ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.04.05 Организационное и правовое обеспечение информационной безопасности

Направление подготовки: *10.03.01Информационная 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	**1,2**		
Семестр/триместр	**2,3**		

Лекции	**36**		
Лабораторные занятия	**54**		
Практические (семинарские) занятия	**36**		
в т. ч. практическая подготовка			
Форма(ы) промежуточной аттестации	**Зачет (2 семестр) Экзамен (3 семестр) – 0,8 КП**		
Контроль	**9**		
Иные формы работы	**1**		
Самостоятельная работа	**79,2**		

Всего часов:216
Трудоемкость: 6зачетных единиц.
Разработчик(и) рабочей программы:
к.п.н, доцент кафедры ММКТиИБ Л.Н. Алекандрова

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

освоение компетенций по применению комплекса мероприятий в системе защиты информации на основе реализации требований по правовой защите информации и организационному обеспечению информационной безопасности.

Задачи изучения дисциплины:

- формирование знаний об информационном законодательстве Российской Федерации, а также международном законодательстве в области защиты информации;
- овладение навыками практического применения нормативно-правовых документов при организации защиты информации в организации или на предприятии.

Место дисциплины в структуре ОПОП: реализуется в рамках базовой части блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-5	Знать: - основные нормативно-правовые акты и иные документы, регламентирующие деятельность по защите информации; - организационно-управленческие методы и инструментарий, обеспечивающие деятельность по защите информации в сфере профессиональной деятельности.	Знает: - нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе; - принципы и методы организационной защиты информации, способы оценки эффективности мер по информационной безопасности.
	Уметь: - использовать нормативно-правовые документы, связанные с обеспечением профессиональной деятельности на объектах защиты; – обосновывать организационно-управленческие решения в области обеспечения информационной безопасности систем, подлежащих информационной защите.	Умеет: - осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей по защите информации, применять нормативные правовые акты и нормативные методические документы в области защиты информации; - мотивированно обосновывать управленческие решения в области обеспечения информационной безопасности в нестандартных ситуациях и готовность нести за них ответственность.
	Владеть: - навыками аналитической работы с	Владеет: - навыками подбора, анализа и крити-

	нормативно-правовыми документами, в частности с нормативной базой РФ, в сфере профессиональной деятельности на конкретных объектах защиты; - методами разработки проектов нормативных и организационно-распорядительных документов для конкретных объектов защиты.	ческой оценки нормативно-правовой документации в сфере защиты информации, регламентирующей деятельность конкретного предприятия; - навыками разработки, оформления и внедрения в деятельность предприятия документации по регламентации мероприятий и оказанию услуг в области защиты информации
ОПК-6	Знать: - основные нормативные правовые акты, технические стандарты и спецификации, нормативные методические документы ФСБ РФ и ФСТЭК РФ в сфере информационной безопасности; - стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации объектов информатизации и сертификации средств защиты информации.	Знает: - классификацию видов тайн, иерархическую схему законодательной и нормативной базы РФ в области обеспечения ИБ, а также их содержание, в том числе федеральные законы, Указы и распоряжения Президента РФ, Постановления Правительства РФ, приказы ФСТЭК, организационно-распорядительные и другие нормативные и методические документы по технической защите информации.
	Уметь: - использовать нормативно-правовые документы, технические стандарты и спецификации, нормативные методические документы ФСБ РФ и ФСТЭК РФ в сфере информационной безопасности на конкретных объектах защиты; - обоснованно выбирать и применять соответствующие конкретной ситуации стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации автоматизированных систем.	Умеет: - обоснованно выбирать и применять соответствующие конкретной ситуации положения законодательных актов РФ в области обеспечения ИБ, в том числе федеральных законов, Указов и распоряжений Президента РФ, Постановлений Правительства РФ, приказов ФСТЭК, организационно-распорядительных и других нормативных и методических документов по технической защите информации.
	Владеть: - навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям нормативно-правовой базе, стандартам и спецификациям, нормативным методическим документам ФСБ РФ и ФСТЭК РФ в сфере информационной безопасности; - методами теоретического и экспериментального исследования при решении различных профессиональных задач с учетом основополагающих документов по лицензированию, стандартизации, сертификации.	Владеет: - приемами работы с нормативно-правовыми документами, техническими стандартами и спецификациями, связанными с обеспечением информационной безопасности на конкретных объектах защиты.
ОПК-8	Знать:	Знает:

