ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института математики, естествознания и техники
_____/Н.В.Черноусова/

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.05 Техническая защита информации

Направление подготовки: *10.03.01 Информационная безопасность*
Направленность (профиль): *Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*
Квалификация (степень): *бакалавр*
Форма обучения: *очная*

Институт: *математики, естествознания и техники*
Кафедра: *математического моделирования, компьютерных технологий и информационной безопасности*

	очная форма	**очно-заочная форма**	**заочная форма**
Курс	**3**		
Семестр	**5,6**		

Лекции	**36**		
Лабораторные занятия	**54**		
Практические (семинарские) занятия	**36**		
в т. ч. практическая подготовка	**8**		
Форма(ы) промежуточной аттестации	**Зачет Экзамен - 0,3**		
Контроль	**9**		
Иные формы работы			
Самостоятельная работа	**116,7**		

Всего часов: 252
Трудоемкость: 7 зачетных единицы.

Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент С.А. Рощупкин

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

– формирование знаний по основам инженерно-технической защиты информации, развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода, а также навыков и умения в применении знаний для конкретных условий.

Задачи изучения дисциплины:

– обнаружение и классификации фактов несанкционированного доступа к закрытой информации;

– выявление угрозы информационной безопасности объекта;

– организация работ по перекрытию основных каналов утечки информации и методов контроля эффективности, проведенных мероприятий.

Место дисциплины в структуре ОПОП: реализуется в вариативной части (части, формируемой участниками образовательных отношений) блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ПКС-1	**Знать**: - сущность и понятие информационной безопасности, характеристику ее составляющих, источники угроз и меры по их предотвращению; - методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, диагностике, анализу, сопровождению и совершенствованию систем защиты информации.	**Знает:** - принципы обеспечения информационной безопасности с помощью технических средств защиты информации; - терминологию, основные руководящие и регламентирующие документы в области технической защиты информации.
	Уметь: - оценивать защищенность, классифицировать основные угрозы, обеспечивать информационную безопасность компьютерных систем, применяя необходимые программно-аппаратные средства и системы защиты информации; - принимать управленческие и административные решения в сфере защиты информации.	**Умеет:** - определять необходимый инструментарий и технические средства защиты информации.
	Владеть: - категориальным аппаратом в области обеспечения комплекса мер по администрированию и диагностике систем защиты информации; - правилами, методами, средствами, процедурами управления и администрирования информационной безопасностью объекта.	**Владеет:** - навыками установки, настройки и методами, инструментами тестирования технических средств защиты информации;

ПКС-2	**Знать**: - основные виды и классификацию информационных ресурсов организации (предприятия); - сущность профессиональной деятельности по обеспечению защиты информации в процессе эксплуатации автоматизированных систем.	**Знает:** - основные виды обеспечения информационной безопасности с помощью технических средств защиты информации.
	Уметь: - выделять из общих информационных ресурсов предприятия информацию, подлежащую защите; - строить модели защиты информации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем.	**Умеет:** - строить модели технической защиты информации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем.
	Владеть: - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем: - навыками реализации моделей защиты информации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем.	**Владеет:** - способностью определять информационные ресурсы, подлежащие технической защите.

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего часов	Аудиторные занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
5 семестр						
Раздел 1. «Вводная лекция»		**16**	**4**	**4**	**4**	**4**
1	Тема 1. Концептуальные основы технического обеспечения информационной безопасности. Угрозы информационной безопасности на объекте защиты. Организация службы технической безопасности. Организация и обеспечение работы с информацией ограниченного доступа. Нормативно-методическое обеспечение организации безопасности информации	16	4	4	4	4
Раздел 2. «Угрозы безопасности информации»		**32**	**8**	**8**	**8**	**8**

