Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)

«УТВЕРЖДАЮ»
Проректор по УМР
А.А. Панфилов
«17» 12.2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении
(наименование дисциплины)

Направление подготовки 22.03.01 «Материаловедение и технологии материалов»

Профиль подготовки

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость, зач. ед. (час.)	Лекций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
VIII	2 (72)		20		52	зачет
Итого	2 (72)		20		52	зачет

г. Владимир
2015 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины (модуля) «Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении» является освоение системы знаний, позволяющих ориентироваться в основах информационной безопасности и организации работ в сфере защиты интеллектуальной собственности.

В результате освоения данной дисциплины у студентов формируются основные общекультурные, общепрофессиональные и профессиональные компетенции, отвечающие требованиям ФГОС ВО, к результатам освоения ОПОП ВО по направлению 22.03.01 «Материаловедение и технологии материалов».

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина «Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении» относится к вариативной части блока 1 образовательной программы подготовки бакалавров по направлению 22.03.01 «Материаловедение и технологии материалов». Дисциплину «Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении» студенты изучают в 8-м семестре.

Курс «Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении» посвящен ознакомлению с современными тенденциями развития информационной безопасности и организации работ в сфере защиты интеллектуальной собственности. Для успешного усвоения студентами курса «Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении» необходимо знание основных курсов «Информатика», «Правоведение», «Основы информационных технологий в материаловедении», «Философия».

Изучение дисциплины «Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении» обеспечит формирование у бакалавров профессионального подхода к решению задач технического и научно-исследовательского характера. Знание, умения и навыки, полученные в ходе освоения дисциплины, используются при выполнении выпускных квалификационных работ.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

знать:

- закономерности исторического развития общества в области информационной безопасности и защиты интеллектуальной собственности (ОК-2);
- законодательство об охране объектов интеллектуальной собственности (ПК-2);
- виды ответственности за нарушение прав владельцев интеллектуальной собственности(ПК-2);
- положения об охранных грамотах (патентах и свидетельствах), выдаваемых на объекты интеллектуальной промышленной собственности(ПК-2);
- правовые положения об изобретениях, полезных моделях и промышленных образцах; правовые положения о ноу-хау(ПК-2);
- правовые положения о фирменных наименованиях, товарных знаках и знаках обслуживания; методики правового анализа научно-технических и патентных документов(ПК-2);
- правила составления и подачи заявок на изобретения, полезные модели и промышленные образцы (ПК-2);
- базовый понятийный аппарат в области ИБ (ОПК-1);
- виды и состав угроз информационной безопасности; принципы и общие методы обеспечения информационной безопасности (ОПК-1);
- основные положения государственной политики обеспечения информационной безопасности (ОПК-1);
- критерии, условия и принципы отнесения информации к защищаемой; виды носителей защищаемой информации (ОПК-1);
- виды тайн конфиденциальной информации; виды уязвимости защищаемой информации (ОПК-1);
- источники, виды и способы дестабилизирующего воздействия на защищаемую информацию (ОПК-1);
- каналы и методы несанкционированного доступа к конфиденциальной информации; классификацию видов, методов и средств защиты информации (ОПК-1).

уметь:

- проводить правовой анализ научно-технических и патентных документов (ПК-2);

- оформлять заявочные материалы на объекты интеллектуальной промышленной собственности (ПК-2);

- выявлять угрозы информационной безопасности применительно к объектам защиты (ОПК-1);

- определять состав конфиденциальной информации применительно к видам тайны (ОПК-1);

- выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия (ОПК-1);

- выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации (ОПК-1);

- определять направления и виды защиты информации с учетом характера информации и задач по ее защите (ОПК-1);

- организовывать системное обеспечение защиты информации (ОПК-1).

- анализировать основные этапы и закономерности исторического развития общества для формирования гражданской позиции относительно информационной безопасности и защиты интеллектуальной собственности (ОК-2).

