Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 20 г.

Рабочая программа дисциплины (с аннотацией)

Организационное и правовое обеспечение информационной безопасности

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 5 курса ОФО

Составитель:
Чернышев О. Л.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью изучения дисциплины является формирование базы знаний о нормативно-правовых нормах и методах деятельности в области обеспечения информационной безопасности автоматизированных систем.

Задачами освоения дисциплины являются:

1) ознакомить с основами законодательства Российской Федерации в области защиты информации;

2) получение теоретических знаний об основах организационно-правового обеспечения информационной безопасности;

3) изучение общих принципов и методов практического применения нормативно-правовых документов при организации защиты информации в организации или на предприятии.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Основы информационной безопасности», «Введение в специальность».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Сертификация по требованиям безопасности и аттестация объектов информатизации», «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 3 зачетные единицы, 108 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 часов, в т.ч. практическая подготовка – 0 часов;

практические занятия – 17 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 57 часа.

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
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	**УК-2.1** Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления
	УК-2.2 Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения
	УК-2.3 Разрабатывает план реализации

	проекта с учетом возможных рисков реализации и возможностей их устранения, планирует необходимые ресурсы, в том числе с учетом их заменяемости
	УК-2.4 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта
	УК-2.5 Предлагает процедуры и механизмы оценки качества проекта, инфраструктурные условия для внедрения результатов проекта
УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	**УК-3.1** Вырабатывает стратегию командной работы и на ее основе организует отбор членов команды для достижения поставленной цели
	УК-3.2 Организует и корректирует работу команды, в т.ч. на основе коллегиальных решений
	УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон; создает рабочую атмосферу, позитивный эмоциональный климат в команде
	УК-3.4 Организует (предлагает план) обучение членов команды и обсуждение результатов работы, в т.ч. в рамках дискуссии с привлечением оппонентов
	УК-3.5 Делегирует полномочия членам команды и распределяет поручения, дает обратную связь по результатам, принимает ответственность за общий результат
УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	**УК-9.2** Использует правовые базы данных и прочие ресурсы для получения информации о своих правах и обязанностях, связанных с осуществлением экономической политики государства
УК-10.4 Способен формировать нетерпимое отношение к коррупционному поведению	**УК-10.1** Определяет социально-правовую сущность коррупции, основные причины и виды коррупционных проявлений, обосновывает несовместимость коррупции и эффективной профессиональной деятельности

	УК-10.2 Анализирует тексты нормативных правовых актов по вопросам противодействия коррупции, а также тексты иных нормативных правовых актов в целях выявления положений, носящих потенциально коррупциогенный характер
	УК-10.3 Выявляет коррупционные составляющие, признаки и формы коррупционного поведения, в том числе, конфликта интересов в конкретной сфере профессиональной деятельности
	УК-10.4 Разъясняет субъектам права меры ответственности, предусмотренные действующим законодательством за совершение коррупционных правонарушений
	УК-10.5 Предлагает методы профилактики коррупционного поведения, способы распространения правовых антикоррупционных знаний, комплексные меры по минимизации коррупционных рисков в сфере профессиональной деятельности
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	**ОПК-5.2** Обосновывает решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей
	ОПК-5.3 Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации
	ОПК-5.4 Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации
	ОПК-5.5 Формулирует основные требования информационной безопасности при эксплуатации компьютерной системы
ОПК-6 Способен при решении профессиональных задач организовывать защиту	**ОПК-6.2** Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту

информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	информации ограниченного доступа в организации
	ОПК-6.3 Определяет политику контроля доступа работников к информации ограниченного доступа

5. Форма промежуточной аттестации и семестр прохождения – зачет в 9 семестре.

6. Язык преподавания русский**.**

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

Очная форма обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе Контроль (час.)
		Лекции	Практические занятия		
			всего	в т.ч. практическая подготовка	
Раздел 1 Правовое обеспечение информационной безопасности	52	16	6	2	28
Раздел 2 Организационное обеспечение информационной безопасности	56	18	7	2	29
ИТОГО	108	34	13	4	57

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии

Тема 1. Правовое обеспечение информационной безопасности	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция.
Тема 2. Организационное обеспечение информационной безопасности	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения <u>текущей аттестации</u>

<u>Задания для практических (семинарских) занятий</u>

Раздел I.