2	Тема 2. Основные направления защиты информации от технических средств несанкционированного съема.	16	4	4	4	4
3	Тема 3. Роль технических средств в обеспечении безопасности информации.	16	4	4	4	4
Раздел 3. «Основные способы ведения промышленного шпионажа»		**24**	**6**	**6**	**6**	**6**
4	Тема 4. Каналы утечки информации их характеристика и место в системе технической разведки.	8	2	2	2	2
5	Тема 5. Основные физические поля, по которым происходит утечка информации и их характеристики.	8	2	2	2	2
6	Тема 6. Классификация технических средств негласного съема информации.	8	2	2	2	2
	Форма отчетности	зачет				
	Итого за 5 семестр	72	18	18	18	18
	в т.ч. практическая подготовка	4				
6 семестр						
Раздел 4. «Каналы утечки информации в технических средствах ее обработки и хранения»		**42**	**4**	**4**	**8**	**26**
7	Тема 7. Каналы утечки информации за счет акустических полей. Каналы утечки информации за счет электромагнитных излучений и наводок.	13	1	2	2	8
8	Тема 8. Каналы утечки информации по цепям питания и заземления. Каналы утечки информации за счет рассеянных оптических полей.	14	1	1	4	8
9	Тема 9. Каналы утечки информации за счет оптико- , электро- и вибро-акустических преобразований	15	2	1	2	10
Раздел 5. «Технические средства несанкционированного доступа»		**50**	**6**	**6**	**12**	**26**
10	Тема 10. Основные средства несанкционированного доступа к конфиденциальной информации. Возможности средств акустической разведки и особенности их применения.	16	2	2	4	8
11	Тема 11. Возможности средств оптической разведки и особенности их применения. Основные характеристики и методы применения радио-микрофонов и радио-закладок.	18	2	2	4	10
12	Тема 12. Устройства подслушивания, использующие проводную связь. Аппаратура лазерной разведки. Устройства съема информации с технических средств ее передачи и хранения	16	2	2	4	8
Раздел 6. «Защита информации в помещениях и сетях связи»		**42**	**4**	**4**	**8**	**26**
13	Тема 13. Аппаратура контроля линий связи. Средства защиты линий связи Криптографические методы и средства защиты. Технические	22	2	2	4	14

	средства пространственного и линейного зашумления. Защита от ВЧ навязывания. Защита от несанкционированной аудиозаписи. Основные методы и средства контроля степени защищенности объектов и сетей.					
14	Тема 14. Аппаратура измерения уровня сигнала в электрических цепях и сетях связи. Аппаратура измерения уровня побочных излучений. Проверка степени защищенности маскирующими сигналами.	20	2	2	4	12
Раздел 7. «Основы защиты информации в компьютерных сетях»		**36,7**	**4**	**4**	**8**	**20,7**
15	Тема 15. Виды потенциально опасных воздействий. Защита от ошибок обслуживающего персонала. Защита от заражений компьютерными вирусами.	18,7	2	2	4	10,7
16	Тема 16. Программно-аппаратные средства защиты информации от несанкционированного доступа.	18	2	2	4	10
	Форма отчетности	**Экзамен – 0,3**				
	Контроль	**9**				
	Экзамен	**0,3**				
	Итого за 6 семестр	***180***	***18***	***18***	***36***	***98,7***
	в т.ч. практическая подготовка	4				
	ИТОГО	**252**	**36**	**36**	**54**	**116,7**

Очно-заочная форма обучения не реализуется

Заочная форма обучения не реализуется

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме тестирования, реферата.