владеть:

- знаниями и навыками для определения наиболее эффективного пути правовой охраны и коммерциализации интеллектуальной собственности (ПК-2);

- собственной гражданской позицией относительно действий в рамках информационной безопасности и защиты интеллектуальной собственности (ОК-2);

- навыками оценки патентоспособности объектов интеллектуальной собственности; навыками оценки соблюдения законодательства в области защиты объектов интеллектуальной собственности (ПК-2);

- навыками оценки результатов интеллектуального творчества с потенциалом возможностей их правовой защиты (ПК-2);

- Основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации (ОПК-1);

- информацией о современных и перспективных системах автоматизации информационно-аналитической работы (ОПК-1).

В результате освоения дисциплины «Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении» студент должен обладать следующими:

Общекультурными компетенциями:

- Обладать способностью анализировать основные этапы и закономерности исторического развития общества для формирования гражданской позиции (ОК-2);

общепрофессиональными компетенциями:

- Обладать способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1).

профессиональными компетенциями:

-Обладать способностью осуществлять сбор данных, изучать, анализировать и обобщать научно-техническую информацию по тематике исследования, разработке и использованию технической документации, основным нормативным документам по вопросам интеллектуальной собственности, подготовке документов к патентованию, оформлению ноу-хау (ПК-2).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Разделы дисциплины и виды занятий:

Общая трудоемкость дисциплины составляет 2 зачетных единицы (72 часа).

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы с применением интерактивных методов (в часах / %)	Формы текущего контроля успевае-мости *(по неделям семестра)*, форма промежу-точной аттестации *(по семест-рам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1	Защита интеллектуальной деятельности	8	1-8		16			20		14/32	**Рейтинг-контроль №1 Рейтинг-контроль №2**
2	Основы информационной безопасности	8	9-10		4			32		4/40	**Рейтинг-контроль №3**
	Всего	**8**	**1-10**		**20**			**52**	+	**18/33**	**зачет**

Практические занятия

Практические занятия являются формой групповой аудиторной работы в небольших группах для освоения практических навыков с целью формирования основных компетенций, необходимых для освоения основной образовательной программы.

Практические занятия по дисциплине «Основы информационной безопасности и защита интеллектуальной деятельности в материаловедении» проводятся с элементами деловой игры. Преподаватель при проведении занятий выполняет функцию консультанта, который лишь направляет работу студентов. Занятия осуществляются в диалоговом режиме, основными субъектами которого являются студенты.

Таблица 2. Перечень тем практических занятий

№ п/п	Номер раздела дисциплины	Темы практических работ	Трудоемкость, час
1.	Раздел 1	Авторское право и смежные права. Смежные права, понятие, сущность. Субъекты и объекты смежных прав. Передача прав на произведение авторского права. Коллективное управление имущественными правами. Защита прав.	2
2.	Раздел 1	Правовая защита интеллектуальной собственности. Патент - понятие, назначение. Объекты патентного права – изобретение.	2
3.	Раздел 1	Объект патентного права - полезная модель.	2
4.	Раздел 1	Объект патентного права - промышленный образец.	2
5.	Раздел 1	Фирменное наименование - понятие и назначение. Товарный знак и знак обслуживания. Общеизвестный товарный знак. Регистрация товарного знака.	2
6.	Раздел 1	Коммерческая тайна. Понятие, признаки, правовой режим. Законные способы получения коммерческой тайны. Режим коммерческой тайны. Исключения. Меры по охране конфиденциальности информации.	2
7.	Раздел 1	Передача прав. Лицензионный договор - понятие, виды. Недействительность патента, оспаривание патента. Досрочное прекращение действия патента. Ответственность: гражданско-правовая, административная, уголовная.	2
8.	Раздел 1	Промышленная собственность.	2
9.	Раздел 2	Компьютерная программа (программа для ЭВМ) - понятие и правовой режим. Передача прав на программное обеспечение по авторскому договору. Продажа экземпляров программного обеспечения. Компьютерное пиратство. Виды и методы борьбы с	4

		ним.	
		Всего практических работ	**40**

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании курса используются преимущественно традиционные образовательные технологии: практические занятия.

Иллюстрационный материал оформлен в виде презентации с использованием стандартной программы в PowerPoint. Для демонстрации данного наглядно-иллюстрированного материала практических работ используется соответствующая аппаратура (ноутбук, проектор).

В рамках проведения практических занятий запланирован разбор конкретных ситуаций с целью формирования и развития профессиональных компетенций у обучающихся, а также предусмотрено проведение занятий в активной форме.