Задание 1 (УК-2.1; УК-2.2; УК-2.3; УК-2.4; УК-2.5; УК-3.1; УК-3.2; УК-3.3; УК-3.4; УК-3.5; УК-9.2, ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-6.2; ОПК-6.3): Составьте план мероприятий по защите коммерческой тайны (в соответствии с законом РФ «О коммерческой тайне»). Укажите перечень внутрифирменных документов, которые будут использоваться в целях правовой защиты секретов вашей фирмы. Составьте перечень сведений, составляющих коммерческую тайну вашей фирмы.

Задание 2 (УК-2.1; УК-2.2; УК-2.3; УК-2.4; УК-2.5; УК-3.1; УК-3.2; УК-3.3; УК-3.4; УК-3.5; УК-9.2, ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-6.2; ОПК-6.3): Обоснуйте необходимость проведения лицензирования выбранного вида деятельности. Укажите порядок и необходимость (обязательная или добровольная) сертификации средств, используемых в выбранном виде деятельности. Укажите перечень сертификационных документов, необходимых для выбранной деятельности фирмы. Составьте для вашей фирмы документы, необходимые для осуществления заданного вида деятельности.

Раздел II.

Задание 1 (УК-10.1; УК-10.2; УК-10.3; УК-10.4; УК-10.5, ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-6.2; ОПК-6.3): Оцените угрозы вашим информационным ресурсам (укажите наиболее вероятные виды компьютерных преступлений из приведенных в файле). Укажите мероприятия, проводимые при создании системы защиты информации в вашей компьютерной сети. Укажите перечень РД ГТК, учитываемых при разработке «Политики безопасности» на вашем предприятии. Определите и обоснуйте требования по защите вашей конфиденциальной информации – группу и класс защищенности СВТ от НСД.

Задание 2 (УК-10.1; УК-10.2; УК-10.3; УК-10.4; УК-10.5, ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-6.2; ОПК-6.3): Смоделировать политику безопасности

образовательного учреждения и составить матрицу доступа для образовательного учреждения. Составить иерархию ролей для данного образовательного учреждения с описанием ролей сотрудников. При описании должен быть реализован принцип минимизации привилегий.

Оценочные материалы для проведения <u>промежуточной аттестации</u>

Проверяемые индикаторы достижения компетенций: **УК-2.1; УК-2.2; УК-2.3; УК-2.4; УК-2.5; УК-3.1; УК-3.2; УК-3.3; УК-3.4; УК-3.5; УК-9.2; УК-10.1; УК-10.2; УК-10.3; УК-10.4; УК-10.5; ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-6.2; ОПК-6.3**

Каждый студент решает индивидуальный тест и отвечает на теоретический вопрос.

Примерные вопросы к зачету

1. Структура информационной сферы и характеристика ее элементов.
2. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения.
3. Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности.
4. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации. Понятие и виды защищаемой информации по законодательству РФ.
5. Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.
6. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
7. Органы защиты государственной тайны и их компетенция. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).
8. Понятие информации конфиденциального характера по российскому законодательству. Основные виды «конфиденциальной» информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства.
9. Правовые режимы «конфиденциальной» информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
10. Юридическая ответственность за нарушения правовых режимов «конфиденциальной» информации (дисциплинарная, гражданско-правовая, административная и уголовная).
11. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности.

12. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности.

13. Понятие подтверждения соответствия по российскому законодательству, формы подтверждения. Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности.

14. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

15. Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав. Объекты и субъекты авторского права.

16. Авторские права (личные неимущественные права и исключительное право). Правовая охрана баз данных, топологий интегральных микросхем и единых технологий. Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

17. Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими.

18. Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации.

19. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения.

20. Безопасность при транспортировке носителей информации.

21. Защита документов от подделок. Обнаружение фальсификации документов.

22. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.

23. Физическая защита неподвижных объектов. Пропускной режим.