Типовой вариант тестирования

1. Кто является основным ответственным за определение уровня классификации информации?
A. Руководитель среднего звена
B. Высшее руководство
C. Владелец
D. Пользователь
2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
A. Сотрудники
B. Хакеры
C. Атакующие
D. Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
C. Улучшить контроль за безопасностью этой информации
D. Снизить уровень классификации этой информации
4. Что самое главное должно продумать руководство при классификации данных?
A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
B. Необходимый уровень доступности, целостности и конфиденциальности
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные
5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
A. Владельцы данных
B. Пользователи
C. Администраторы
D. Руководство
6. Что такое процедура?
A. Правила использования программного и аппаратного обеспечения в компании
B. Пошаговая инструкция по выполнению задачи
C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
D. Обязательные действия
7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
A. Поддержка высшего руководства
B. Эффективные защитные меры и методы их внедрения
C. Актуальные и адекватные политики и процедуры безопасности
D. Проведение тренингов по безопасности для всех сотрудников
8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
B. Когда риски не могут быть приняты во внимание по политическим соображениям
C. Когда необходимые защитные меры слишком сложны
D. Когда стоимость контрмер превышает ценность актива и потенциальные потери
9. Что такое политики безопасности?
A. Пошаговые инструкции по выполнению задач безопасности
B. Общие руководящие требования по достижению определенного уровня безопасности
C. Широкие, высокоуровневые заявления руководства
D. Детализированные документы по обработке инцидентов безопасности
10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
A. Анализ рисков
B. Анализ затрат / выгоды
C. Результаты ALE
D. Выявление уязвимостей и угроз, являющихся причиной риска
11. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды
B. Оценить возможные потери для каждой контрмеры
C. Количественно оценить затраты / выгоды
D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

A. Среднесрочное планирование
B. Долгосрочное планирование
C. Ежедневное планирование
D. Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?

A. Нечто, приводящее к ущербу от угрозы
B. Любая потенциальная опасность для информации или систем
C. Любой недостаток или отсутствие информационной безопасности
D. Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов
B. Контрмер и защитных механизмов
C. Физической безопасности и технических средств защиты
D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности
B. Классификацию данных после внедрения механизмов безопасности
C. Уровень доверия, обеспечиваемый механизмом безопасности
D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность
B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

A. Угрозы х Риски х Ценность актива
B. (Угрозы х Ценность актива х Уязвимости) х Риски
C. SLE х Частоту = ALE
D. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий
B. Количественная оценка воздействия потенциальных угроз
C. Выявление рисков
D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка
B. Выполнение анализа рисков
C. Определение цели и границ
D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка
B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Что является наилучшим описанием количественного анализа рисков?

A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
D. Метод, основанный на суждениях и интуиции

22. Почему количественный анализ рисков в чистом виде не достижим?

A. Он достижим и используется
B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
C. Это связано с точностью количественных элементов
D. Количественные измерения должны применяться к качественным элементам

23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

A. Много информации нужно собрать и ввести в программу
B. Руководство должно одобрить создание группы
C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
D. Множество людей должно одобрить данные

24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

A. Стандарты
B. Должный процесс (Due process)
C. Должная забота (Due care)
D. Снижение обязательств

25. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

A. Список стандартов, процедур и политик для разработки программы безопасности
B. Текущая версия ISO 17799
C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
D. Открытый стандарт, определяющий цели контроля

Примерная тематика рефератов

1. Законодательный уровень информационной безопасности.
2. Обзор российского законодательства в области информационной безопасности.
3. Закон «Об информации, информатизации и защите информации».
4. Закон «О лицензировании отдельных видов деятельности».
5. Обзор зарубежного законодательства в области информационной безопасности.
6. Стандарты и спецификации в области информационной безопасности.
7. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт.
8. Механизмы безопасности.
9. Классы безопасности.

10. Сетевые механизмы безопасности.
11. Администрирование средств безопасности.
12. О необходимости объектно-ориентированного подхода к информационной безопасности.
13. Основные понятия объектно-ориентированного подхода.
14. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
15. Административный уровень информационной безопасности. Основные понятия.
16. Административный уровень информационной безопасности. Политика безопасности.
17. Административный уровень информационной безопасности. Программа безопасности.
18. Административный уровень информационной безопасности. Синхронизация программы безопасности с жизненным циклом систем.
19. Управление рисками. Основные понятия.
20. Подготовительные этапы управления рисками.
21. Основные этапы управления рисками.
22. Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня.
23. Процедурный уровень информационной безопасности. Управление персоналом.
24. Процедурный уровень информационной безопасности. Физическая защита.
25. Процедурный уровень информационной безопасности. Поддержание работоспособности.
26. Процедурный уровень информационной безопасности. Реагирование на нарушение режима безопасности.
27. Процедурный уровень информационной безопасности. Планирование восстановительных работ.
28. Основные понятия программно-технического уровня информационной безопасности.
29. Архитектурная безопасность.
30. Идентификация и аутентификация. Парольная аутентификация.
31. Управление доступом. Ролевое управление доступом.
32. Возможный подход к управлению доступом в распределенной объектной среде.