Студенты самостоятельно изучают отдельные темы, отдельные вопросы, дополнительную литературу до изучения теоретического материала, что позволяет преподавателю опереться на изученный студентами материал. При этом вырабатываются значительный багаж знаний, навыков и умений, способность анализировать, осмысливать и оценивать современные события, решать профессиональные задачи на основе единства теории и практики, что гарантирует успешное освоение профессии.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Текущий контроль проводится на практических занятиях с целью определения качества усвоения лекционного материала и части дисциплины, предназначенной для самостоятельного изучения. Наиболее эффективным является его проведение по окончании изучения очередной учебной темы в письменном форме или с использованием фонда тестовых заданий или вопросов для текущего контроля.

Задания для рейтинг-контроля

Вопросы для рейтинг-контроля 1

1. Понятие интеллектуальной собственности.
2. Законодательство об охране интеллектуальной собственности.
3. Виды объектов авторских прав.
4. Объекты и субъекты авторского права.
5. Права авторов произведений науки, литературы и искусства.
6. Авторский договор.
7. Смежные права. Защита авторских и смежных прав.
8. Изобретения, полезные модели и промышленные образцы как объекты авторских прав.
9. Авторы изобретений, полезных моделей и промышленных образцов. Заявители и
10. патентообладатели.
11. Оформление исключительных прав на изобретения, полезные модели и
12. промышленные образцы.
13. Охранные документы на изобретения полезные модели и промышленные образцы.
14. Права авторов на изобретения полезные модели и промышленные образцы.
15. Защита прав авторов.
16. Фирменные наименования как объекты промышленной собственности.
17. Товарные знаки и знаки обслуживания как объекты промышленной собственности.
18. Понятие и признаки наименования места происхождения товара.
19. Защита прав наименования места происхождения товара.
20. Защита прав от недобросовестной конкуренции.
21. Ответственность за недобросовестную конкуренцию.
22. Служебная и коммерческая тайна.
23. Нетрадиционные объекты интеллектуальной собственности.
24. Принципы авторского права.
25. Основные задачи авторского права.
26. Понятие и признаки объекта авторского права.
27. Произведения, не охраняемые авторским правом.
28. Оригинальные и производные произведения.
29. Обнародованные и необнародованные произведения.
30. Служебные и неслужебные произведения.
31. Соавторство и его виды.

Вопросы для рейтинг-контроля 2

1. Ответственность за нарушение авторских прав.

2. Способы защиты авторских прав.
3. Характеристика признака «новизна».
4. Характеристика признака «изобретательский уровень».
5. Характеристика признака «промышленная применимость».
6. Компетенция патентного ведомства.
7. Апелляционная палата патентного ведомства.
8. Высшая патентная палата РФ.
9. Патентные поверенные.
10. Этапы экспертизы заявок на изобретение.
11. Зарубежное патентование российских изобретений.
12. Уступка прав.
13. Виды лицензий (исключительная, неисключительная открытая).
14. Виды защита прав авторов и патентообладателей.
15. Международные соглашения в области охраны интеллектуальной собственности.
16. Законодательство о правовой охране открытий.
17. Рационализаторские предложения.
18. Устав коллективного знака.
19. Организации, занимающиеся вопросами открытий.
20. Понятия и признаки изобретения.
21. Основные задачи института промышленной собственности.

Вопросы для рейтинг-контроля 3

1. Основные понятия информационной безопасности. Субъекты информационных отношений;
2. Какая информация является предметом защиты?
3. Понятие доступности, целостности и конфиденциальности.
4. Понятие угрозы,атаки, уязвимости. Примеры Угроз;
5. Понятие угрозы,атаки, уязвимости. Примеры уязвимостей;
6. Понятие угрозы,атаки, уязвимости. Примеры Атак;
7. Источник угроз ИБ. Понятие нарушителя. Модель нарушителя;
8. Модель безопасности по ГОСТ 13335-1-2006;
9. Угроза ИБ. Источники угроз ИБ. Модель угроз ИБ;
10. Угрозы ИБ. Классификация угроз ИБ. Классификация по расположению источника. Классификация по активности АИС.
11. Угрозы ИБ. Классификация угроз ИБ. Классификация по размеру ущерба.
12. Классификация по отношению к защищаемой информации.
13. Угрозы ИБ. Классификация угроз ИБ. Классификация по аспекту ИБ.

