.ru/MegaPro/Web>
3. ЭБС «Лань»: <https://e.lanbook.com/>
4. ЭБС «Университетская библиотека онлайн»: <https://www.biblioclub.ru/>
5. ЭБС «IPRBooks»: <https://www.iprbookshop.ru/>
6. Электронная образовательная платформа «Юрайт» (ЭБС «Юрайт»): <https://urait.ru/>
7. Научная электронная библиотека eLIBRARY: <https://elibrary.ru/>
8. Информационная система «ТЕХНОРМАТИВ». Конфигурация «МАК-СИМУМ» : сетевая версия (годовое обновление): [нормативно-технические, нормативно-правовые и руководящие документы (ГОСТы, РД, СНИПы и др.]. Диск 1,2,3,4. - М. :Технорматив, 2014. - (Документация для профессионалов). - CD. - Текст : электронный. - 119600 р. – (105501-1).
9. База данных учебно-методических комплексов: <https://lib.tstu.tver.ru/header/umk.html>

УМК размещен: <https://elib.tstu.tver.ru/MegaPro/GetDoc/Megapro/111777>.

8. Материально-техническое обеспечение

Кафедра электронных вычислительных машин имеет аудитории для проведения лекционных и лабораторных занятий по дисциплине; специализированный учебный класс для проведения компьютерных практикумов и самостоятельной работы, оснащенный современной компьютерной и офисной техникой, необходимым программным обеспечением, электронными учебными пособиями и законодательно-правовой поисковой системой, имеющий безлимитный выход в глобальную сеть.

9. Оценочные средства для проведения промежуточной аттестации

9.1. Оценочные средства для проведения промежуточной аттестации в форме экзамена

Учебным планом экзамен не предусмотрен.

9.2. Оценочные средства промежуточной аттестации в форме зачёта

1. Шкала оценивания промежуточной аттестации – «зачтено», «не зачтено».

2. Вид промежуточной аттестации в форме зачёта.

Вид промежуточной аттестации устанавливается преподавателем по согласованию с заведующим кафедрой по результатам текущего контроля знаний обучающегося без дополнительных контрольных испытаний.

3. Критерии проставления зачёта при промежуточной аттестации без выполнения дополнительного итогового контрольного испытания.

Оценка «зачтено» выставляется обучающемуся при условии выполнения и защиты им всех практических работ, предусмотренных в Программе.

9.3. Оценочные средства для проведения промежуточной аттестации в форме курсовой работы

Учебным планом курсовая работа или курсовой проект не предусмотрены.

10. Методические рекомендации по организации изучения дисциплины

Студенты перед началом изучения дисциплины ознакомлены с системами кредитных единиц и балльно-рейтинговой оценки.

Студенты, изучающие дисциплину, обеспечиваются электронными изданиями или доступом к ним, учебно-методическим комплексом по дисциплине.

11. Внесение изменений и дополнений в рабочую программу дисциплины

Содержание рабочих программ дисциплин ежегодно обновляется протоколами заседаний кафедры по утвержденной «Положением о структуре, содержании и оформлении рабочих программ дисциплин по образовательным программам, соответствующим ФГОС ВО с учетом профессиональных стандартов» форме.