Промежуточная аттестация обучающихся осуществляется в форме зачета и экзамена с использованием следующих оценочных материалов: *перечень вопросов к зачету и экзамену*.

Вопросы к зачету
(5 семестр, очная форма обучения)

1. Система информационной безопасности, направления защиты.
2. Технические средства обеспечения безопасности информации, их классификация.
3. Характеристика защитных средств.
4. Служба технической разведки, ее функции.
5. Характеристика физических и электрических полей.
6. Средства съема информации, порядок их применения.
7. Участие сотрудников службы безопасности в технической защите информации.
8. Акустические поля, их характеристика.
9. Утечка информации по ПЭМИН (побочное электромагнитное излучение и наводки).
10. Оптические поля, их характеристика.
11. Вибро-акустические каналы течки информации.
12. Технические средства несанкционированного доступа к информации.
13. Акустическая разведка, ее возможности и принципы работы технических средств.
14. Оптическая разведка, ее возможности и принципы работы технических средств.
15. Принципиальные схемы установки радио-микрофонов и радио

закладок.
16. Проводная связь, ее слабые места.
17. Средства лазерной разведки, принцип работы.
18. Порядок съема информации с технических средств ее передачи и
хранения.
19. Понятие ТКУИ (технические каналы утечки информации), классификация и факторы их возникновения.
20. Защищаемы объекты, их характеристика
21. Основные технические средства обработки информации, их характеристика.
22. Вспомогательные технические средства обработки информации, их характеристика.
23. Организационные мероприятия по защите информации по техническим каналам утечки информации.

Вопросы к экзамену
(6 семестр, очная форма обучения)

1. Аттестат соответствия, порядок его получения.
2. Защита помещений и сетей от утечки по техническим каналам утечки информации.
3. Типы закладных устройств, порядок их применения
4. Методы и технические средства выявления закладных устройств
5. Физический поиск закладных устройств.
6. Индикаторы поля, порядок их применения.
7. Программные средства выявления каналов утечки информации.
8. Технические комплексы выявления каналов утечки информации.
9. Нелинейные радиолокаторы, порядок их применения.
10. Порядок применения аппаратуры контроля линий.
11. Средства защиты линий связи, их характеристика.
12. Средства зашумления, их характеристика.
13. Аппаратура измерения уровня сигнала в электрических цепях и сетях связи, порядок ее использования.
14. Степени защищенности помещений, порядок ее определения.
15. Порядок аттестации помещений
16. Лицензирование деятельности в области ИБ
17. Виды потенциально опасных воздействий на ЭВМ.
18. Виды потенциально опасных воздействий.
19. Защита от ошибок обслуживающего персонала.
20. Защита от заражений компьютерными вирусами.
21. ПАС защиты информации на уровне автономных ПЭВМ.
22. ПАС защиты информации на уровне ЛВС.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Рагозин, Ю.Н. Инженерно-техническая защита информации : учебное пособие / Ю.Н. Рагозин. – Санкт-Петербург : ИЦ "Интермедия", 2018. – 168 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481159 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-4383-0161-5. – Текст : электронный.

4.2. Дополнительная литература

1. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 01.09.2021). – Библиогр. в кн. – Текст : электронный.
2. Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636 (дата обращения: 01.09.2021). – Библиогр.: с. 213. – Текст : электронный.
3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.
4. Сагдеев, К.М. Физические основы защиты информации : учебное пособие / К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 394 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=458285 (дата обращения: 01.09.2021). – Библиогр.: с. 387-388. – Текст : электронный.
5. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов : / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 4-е изд., стер. – Москва : ФЛИНТА, 2016. – 224 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93351 (дата обращения: 01.09.2021). – Библиогр.: с. 192-193. – ISBN 978-5-9765-1274-0. – Текст : электронный.

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://edu.ru/	**Российское образование: Федеральный портал. Включает** ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:
- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.