Классификация по компонентам АИС.

14. Методы, меры обеспечения ИБ и средства ЗИ. Классификация методов, мер и средств ЗИ.
15. Методы, меры обеспечения ИБ и средства ЗИ. Основные методы обеспечения ИБ. Привести примеры
16. Методы, меры обеспечения ИБ и средства ЗИ. Правовые (законодательные) меры и средства защиты информации. Привести примеры. Достоинства и недостатки законодательных мер и средств ЗИ;
17. Методы, меры обеспечения ИБ и средства ЗИ. Морально-этические меры и средства защиты информации. Привести примеры. Достоинства и недостатки морально-этических мер и средств ЗИ.
18. Методы, меры обеспечения ИБ и средства ЗИ. Организационные меры и средства защиты информации. Привести примеры. Достоинства и недостатки организационных мер и средств ЗИ.
19. Методы, меры обеспечения ИБ и средства ЗИ. Физические меры и средства защиты информации. Привести примеры. Достоинства и недостатки физических мер и средств ЗИ.
20. Методы, меры обеспечения ИБ и средства ЗИ. Программные меры и средства защиты информации. Привести примеры. Достоинства и недостатки программных средств ЗИ.
21. Методы, меры обеспечения ИБ и средства ЗИ. Аппаратные меры и средства защиты информации. Привести примеры. Достоинства и недостатки аппаратных средств ЗИ.
22. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Биометрическая идентификация;
23. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации.
24. Пароль. Атаки на пароли. Администрирование парольной системы;
25. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Криптографические ключи. Карты памяти (memory card). Смарт-карты (smart card);
26. Количественная оценка стойкости парольной защиты
27. Техники управление доступом. Матрица контроля доступа. Список контроля доступа (ACL). Таблица разрешений;
28. Техники управление доступом. Доступ на основе контента. Доступ на основе контекста. Ограниченный интерфейс. Доступ на основе правил;
29. Управление доступом. Мандатное управление доступом (MAC);
30. Управление доступом. Модель Белла-ЛаПадула;

31. Управление доступом. Избирательное управление доступом (DAC);
32. Управление доступом. Ролевое управление доступом (RBAC);
33. Управление доступом. Классическая модель доступа ОС на базе Linux
34. Механизмы ЗИ. Протоколирование и аудит;
35. Механизмы ЗИ. Шифрование. Цели и задачи. Алгоритмы шифрования;
36. Симметричное шифрование. Достоинства и недостатки.
37. Асимметричное шифрование. Достоинства и недостатки.
38. Механизмы ЗИ. Контроль целостности. Хэш-функция;
39. Механизмы ЗИ. Экранирование. Межсетевые экраты;
40. Механизмы ЗИ. Туннелирование. VPN;
41. Механизмы ЗИ. Резервное копирование и восстановление;
42. Механизмы ЗИ. Защита от компьютерных вирусов;
43. Механизмы ЗИ. Обнаружение вторжений. IDS/IPS;
44. Механизмы ЗИ. Анализ защищенности.

Вопросы для проведения зачета

1. Понятие интеллектуальной собственности.
2. Какие охранные документы на объекты интеллектуальной собственности
3. выдаются в РФ?
4. Каково содержание признака новизны изобретения?
5. Чем характеризуется устройство как объект изобретения?
6. Каковы особенности формулы изобретения на устройство?
7. Каковы особенности описания изобретения на устройство?
8. Чем характеризуется способ как объект изобретения?
9. Назначение формулы изобретения. Требования к формуле изобретения.
10. Каковы особенности формулы изобретения на способ?
11. Какие требования предъявляются к описанию изобретения?
12. Какие источники информации исключают новизну изобретения?
13. Каковы требования к заявлению о выдаче патента?
14. Какие объекты не признаются изобретениями в РФ?
15. Какие документы должна содержать заявка на выдачу патента?
16. Что является объектами патентного права?
17. Лицензионный договор и его виды.
18. Условия патентоспособности объектов патентного права.
19. Сроки действия патента на объекты патентного права.
20. Какие результаты интеллектуальной деятельности могут быть отнесены к полезным моделям?

