Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП

_____ А.А. Голубев

«16» 03 2024 г.

Рабочая программа дисциплины (с аннотацией)

Защита экономической информации

Направление подготовки

01.03.01 Математика

Профиль подготовки

Математическое обеспечение экономической деятельности

Для студентов 3 курса

Форма обучения очная

Составители: _____

д.ф.-м.н., профессор Шаров Г.С.

к.т.н., доцент Семёнов С.В.

Тверь, 2024

I. Аннотация

1. Цели и задачи дисциплины

Целью освоения дисциплины является: освоение заданных дисциплинарных компетенций в области применения методов обеспечения экономической безопасности государства, отдельных организаций и предприятий об основных экономических проблемах зашиты информации.

Задачами освоения дисциплины являются:

1. Изучение закономерностей влияния видов хозяйственной деятельности на экономику предприятия, с учётом решения проблем защиты информации.
2. Формирование умений находить взаимосвязи методов защиты информации и экономической эффективности работы предприятия.
3. Овладение навыками оценки изменения финансовых результатов от хозяйственной деятельности предприятия в зависимости от использования средств защиты информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к группе дисциплин по выбору в части, формируемой участниками образовательных отношений. Дисциплина формирует профессиональные компетенции. Её изучение базируется на следующих дисциплинах: Экономика, Теория вероятностей и математическая статистика, Основы программирования.

Знания и практические навыки, полученные при изучении дисциплины «Защита экономической информации», используются студентами при разработке курсовых и выпускных работ.

3. Объём дисциплины: 5 зачётных единиц, 180 академических часов,
в том числе:
контактная аудиторная работа: 68 часов,
в том числе
лекции 34 часа, в том числе практическая подготовка – 0 часов,
практические занятия 34 часа, в том числе практическая подготовка – 6 часов;
самостоятельная работа: 112 часов, в том числе контроль 27 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ПК-1 Способен осуществлять научно-исследовательскую работу на основе математических и естественных наук, основ программирования и информационных технологий	ПК-1.2 Проводит анализ, обоснование и выбор решения прикладных задач ПК-1.3 Проектирует научное исследование в соответствии с задачами профессиональной деятельности

5. Форма промежуточного контроля: экзамен (6 семестр).

6. Язык преподавания русский**.**

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

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе контроль (час.)
		Лекции	Практические занятия	в т.ч. практич. подготовка	
Тема 1. Информационная безопасность и уровни её обеспечения.	24	2	2	*0*	20
Тема 2. Основные нормативные документы в сфере обеспечения информационной безопасности.	24	2	2	*0*	20
Тема 3. Информационная безопасность вычислительных сетей.	40	10	10	*0*	20
Тема 4. Криптографические методы защиты информации.	46	10	10	*4*	26
Тема 5. Технологии и методы построения защищенных информационных систем	46	10	10	*2*	26
ИТОГО	180	34	34	*6*	112

Учебная программа дисциплины

Тема 1. Информационная безопасность и уровни её обеспечения.

Введение в информационную безопасность. Понятие информационной безопасности. Роль информационной безопасности в современном мире. История безопасности. Компоненты защиты. Комплексный подход к обеспечению информационной безопасности. Лицензирование деятельности в области защиты информации. Сертификация средств защиты информации. Законодательство в сфере информационной безопасности. Уровни информационной безопасности: законодательный, административный, процедурный, программно-технический.

Тема 2. Основные нормативные документы в сфере обеспечения информационной безопасности.

Правовую основу обеспечения экономической безопасности составляют: Конституция РФ; международные договоры РФ; федеральные конституционные законы; Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»; другие федеральные законы и иные нормативные правовые акты РФ; постановления Правительства РФ; законы и иные нормативные правовые акты субъектов РФ, органов местного самоуправления, принятые в пределах их компетенции в области экономической безопасности.

Тема 3. Технологии и методы построения защищенных информационных систем.