	- принципы и методы подбора, изучения, систематизации и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; - методы поиска и обобщения информации, информационно-коммуникационные технологии для поиска и обработки необходимой информации, актуальные источники информации.	- основные виды и классификацию информационных ресурсов организации; - методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	Уметь: - осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; - обобщать общие объемы информации, полученные в результате изучения различных источников, проводить подробное и всестороннее рассмотрение проблемы, оценивать ее значимость, ценность для науки и практики.	Умеет: - решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	Владеть: - навыками осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности; - навыками работы с библиографическими источниками и информационно-коммуникационными технологиями для обработки массивов информации.	Владеет: - способами работы с различными источниками информации в области ИБ, обработки информационных ресурсов и получение новых, в том числе с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-2.3	Знать: - правовые основы информационной безопасности, в том числе локальные акты и стандарты; - организационно-управленческие и иные методы, нормативные требования, применяемые при аттестации автоматизированных систем.	Знает: - характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ; - виды и степень ответственности за правонарушения и преступления в информационной сфере; - порядок работы с персоналом по вопросам обеспечения защиты информации ограниченного доступа, проведения мероприятий по физической и технической защите конфиденциаль-

		ной информации, организации службы безопасности предприятия;
	Уметь: - использовать локальные нормативные акты и стандарты информационной безопасности для конкретных объектов защиты; - разрабатывать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности.	Умеет: - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать правовые акты и осуществлять правовую оценку информации; - разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.
	Владеть: - навыками работы с нормативной документацией, в области обеспечения информационной безопасности на конкретных объектах защиты; - комплексом мер по обеспечению информационной безопасности автоматизированных систем.	Владеет: - навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; - навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности; - навыками организации и управления деятельностью служб защиты информации на предприятии.

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

№ п/п	Наименование разделов и тем	Всего	Аудиторные занятия			Сам. раб.
			ЛК	ПЗ	ЛБ	
	Раздел 1. Основы законодательства РФ по обеспечению национальной и информационной безопасности	**30**	**8**	**8**	**8**	**6**
1	Тема 1.1. Информационная безопасность в системе национальной безопасности Российской Федерации. Национальные интересы в информационной сфере. Доктрина информационной безопасности	14	4	4	4	2
2	Тема 1.2. Информация и ин-	8	2	2	2	2

	формационные отношения как объект правового регулирования					
3	Тема 1.3. Источники угроз информационной безопасности РФ. Понятие информационной войны	8	2	2	2	2
	Раздел 2. Правовое обеспечение информационной безопасности.	**42**	**10**	**10**	**10**	**12**
4	Тема 2.1. Правовой режим защиты государственной тайны	12	3	3	3	3
5	Тема 2.2. Правовые режимы защиты конфиденциальной информации	12	3	3	3	3
6	Тема 2.3. Правовой режим защиты государственной тайны	9	2	2	2	3
7	Тема 2.4. Правонарушения в информационной сфере и особенности защиты от них	9	2	2	2	3
	Зачет:					
	Итого за 2 семестр	**72**	**18**	**18**	**18**	**18**
	Раздел 3. Организационные методы защиты информации	**133,2**	**18**	**18**	**36**	**61,2**
8	Тема 3.1. Понятие организационной защиты информации	28	4	4	8	12
9	Тема 3.2. Организация режима секретности	28	4	4	8	12
10	Тема 3.3. Допуск к государственной тайне	28	4	4	8	12
11	Тема 3.4. Организация защиты информации в различных направлениях деятельности предприятия (организации)	26	4	4	6	12
12	Тема 3.5.Организация работы службы безопасности предприятия	23.2	2	2	6	13,2
	КП	1				
	Контроль:	9				
	Экзамен	0,8				
	Итого за 3 семестр	**72**	**18**	**18**	**36**	**61,2**
	в т.ч. практическая подготовка					
	ИТОГО:	**216**	**36**	**36**	**54**	**79,2**

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 контрольной работы в виде теста, реферата.