21. Условия патентоспособности промышленного образца.
22. Какие требования предъявляются к реферату изобретения?
23. Что может быть объектами интеллектуальной собственности?
24. Какую информацию целесообразно охранять как коммерческую тайну?
25. Как оформляются графические материалы, иллюстрирующие изобретение?
26. Каким видам экспертизы подвергаются заявочные материалы на изобретение?
27. Какие результаты интеллектуальной деятельности не признаются
28. патентоспособными изобретениями?
29. Какие права имеют автор и патентообладатель?
30. Что такое аналог и прототип изобретения?
31. Что такое товарный знак и знак обслуживания?
32. Функции товарного знака
33. Как программам для ЭВМ и базам данных предоставляется правовая охрана?
34. Что такое "ноу-хау"?
35. Каков срок действия авторского права?
36. Что относится к смежным правам?
37. Что относится к служебным изобретениям?
38. Как обладатель исключительных авторских прав может оповестить о своих
39. правах на объекты авторского права?
40. Необходима ли государственная регистрация программ для ЭВМ и баз данных
41. для подтверждения исключительных прав на них?
42. Кто имеет право на подачу заявки на выдачу охранных документов на объекты
43. патентного права?
44. Что такое патентоспособность и патентная чистота?
45. Какие результаты интеллектуальной деятельности являются объектами
46. авторского права?
47. На что не распространяется авторское право?
48. Основные понятия информационной безопасности. Субъекты информационных отношений;
49. Какая информация является предметом защиты?
50. Понятие доступности, целостности и конфиденциальности.
51. Понятие угрозы,атаки, уязвимости. Примеры Угроз;
52. Понятие угрозы,атаки, уязвимости. Примеры уязвимостей;

53. Понятие угрозы,атаки, уязвимости. Примеры Атак;
54. Источник угроз ИБ. Понятие нарушителя. Модель нарушителя;
55. Модель безопасности по ГОСТ 13335-1-2006;
56. Угроза ИБ. Источники угроз ИБ. Модель угроз ИБ;
57. Угрозы ИБ. Классификация угроз ИБ. Классификация по расположению источника. Классификация по активности АИС.
58. Угрозы ИБ. Классификация угроз ИБ. Классификация по размеру ущерба.
59. Классификация по отношению к защищаемой информации.
60. Угрозы ИБ. Классификация угроз ИБ. Классификация по аспекту ИБ. Классификация по компонентам АИС.
61. Методы, меры обеспечения ИБ и средства ЗИ. Классификация методов, мер и средств ЗИ.
62. Методы, меры обеспечения ИБ и средства ЗИ. Основные методы обеспечения ИБ. Привести примеры
63. Методы, меры обеспечения ИБ и средства ЗИ. Правовые (законодательные) меры и средства защиты информации. Привести примеры. Достоинства и недостатки законодательных мер и средств ЗИ;
64. Методы, меры обеспечения ИБ и средства ЗИ. Морально-этические меры и средства защиты информации. Привести примеры. Достоинства и недостатки морально-этических мер и средств ЗИ.
65. Методы, меры обеспечения ИБ и средства ЗИ. Организационные меры и средства защиты информации. Привести примеры. Достоинства и недостатки организационных мер и средств ЗИ.
66. Методы, меры обеспечения ИБ и средства ЗИ. Физические меры и средства защиты информации. Привести примеры. Достоинства и недостатки физических мер и средств ЗИ.
67. Методы, меры обеспечения ИБ и средства ЗИ. Программные меры и средства защиты информации. Привести примеры. Достоинства и недостатки программных средств ЗИ.
68. Методы, меры обеспечения ИБ и средства ЗИ. Аппаратные меры и средства защиты информации. Привести примеры. Достоинства и недостатки аппаратных средств ЗИ.
69. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Биометрическая идентификация;
70. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации.
71. Пароль. Атаки на пароли. Администрирование парольной системы;