Информационные системы, Безопасность корпоративных информационных систем, основные понятия, методологии безопасности. Организационно-методо-

логические основы оценки информационной безопасности. Нормативно-правовая база информационной безопасности корпоративных информационных систем. Оценка выполнения требований по обеспечению защиты от несанкционированного доступа к информации в корпоративных информационных системах. Оценка выполнения требований к процессам системы управления информационной безопасностью (СУИБ). Оценка выполнения требований к организационно-правовому обеспечению применения средств защиты информации. Оценка выполнения требований по обеспечению защиты информации от вредоносных программ. Оценка выполнения требований по обеспечению информационной безопасности компонентов корпоративных информационных систем.

Тема 4. Криптографические методы защиты информации.

Основные понятия криптографии. Простейшие шифры. Симметричные шифры. Ассиметричные системы.

Тема 5. Технологии и методы построения защищенных информационных систем.

Основные понятия, определения и проблемы в области построения защищенных систем обработки информации. Обзор и сравнительный анализ стандартов в области защиты информационных систем. Исследование причин нарушений безопасности информационных систем. Анализ и оценка информационных рисков, угроз и уязвимостей информационной системы. Специальные методы моделирования, используемые при построении защищенных систем обработки информации. Методы принятия решений, используемые при выборе эффективных проектов защиты информации в информационной системе. Перспективные направления в области проектирования защищенных систем обработки информации.

III. Образовательные технологии

Преподавание учебной дисциплины строится на сочетании аудиторных занятий и различных форм самостоятельной работы студентов.

Также на занятиях практикуется самостоятельная работа студентов, выполнение заданий в малых группах, письменные работы, моделирование дискуссионных ситуаций, работа с раздаточным материалом, привлекаются ресурсы сети INTERNET. Курс предусматривает выполнение контрольных и самостоятельных работ, письменных домашних заданий. В качестве форм контроля используются различные варианты взаимопроверки и взаимоконтроля.

Интерактивное взаимодействие студентов с одной стороны и преподавателя с другой, а также студентов между собой и с преподавателем во время практических занятий.

Образовательные технологии

1. Дискуссионные технологии
2. Информационные (цифровые)
3. Технологии развития критического мышления

Современные методы обучения

1. Активное слушание
2. Лекция (традиционная)

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

1. Оценочные материалы для проведения текущей аттестации

Типовое тестовое задание

1. Главными целями деятельности по обеспечению ИБ являются:

А. Ликвидация угроз объектам информационной безопасности

Б. Минимизация возможного ущерба

В. Исполнение законодательства в области ИБ

Г. Минимизация производственных издержек

Д. Повышение культуры производства

2. Негативные воздействия на объекты ИБ различают:

А. По степени изменения свойств объекта безопасности

Б. По возможности ликвидации последствий проявления угрозы

В. По величине затрат на предотвращение негативного воздействия

3. Укажите свойства угроз:

А. Избирательность

Б. Массовость

В. Стохастичность

Г. Предсказуемость

Д. Вредоносность

4. Выберите верное утверждение(я): Опасность …

А. Это совокупность факторов и условий, возникающих в процессе взаимодействия различных объектов (их элементов) и способных оказывать негативное воздействие на конкретный объект информационной безопасности

Б. Это состояние, в котором находится объект безопасности вследствие возникновения угрозы этому объекту

В. Свойство объекта взаимодействия или находящихся во взаимодействии элементов объекта безопасности, выступающих в качестве источника угроз

Г. является свойством объекта информационной безопасности и характеризует его способность противостоять проявлению угроз

5. По источнику угрозы ИБ делят на:

А. Внутренние

Б. Локальные

В. Общие

Г. Внешние

Д. Частные

6. По видам объектов безопасности угрозы ИБ делят на:

А. Угрозы собственно информации

Б. Угрозы персоналу объекта защиты

В. Угрозы программному обеспечению

Г. Угрозы правовому обеспечению

Д. Угрозы деятельности по обеспечению информационной безопасности

7. К косвенному ущербу ИБ относится:

А. Реализация украденного «стартапа» конкурентами

Б. Затраты на закупку сканеров отпечатков пальцев для доступа к рабочему месту

В. Найм специалистов по обеспечению ИБ

Г. попадание платного контента предприятия в бесплатные обменные сети

Д. Замедление бизнес-процессов в виду запрета доступа некоторым категориям

сотрудников к документам данного процесса и, как следствие, возросшая нагрузка на

сотрудников и увеличение фонда оплаты труда

8. ИБ направлена на обеспечение:

А. Целостности данных

Б. Репрезентативности данных

В. Адекватности данных

Г. Конфиденциальности данных

Д. Достоверности данных

Е. Доступности данных

9. Укажите виды классификаций угроз ИБ:

А. По источнику (его местонахождению)

Б. По вероятности реализации

В. По вероятности избежания угрозы ИБ

Г. По размерам наносимого ущерба

Д. По природе происхождения

Е. По природе средств защиты

Ж. По предпосылкам возникновения

З. По видам объектов безопасности

10. К прямому ущербу ИБ относится:

А. Потери из-за реализации «стартапа» компании конкурентами

Б. Затраты на закупку сканеров отпечатков пальцев для доступа к рабочему месту

В. Замедление бизнес-процессов в виду запрета доступа некоторым категориям

сотрудников к документам данного бизнес-процесса и, как следствие, возросшая нагрузка на сотрудников и увеличение фонда оплаты труда

Г. Использование конкурентами корпоративного механизма доступа к данным

Д. Проигрыш заявки на гос. закупку в виду утечки сведений по данной заявке

Ключ: 1-А,Б, 2-А,Б, 3-А,Г,Д 4-Б,Г, 5-А,Г, 6-А,Б,Д, 7-Б,В,Д, 8-А,Г,Е, 9-А,Б,Г,Д,Ж,З 10-А,Г,Д.

Примерные темы докладов

1. Информационные ресурсы, подлежащие защите в сфере финансовой деятельности.

2. Классификация угроз информационной безопасности и их сравнительный анализ.

3. Информационная безопасность в современных условиях хозяйствования.

Общегосударственные цели, задачи и методы обеспечения информационной безопасности.

4. Понятия о видах вирусов. Классификация вирусов и угрозы для информационной инфраструктуры хозяйствующих субъектов.

5. Вида возможных нарушений информационной безопасности в сфере финансовой деятельности.

6. Отечественные и международные стандарты обеспечения информационной безопасности.

7. Особенности современной нормативно-правовой и методологической базы обеспечения информационной безопасности.

8. Основные нормативные руководящие документы, касающиеся конфиденциальной информации и государственной тайны, нормативно-справочные документы по обеспечению информационной безопасности применяемые в финансовой деятельности.

9. Общие критерии оценки безопасности информационных систем и технологий ГОСТ 15408, как основа определения требований к обеспечению информационной безопасности.

10. Место информационной безопасности экономических систем в национальной безопасности страны.

11. Цели и задачи обеспечения национальной безопасности. Система целеполагания в структуре государственного и муниципального управления при обеспечении информационной безопасности.

12. Основные положения концепции информационной безопасности. Сравнительная таблица.

13. Государственные информационные

14. Взаимосвязь государственных и коммерческих информационных ресурсов (конфиденциальной информации и государственной тайны).

15. Модели безопасности, и их применение.

16. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Оценка системы защиты информации.

17. Оценка эффективности средств и механизмов обеспечения информационной безопасности.

18. Методы анализа способов нарушений информационной безопасности.

19. Программно-аппаратные комплексы криптографической защиты, их характеристики и особенности применения. Сравнительная таблица.

20. Нормативно-правовая база криптографической защиты.