Типовой вариант контрольной работы

Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. **конфиденциальная информация**

Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…

1. **комплексное обеспечение ИБ**
2. безопасность АС
3. угроза ИБ
4. атака на АС
5. политика безопасности

Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной сети от заданного множества угроз безопасности:

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. **политика безопасности**

К функциям информационной безопасности относятся:

1. совершенствование законодательства РФ в сфере обеспечения информационной безопасности
2. **выявление источников внутренних и внешних угроз**
3. страхование информационных ресурсов
4. защита государственных информационных ресурсов
5. подготовка специалистов по обеспечению информационной безопасности

Информационная безопасность это:

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
2. **Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз**
3. Состояние, когда не угрожает опасность информационным системам
4. Политика национальной безопасности России

Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:

1. защита информации от непреднамеренного воздействия
2. защита информации от несанкционированного воздействия
3. защита информации от несанкционированного доступа
4. **защита от утечки информации**

К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»

1. **Информация без ограничения права доступа**
2. Информация с ограниченным доступом
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

1. Государственная тайна
2. Коммерческая тайна
3. **Банковская тайна**
4. Конфиденциальная информация

Примерная тематика рефератов

1. Информационное общество и его безопасность
2. Информация – фактор существования и развития общества
3. Обеспечение информационной безопасности
4. Система обеспечения ИБ
5. Элементы теории права
6. Основы теории правового обеспечения ИБ
7. Законодательство об информации, информационных технологиях и о защите информации
8. Законодательство о персональных данных
9. Законодательство в сфере интеллектуальной собственности
10. Законодательство о коммерческой тайне
11. Законодательство о государственной тайне
12. Законодательство о ЭЦП
13. Законодательство о техническом регулировании
14. Юридическая ответственность
15. Защита прав и законных интересов субъектов информационной сферы
16. Организация системы обеспечения безопасности информации
17. Корпоративное нормативное регулирование
18. Организация объектовых режимов безопасности
19. Управление персоналом на предприятиях и в организациях служебной тайны.

Промежуточная аттестация обучающихся осуществляется в форме зачета, экзамена, курсового проекта с использованием следующих оценочных материалов:

Вопросы к зачету
(2 семестр, очная форма обучения)

1. Нормативно - правовые основы защиты служебной тайны.
2. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения.
3. Правовые основы защиты коммерческой тайны.
4. Виды информации, составляющей коммерческую тайну.

5. Права и обязанности обладателя коммерческой тайны.
6. Основные угрозы коммерческой тайны.
7. Правовая защита коммерческой тайны.
8. Правовые основы защиты банковской тайны.
9. Раскрытие информации, относящейся к банковской тайне.
10. Нарушение банковской тайны и ответственность за подобные нарушения.
11. Нотариальная тайна и ее особенности. Тайна завещания.
12. Врачебная тайна и ее особенности.
13. Адвокатская тайна и ее особенности.
14. Тайна страхования и ее особенности.
15. Тайна связи и ее особенности. Тайна переписки, почтовых, телеграфных и иных сообщений.
16. Тайна усыновления (удочерения). Тайна исповеди.
17. Формирование российского законодательства в области защиты персональных данных.
18. Основные понятия и содержание закона РФ «О персональных данных».
19. Подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.
20. Государственный надзор и контроль обработки персональных данных, ответственность за нарушения российского законодательства в данной области.
21. Правовые основы лицензирования в области защиты информации.
22. Правовые основы сертификации в области защиты информации.
23. Особенности правонарушений в информационной сфере.
24. Преступления в сфере компьютерной информации: виды, состав.
25. Основы расследования преступлений в сфере компьютерной информации.
26. Правовая защита информационных систем.
27. Правовая защита результатов интеллектуальной деятельности.
28. Соотношение организационных мер защиты информации с мерами правового и технического характера.
29. Основные термины, связанные с организацией защиты информации.
30. Организационные меры, направленные на защиту государственной тайны.
31. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
32. Особенности системы организационной защиты государственной тайны.
33. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны.
34. Организация деятельности режимно-секретных органов.
35. Установление и изменение степени секретности сведений, отнесенных к государственной тайне.

Вопросы к экзамену
(3 семестр, очная форма обучения)

1. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.
2. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы.
3. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
4. Документальное оформление для отправки на согласование.
5. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности.
6. Организация доступа к сведениям, составляющим государственную тайну.
7. Понятие «охрана». Цели и задачи охраны.

8. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны.
9. Виды, способы и особенности охраны различных объектов.
10. Понятие о рубежах охраны. Многорубежная система охраны.
11. Факторы выбора методов и средств охраны.
12. Организация охраны объектов защиты в процессе их транспортировки.
13. Понятие «режим», цели и задачи режимных мероприятий. Виды режима.
14. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков.
15. Виды пропускных документов.
16. Порядок организации работы бюро пропусков.
17. Контрольно-пропускные пункты, их оборудование Рiорганизация работы.
18. Понятие «внутриобъектовый режим» и его общие требования.
19. Противопожарный режим и его обеспечение.
20. Подбор и расстановка кадров.
21. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала.
22. Основные формы обучения и методы контроля знаний.
23. Мотивация персонала к исполнению требований по защите информации.
24. Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика.
25. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.
26. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
27. Организационные меры по защите информации при увольнении сотрудника.
28. Требования режима защиты информации при приеме в организации посетителей. Порядок доступа посетителей и командированных лиц к конфиденциальной информации. Порядок пребывания посетителей на территории и в помещениях организации.
29. Обеспечение защиты информации при выезде за рубеж командируемых лиц.
30. Основные виды и формы рекламы. Общие требования режима защиты информации в процессе рекламной деятельности.
31. Основные методы защиты информации в рекламной деятельности. Понятие «публикация в открытой печати». Общие требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.
32. Особенности защиты информации при опубликовании материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.
33. Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности.
34. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
35. Основные документы службы информационной безопасности.