72. Механизмы ЗИ. Идентификация и аутентификация. Требования к идентификации. Криптографические ключи. Карты памяти (memory card). Смарт-карты (smart card);
73. Количественная оценка стойкости парольной защиты
74. Техники управление доступом. Матрица контроля доступа. Список контроля доступа (ACL). Таблица разрешений;
75. Техники управление доступом. Доступ на основе контента. Доступ на основе контекста. Ограниченный интерфейс. Доступ на основе правил;
76. Управление доступом. Мандатное управление доступом (MAC);
77. Управление доступом. Модель Белла-ЛаПадула;
78. Управление доступом. Избирательное управление доступом (DAC);
79. Управление доступом. Ролевое управление доступом (RBAC);
80. Управление доступом. Классическая модель доступа ОС на базе Linux
81. Механизмы ЗИ. Протоколирование и аудит;
82. Механизмы ЗИ. Шифрование. Цели и задачи. Алгоритмы шифрования;
83. Симметричное шифрование. Достоинства и недостатки.
84. Асимметричное шифрование. Достоинства и недостатки.
85. Механизмы ЗИ. Контроль целостности. Хэш-функция;
86. Механизмы ЗИ. Экранирование. Межсетевые экраты;
87. Механизмы ЗИ. Туннелирование. VPN;
88. Механизмы ЗИ. Резервное копирование и восстановление;
89. Механизмы ЗИ. Защита от компьютерных вирусов;
90. Механизмы ЗИ. Обнаружение вторжений. IDS/IPS;
91. Механизмы ЗИ. Анализ защищенности.

Самостоятельная работа

Самостоятельная работа студентов является важнейшим компонентом образовательного процесса, развивающим их способности к самообучению и повышению своего профессионального уровня.

Цель самостоятельной работы - самостоятельно приобретать новые знания, используя современные образовательные технологии, обобщать, оформлять, представлять и докладывать результаты выполненной работы, а также критически анализировать полученные знания и аргументировано отстаивать свои предложения.

Самостоятельная работа направлена на закрепление и углубление освоения учебного материала, она включает в себя следующие виды работы студентов: работа с информационным материалом, передаваемым преподавателем до начала занятий, самостоятельная работа по изучению

автоматизированные системы проектирования, подготовка рефератов, подготовка к практическим занятиям, подготовка к зачету.

Самостоятельная работа заключается в изучении отдельных тем курса по заданию преподавателя. Несмотря на то, что учебным планом не предусмотрено написание рефератов, с целью активизации самостоятельной работы преподаватель может предложить студенту выполнить реферативную работу. При этом обучающимся может быть предложена и своя тематика.

Студенты готовят рефераты, делают по нему презентации и докладывают перед коллегами в группе группы. Лучшие доклады представляются на вузовской студенческой конференции.

Тематика самостоятельной работы студентов

1. Понятие результатов интеллектуальной деятельности.
2. Значение результатов интеллектуальной деятельности для развития
3. экономики страны.
4. Научно-технический потенциал страны как ресурсная основа инновационной сферы.
5. Инновационная продукция.
6. Субъекты творческой деятельности, их взаимодействие в процессе создания и реализации результатов интеллектуальной деятельности.
7. Различные уровни интеллектуальной деятельности: международный, федеративный, субъекта федерации, муниципальный, частный.
8. Государственная политика в области интеллектуальной деятельности.
9. Развитие различных форм интеграции науки, образования,
10. производства (технопарки, инновационные бизнес-инкубаторы и т. д.).
11. Государственная поддержка субъектов инновационной деятельности.
12. Президент РФ о необходимости и неизбежности инновационного пути развития России.
13. Ключевая отрасль национальной экономики как локомотив инновационного пути развития России.
14. Соглашение о партнёрстве и сотрудничестве между РФ и Европейским союзом 1994 года. Задачи стран – членов ЕС. Обязательность для России
15. директив ЕС.
16. Североамериканская ассоциация свободной торговли – НАФТА. Полномочия ассоциации, структура. Страны-участницы ассоциации.
17. Евразийская патентная конвенция от 09.09.1994 года.
18. Евразийская патентная организация – организационная структура и
19. состав.
20. Патентная инструкция к Евразийской патентной конвенции.