21. ЭЦП и особенности работы в системах государственного и муниципального управления.

Шкала оценки заданий:

- Ответ полностью соответствует условиям задания и обосновано – 5 баллов.
- Ответ в целом соответствует условиям задания, но отдельные аспекты на обоснованы – 4 балла.

• Ответ частично соответствует условиям задания, отдельные аспекты не обоснованы или имеются несущественные ошибки – 3 балла.

• Ответ не соответствует условиям задания, отдельные аспекты не обоснованы или имеются существенные ошибки – 0 баллов.

2. Оценочные материалы для проведения промежуточной аттестации

Планируемый образовательный результат (компетенция, индикатор)	**Типовые контрольные задания**	**Критерии оценивания и шкала оценивания**
ПК-1 Способен осуществлять научно-исследовательскую работу на основе математических и естественных наук, основ программирования и информационных технологии *ПК-1.2 Проводит анализ, обоснование и выбор решения прикладных задач ПК-1.3 Проектирует научное исследование в соответствии с задачами профессиональной деятельности*	1. Опишете алгебраическую модель шифра Цезаря. 2. Расшифровать фразу, зашифрованную столбцовой перестановкой "ОКЕСНВРП_ЫРЕ-АДЕЫН_В_РСИКО". 3. Опишете алгебраическую модель шифра гаммирования. 4. Зашифровать по алгоритму DES-ECB сообщение, состоящее из первых восьми букв своей фамилии. Если количество букв в фамилии меньше 8 букв, то необходимо добавить недостающее количество букв из имени. В качестве ключа выбрать первые 7 букв шифруемого сообщения.	• *Полно и правильно даны ответы на все поставленные вопросы, приведены необходимые примеры; студент показывает понимание излагаемого материала – 30 – 40 баллов* • *Полно и правильно даны ответы на все поставленные вопросы, приведены примеры, однако имеются неточности; в целом студент показывает понимание изученного материала – 20 – 29 балла* • *Ответ дан в основном правильно, но недостаточно аргументированы выводы, приведены не все необходимые примеры – 10 – 19 баллов* • *Даны неверные ответы на поставленные вопросы – 0 – 9 баллов*

Примерные вопросы к экзамену

1. Основные принципы защиты информационных технологий (четыре задачи системы

защиты).

2. Виды угроз собственной информации в сфере финансовой деятельности.

3. Меры противодействия угрозам собственной информации.

4. Организационно-технические меры защиты информации посредством: охраны

зданий; организации использования оргтехники; контроля за посетителями,

клиентами.

5. Организационные меры защиты информации посредством контроля за сотрудниками.

6. Организация защиты конфиденциальных документов.

7. Информационная безопасность при использовании средств связи.

8. Организационно-технические методы получения информации о конкурентах.

9. Понятие «изъяны защиты». Причины существования изъянов защиты.

10. Классификация изъянов защиты (по источнику появления, по этапам внедрения, по

размещению в информационной системе).

11. Таксономия причин возникновения изъянов защиты.

12. Понятие политики безопасности.

13. Дискретные модели безопасности.

14. Мандатные модели безопасности.

15. Ролевые модели безопасности.

16. Понятия идентификация, аутентификация. Методы и типы аутентификации.

17. Парольные системы защиты.

18. Понятие шифрования. Виды шифрования, применяемые в информационных

системах.

19. Способы контроля целостности данных.

20. Цифровая подпись.

21. Хэш-функция.

22. Компьютерная стеганография.

23. Классификация нарушителей по уровню возможностей.

24. Пароль - как метод защиты информации. Виды паролей. Правила подбора паролей.

25. Классификация мероприятий по защите от несанкционированного доступа.

26. Охарактеризовать область физической безопасности АС.

27. Охарактеризовать область безопасности персонала.

28. Охарактеризовать область безопасности оборудования.

29. Охарактеризовать область безопасности ПО.