24. Проблема безопасности технологии. Организация работы персонала. Резервирование оборудования и дублирование информации. Система инструкций и правил.

25. Администрирование технологического процесса. Контроль доступа и средства поиска и досмотра. Системы контроля доступа.

26. Средства поиска и досмотра. Обнаружение металлов и взрывчатки. Обнаружители наркотиков. Обнаружители газов и отравляющих веществ. Обнаружители радиоактивных веществ.

27. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Виды представления информации.

28. Пути прохождения информации. Учет получения, перемещения, преобразования, хранения и уничтожения информации.

29. Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.

30. Аппаратные закладки.

31. Виброаккустический канал утечки информации.

32. Визуальный канал утечки информации.

33. Программные и аппаратные средства защиты от несанкционированного доступа.

34. Защита на различных уровнях: операционная система, прикладные программы.

35. Разграничение доступа. Регистрация. Остаточная информация. Защита от копирования.

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **3** балла. Для получения зачета необходимо ответить на вопросы теста и дать ответ на теоретический вопрос с суммарной оценкой не менее 2-х балов.

3 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется решение теста верное от 85 – 100% всех заданий.

2 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Верно даны ответы на 70-84% тестовых заданий.

1 балл:

Ответ демонстрирует знание и корректное использование терминологии. Правильные решения тестовых заданий составляют от 41-69%.

0 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Правильные тестовые ответы составляют менее 40%.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

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

Защита информации : учебное пособие / А. П. Жук [и др.]; Северо-Кавказский федеральный университет; Российский государственный гидрометеорологический университет. - Москва : Издательский Центр РИОР, 2023. - 400 с. – Режим доступа: https://znanium.com/catalog/document?id=422331

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. – Режим доступа: https://e.lanbook.com/book/293009

Чепурнова Н.М. Правовые основы информатики [Электронный ресурс]: учебное пособие для студентов вузов, обучающихся по направлению «Прикладная информатика»/ Н.М. Чепурнова, Л.Л Ефимова.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 295 с.— Режим доступа: http://www.iprbookshop.ru/34498.html

б) Дополнительная литература:

Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ А.В. Артемов.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.html

Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ С.В. Петров, П.А Кисляков.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.html

Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html

2) Программное обеспечение

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

3) Современные профессиональные базы данных и информационные справочные системы

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

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

Независимый информационно-аналитический портал по безопасности
SASecurity Information Box
Информационная безопасность на Report.ru
Информационная безопасность / Блог / Хабрахабр
Библиотека информационной безопасности
Библиотека сетевой безопасности
Компьютерная безопасность: уязвимости, ошибки и эксплоиты
Построение безопасности в сетях
Защита информации

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

На лекциях 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, 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.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени затраченного на дисциплину, будут превосходить иные виды работ. 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 и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения оценивается в 100 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических	Реферирование, представление научной статьи, создание и	Максимальный балл за рейтинговую контрольную

		занятиях	отладка кода	работу
1	50	18	12	20
2	50	18	12	20

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»:
https://www.tversu.ru/sveden/files/Pologhenie_o_reytingovoy_sisteme_obucheniya(1).pdf

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
Помещение для самостоятельной работы, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, практики Компьютерный класс 203а 170002, г.Тверь, Садовый пер-к, д. 35. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего	Столы, стулья, переносной ноутбук, компьютеры Столы, стулья, переносной ноутбук, проектор	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 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

контроля и промежуточной аттестации, у*чебная аудитория* 203, 224, 170002, г.Тверь, Садовый пер-к, д. 35		

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы.	Протокол № 11 от 26.06.2013
2.	VII. Методические указания для обучающихся по освоению дисциплины	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 10 от 24.06.2014
3.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы. Обновление ссылок из ЭБС.	Протокол № 1 от 27.09.2015
4.	VII. Методические указания для обучающихся по освоению дисциплины.	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 1 от 01.09.2016
5.	I - X	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
6.	V. Перечень основной и дополнительной учебной литературы, необходимой для	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2017

	освоения дисциплины		
7.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
8.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023