Примерный перечень тем курсовых работ

1. Методы и средства защиты интеллектуальной собственности.
2. Преступления в информационной сфере, компьютерные преступления и борьба с ними.
3. Цифровые следы при работе с электронными устройствами.
4. Угрозы в сети Интернет, основные правила безопасной работы.
5. Безопасность электронной коммерции.
6. Мошенничество в информационной сфере.

7. Методы сокрытия персональной информации в цифровой сфере.
8. Законодательство в области информации, информационных технологий и защиты информации.
9. Законодательство РФ в области обеспечения безопасности персональных данных.
10. Законодательство РФ в сфере интеллектуальной собственности.
11. Институт правовой защиты коммерческой тайны
12. Институт правовой защиты банковской тайны.
13. Защита прав и законных интересов субъектов информационной сферы.
14. Лицензирование деятельности в области защиты информации.
15. Корпоративное нормативное регулирование в области информационной безопасности.
16. Порядок организации охраны объектов информатизации, внутри объектового и пропускного режима.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Ажмухамедов, И.М. Основы организационно-правового обеспечения информационной безопасности: учебное пособие / И.М. Ажмухамедов, О.М. Князева. - Санкт-Петербург: ИЦ "Интермедия", 2017. - 264 с. URL: https://biblioclub.ru/index.php?page=book&id=481107 (дата обращения: 01.09.2021). – Библиогр.: с. 248-256. – ISBN 978-5-4383-0160-8. – Текст : электронный.
2. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие : [16+] / В. В. Бондарев. – 2-е изд. – Москва : МГТУ им. Н.Э. Баумана, 2018. – 252 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571750 (дата обращения: 01.09.2021). – Библиогр.: с. 237-238. – ISBN 978-5-7038-4899-9. – Текст : электронный.

4.2. Дополнительная литература

1. Горбенко, А.О. Основы информационной безопасности (введение в профессию) : учебное пособие / А.О. Горбенко. – Санкт-Петербург : ИЦ "Интермедия", 2017. – 336 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=482788 (дата обращения: 01.09.2021). – ISBN 978-5-4383-0136-3. – Текст : электронный.
2. Основы национальной безопасности: учебное пособие / Н.Д. Эриашвили, Е.Н. Хазов, Л.Т. Чихладзе и др.; под ред. Е.Н. Хазова, Н.Д. Эриашвили. - Москва: Юнити-Дана, 2018. - 335 с. URL: https://biblioclub.ru/index.php?page=book&id=473285 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-238-03030-2. – Текст : электронный.
3. Петренко, В.И. Защита персональных данных в информационных системах : учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2016. - 201 с. URL: https://biblioclub.ru/index.php?page=book&id=459205 (дата обращения: 01.09.2021). – Текст : электронный.
4. Кришталюк, А. Н. Правовые аспекты системы безопасности: курс лекций / А. Н. Кришталюк ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 204 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428612 (дата обращения: 01.09.2021). – Библиогр. в кн. – 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.	https://www.intuit.ru/	Национальный открытый университет - организация, предоставляющая с помощью собственного сайта услуги дистанционного обучения по нескольким образовательным программам, многие из которых касаются информационных технологий. Сайт содержит несколько сотен открытых образовательных курсов, по прохождении которых можно бесплатно получить электронный сертификат. Также возможно платное получение сертификатов о повышении квалификации. Кроме того, организация действует как издательство, выпуская учебную литературу по курсам.	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕСПРАВОЧНЫЕ СИСТЕМЫ

1.	www.school.edu.ru	Российский общеобразовательный портал	Свободный доступ.
2.	www.garant.ru	Гарант.РУ – информационно-правовой портал	Свободный доступ.
3.	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
4.	www.garant.ru	Информационно-правовой портал	Свободный доступ
5.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
6.	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 идр.

–

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.