30. Межсетевые экраны – как метод защиты информации. Дать определение МЭ.

31. Инспектирование и анализ протоколов - как метод защиты информации.

32. Контроль за действиями пользователя и событиями в сети.

33. Принципы восстановления информации и защиты после аварии.

34. Хранение информации. Сжатие и защита информации при хранении.

35. Современные программные угрозы, методы их обнаружения и предупреждения.

36. Методы обнаружения разрушающих программных средств.

37. Намеренное силовое воздействие по каналу связи - как угроза безопасности АС.

38. Предмет криптографии, основные понятия. Общая схема симметричного шифрования.

38. История криптографии.

39. История русской криптографии.

40. Определение шифра, простейшие примеры.
41. Шифры замены, основные понятия.
42. Алгебраические модели шифров.
43. Вероятностные модели шифров.
44. Понятие блочного шифра.
45. Понятие итерированного шифра
46. Шифр Фейстеля, определение и свойства.
47. Алгоритм DES.
48. Режимы DES.
49. Теоретическая стойкость шифров.
50. Практическая стойкость.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

1. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. - Информационная безопасность. Лабораторный практикум (для бакалавров)+ Электронные приложения на сайте www.book.ru - КноРус - 2018 - 131с. - ISBN: 978-5-406-05990-6 - Текст электронный // ЭБС BOOKRU - URL: https://book.ru/book/926191
2. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. - Информационная безопасность. Практикум (+CD) (для бакалавров) - КноРус - 2016 - 131с. - ISBN: 978-5-406-04870-2 - Текст электронный // ЭБС BOOKRU - URL: https://book.ru/book/918700
3. Баранова Е.К., Бабаш А.В. - Криптографические методы защиты информации. Лабораторный практикум +CD (для бакалавров) - КноРус - 2015 - 196с. - ISBN: 978-5-406-03802-4 - Текст электронный // ЭБС BOOKRU - URL: https://book.ru/book/915869
4. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» ; ИНФРА-М, 2016. — 416 с. — (Профессиональное образование). - ISBN 978-5-8199-0331-5 (ИД «ФОРУМ») ; ISBN 978-5-16-003132-3 (ИНФРА-М, print) ISBN 978-5-16-101207-9 (ИНФРА-М, online). - Текст : электронный. - URL: http://znanium.com/catalog/product/549989
5. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ А.А. Петров.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 446 с.— Режим доступа: http://www.iprbookshop.ru/63800.html. — ЭБС «IPRbooks»
6. 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
7. Кукина Е.Г. Введение в криптографию [Электронный ресурс] : практикум / Е. Г. Кукина, В. А. Романьков; Е.Г. Кукина; В.А. Романьков. - Введение в криптографию. - Омск : Омский государственный университет им. Ф.М. Достоевского, 2013. - 91 с.

б) Дополнительная литература

1. Авдошин С.М., Набебин А.А. - Дискретная математика. Модулярная алгебра, криптография, кодирование - Издательство "ДМК Пресс" - 2017 - 352с. - ISBN: 978-5-97060-408-3 - Текст электронный // ЭБС ЛАНЬ - URL: https://e.lanbook.com/book/93575
2. Байкова Л. А. - ОСНОВЫ УЧЕБНО-ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ 2-е изд., испр. и доп. Учебное пособие для СПО - М.:Издательство Юрайт - 2019 - 122с. - ISBN: 978-5-534-12527-6 - Текст электронный // ЭБС ЮРАЙТ - URL: https://urait.ru/book/osnovy-uchebno-issledovatelskoy-deyatelnosti-447730
3. Ростовцев А., Маховенко Е. введение в криптографию с открытым ключом - СПб.:, НПО «Мир и семья» ООО «Интерлайн» - 2001.
4. Чмора Л. Л. Современная прикладная криптография, 2-е изд. стереотипное. – М.: ГЕЛИОС АРВ, 2002.
5. Шнаер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003.
6. Ростовцев А., Маховенко Е. Теоретическая криптография - СПб.:, АНО НПО «Профессионал» - 2005.

2) Программное обеспечение

Google Chrome	бесплатное ПО
Яндекс Браузер	бесплатное ПО
Kaspersky Endpoint Security 10	акт на передачу прав ПК545 от 16.12.2022
Многофункциональный редактор ONLYOFFICE	бесплатное ПО
ОС Linux Ubuntu	бесплатное ПО

3) Современные профессиональные базы данных и информационные справочные системы

№ п/п	Вид информационного ресурса, наименование информационного ресурса	Адрес (URL)
1	ЭБС «ZNANIUM.COM»	https://znanium.com/
2	ЭБС «ЮРАИТ»	https://urait.ru/
3	ЭБС «Университетская библиотека онлайн»	https://biblioclub.ru/
4	ЭБС IPR SMART	http://www.iprbookshop.ru/
5	ЭБС «ЛАНЬ»	http://e.lanbook.com
6	ЭБС ТвГУ	http://megapro.tversu.ru/megapro/Web
7	Репозитарий ТвГУ	http://eprints.tversu.ru
8	Ресурсы издательства Springer Nature	http://link.springer.com/
9	СПС КонсультантПлюс (в сети ТвГУ)	

VI. Методические материалы для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплины

Организуя свою учебную работу, студенты должны:

Во-первых, выявить рекомендуемый режим и характер учебной работы по изучению теоретического курса, практическому применению изученного материала, по выполнению заданий для самостоятельной работы, по использованию информационных технологий и т.д.

Во-вторых, ознакомиться с указанным в методическом материале по дисциплине перечнем учебно-методических изданий, рекомендуемых студентам для подготовки к занятиям и выполнения самостоятельной работы, а также с методическими материалами на бумажных и/или электронных носителях, выпущенных кафедрой своими силами и предоставляемые студентам во время занятий.

Самостоятельная работа студентов, предусмотренная учебным планом, должна соответствовать более глубокому усвоению изучаемого курса, формировать навыки исследовательской работы и ориентировать студентов на умение применять теоретические знания на практике.

1. Работа с учебными пособиями. Для полноценного усвоения курса студент должен, прежде всего, овладеть основными понятиями этой дисциплины. Необходимо усвоить определения и понятия, уметь приводить их точные формулировки, приводить примеры объектов, удовлетворяющих этому определению. Кроме того, необходимо знать круг фактов, связанных с данным понятием. Требуется также знать связи между понятиями, уметь устанавливать соотношения между классами объектов, описываемых различными понятиями.

2. Самостоятельное изучение тем. Самостоятельная работа студента является важным видом деятельности, позволяющим хорошо усвоить изучаемый предмет и одним из условий достижения необходимого качества подготовки и профессиональной переподготовки специалистов. Она предполагает самостоятельное изучение студентом рекомендованной учебно-методической литературы, различных справочных материалов, написание рефератов, выступление с докладом, подготовку к лекционным и практическим занятиям, подготовку к зачёту и экзамену.

3. Подготовка к практическим занятиям. При подготовке к практическим занятиям студентам рекомендуется следовать методическим рекомендациям по работе с учебными пособиями, приведенным выше.

4. Составление глоссария. В глоссарий должны быть включены основные понятия, которые студенты изучают в ходе самостоятельной работы. Для полноты исследования рекомендуется вписывать в глоссарий и те термины, которые студентам будут раскрыты в ходе лекционных занятий.

5. Составление конспектов. В конспекте отражены основные понятия темы. Для наглядности и удобства запоминания использованы схемы и таблицы.

6. Подготовка к экзамену. При подготовке к экзамену студенты должны использовать как самостоятельно подготовленные конспекты, так и материалы, полученные в ходе занятий.

Качество усвоения студентом каждой дисциплины оценивается по 100-балльной шкале.

Интегральная рейтинговая опенка (балл) по каждому модулю (периоду обучения) складывается из оценки текущей работы обучающихся на занятиях семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), оценки индивидуальной работы обучающихся и оценки за выполнение заданий рейтингового контроля успеваемости. При этом доля баллов, выделенных на рейтинговый контроль, не должна превышать 50% общей суммы баллов данного модуля (периода обучения).

Максимальная сумма рейтинговых баллов по учебной дисциплине, заканчивающейся экзаменом, по итогам семестра составляет 60.

Обучающемуся, набравшему 40-54 балла, при подведении итогов семестра (на последнем занятии по дисциплине) в рейтинговой ведомости учета успеваемости и зачетной книжке может быть выставлена оценка «удовлетворительно».

Обучающемуся, набравшему 55-57 баллов, при подведении итогов семестра (на последнем занятии по дисциплине) в графе рейтинговой ведомости учета успеваемости «Премиальные баллы» может быть добавлено 15 баллов и выставлена экзаменационная оценка «хорошо».

Обучающемуся, набравшему 58-60 баллов, при подведении итогов семестра (на последнем занятии по дисциплине) в графе рейтинговой ведомости учета успеваемости «Премиальные баллы» может быть добавлено 27 баллов и выставлена экзаменационная оценка «отлично».

В каких-либо иных случаях добавление премиальных баллов не допускается.

Обучающийся, набравший до 39 баллов включительно, сдает экзамен. При наличии подтвержденных документально уважительных причин, по которым были пропущены занятия (длительная болезнь, обучение в другом вузе в рамках академической мобильности и др.), обучающийся имеет право отработать пропущенные занятия и получить дополнительные баллы в рамках установленных баллов за модуль. Сроки и порядок отработки определяет преподаватель. Баллы выставляются в графе «отработка».

Ответ обучающегося на экзамене оценивается суммой до 40 рейтинговых баллов. Итоговая оценка складывается из суммы баллов, полученных за семестр, и баллов, полученных на экзамене. Обучающемуся, который сдает экзамен, премиальные баллы не начисляются.

Согласно подходам балльно-рейтинговой системы в рамках оценки знаний, умений, владений (умений применять) и (или) опыта деятельности дисциплины установлены следующие аспекты:

- Содержание учебной дисциплины в рамках одного семестра делится на два модуля (периода обучения). По окончании модуля (периода обучения) осуществляется рейтинговый контроль успеваемости знаний студентов.
- Сроки проведения рейтингового контроля:

осенний семестр – I рейтинговый контроль успеваемости проводится согласно графику учебного процесса, II рейтинговый контроль успеваемости - две

последние недели фактического завершения семестра по графику учебного процесса;
весенний семестр – I рейтинговый контроль успеваемости проводится согласно графику учебного процесса, II рейтинговый контроль успеваемости - две последние недели фактического завершения семестра по графику учебного процесса.

VII. Материально-техническое обеспечение дисциплины

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, у*чебная аудитория: №* **208** *(170002 Тверская обл., г. Тверь, пер. Садовый, д. 35)*	*Комплект учебной мебели, CD-магнитола, компьютер: (системный блок + монитор), многофункциональный лазер. копир/принтер/сканер, видеоплеер, телевизор, DVD плеер.*	Google Chrome – бесплатно Kaspersky Endpoint Security 10 для Windows – Акт на передачу прав ПК545 от 16.12.2022 Lazarus – бесплатно OpenOffice – бесплатно Многофункциональный редактор ONLYOFFICE бесплатное ПО – бесплатно ОС Linux Ubuntu бесплатное ПО – бесплатно

VIII. Сведения об обновлении рабочей программы дисциплины

№ п.п.	**Обновленный раздел рабочей программы дисциплины**	**Описание внесенных изменений**	**Дата и № протокола заседания кафедры / методического совета факультета, утвердившего изменения**
1.			
2.			