21. Положение о пошлинах Евразийской патентной организации. Административная инструкция к Евразийской патентной конвенции.
22. Положение о евразийских патентных поверенных.
23. Форма заявления о выдаче евразийского патента на изобретение.
24. История создания ВОИС.
25. Структура, функции, управление ВОИС (Всемирная организация интеллектуальной собственности).
26. Сотрудничество ВОИС (Всемирная организация интеллектуальной собственности) с другими странами в целях развития.
27. Подготовка кадров ВОИС (Всемирная организация интеллектуальной собственности), юридические консультации и помощь.
28. Государственное стимулирование создания и использования
29. изобретений, полезных моделей и промышленных образцов.
30. Требования к документам заявки на выдачу патента на изобретение,
31. полезную модель или промышленный образец.
32. Приоритет изобретения, полезной модели или промышленного образца.
33. Формальная экспертиза заявки на изобретение, полезную модель или
34. промышленный образец. Экспертиза заявки на изобретение, полезную модель
35. или промышленный образец по существу.
36. Решение о выдаче или об отказе в выдаче патента на изобретение,
37. полезную модель или промышленный образец.
38. Изобретения, полезные модели, промышленные образцы, созданные при выполнении работ по государственному или муниципальному контракту.
39. Государственная регистрация изобретений, полезных моделей и
40. промышленных образцов.
41. Использование изобретения, полезной модели или промышленного
42. образца в интересах национальной безопасности.
43. Принудительная лицензия на изобретение, полезную модель или
44. промышленный образец. Открытая лицензия на изобретение, полезную модель или промышленный образец.
45. Форма и государственная регистрация договоров о распоряжении исключительным правом на изобретение, полезную модель и промышленный образец.
46. Прекращение и восстановление действия патента.
47. Особенности правовой охраны и использования секретных изобретений.
48. Промышленный образец как объект правовой охраны.
49. Исключительное право на товарный знак и знак обслуживания.
50. Полезная модель – правовая охрана и защита.

51.Какие признаки объектов являются демаскирующими?
52. Приведите классификацию демаскирующих признаков объектов защиты.
53. Опишите опознавательные демаскирующие признаки объектов защиты.
54. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
55. Что такое информативность демаскирующего признака?
56. Что такое тезаурус?
57. Перечислите основные носители признаковой информации.
58. Перечислите основные источники конфиденциальной информации.
59. В чем отличие прямых источников семантической информации от косвенных?
60. Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации
61.В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
62. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
63. В чем специфика деятельности Федеральной службы безопасности?
64. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
65. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
66. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
67. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
68. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
69. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
70. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
71. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
72.Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?
73. Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
74. Дайте определение информационной безопасности, прокомментируйте

его составляющие.

75. Что такое защита информации?
76. Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни.
77. Какую информацию нельзя засекречивать как имеющую статус государственной тайны?
78. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
79. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
80. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
81. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
82. Какая информация не может быть отнесена к коммерческой тайне?
83. Перечислите основные объекты банковской тайны.
84. Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
85. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
86. Перечислите основные объекты интеллектуальной собственности.
87. Что такое объекты угроз ИБ и в чем они выражаются?
88. Каковы основные источники угроз защищаемой информации?
89. Каковы цели угроз информации со стороны злоумышленников?
90. Перечислите основные источники конфиденциальной информации.
91. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
92. Перечислите базовые способы защиты информации.
93. Изобразите графически схему концептуальной модели системы ИБ.
94. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
95. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
96. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
97. Как осуществляется утечка конфиденциальной информации?
98. Каким образом непреднамеренное разглашение информации может

привести к ее утечке?

99. Что такое наблюдение в теории информационной безопасности?

100. Что такое подслушивание в теории информационной безопасности?

101. Что такое перехват в теории информационной безопасности?

102. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.

103. Какие организации формируют структуру разведывательного сообщества США?

104. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.

105. Охарактеризуйте программные атаки на доступность.

106. Приведите примеры «бомбы», «червя», «вируса».

107. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.

108. Что в ИБ понимают под маскарадом?

109. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации

110. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации

111. Назовите три группы мероприятий по технической защите информации.

112. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?

113. Прокомментируйте основные организационно-технические мероприятия по ЗИ.

114. Прокомментируйте основные технические мероприятия по технической защите информации.

115. Раздел 9

116. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.

117. В чем заключается специфика управления, как сервиса безопасности?

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Сычев А.Н. Защита интеллектуальной собственности и патентоведение [Электронный ресурс]: учебное пособие/ Сычев А.Н.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2012.— 160 с., http://www.iprbookshop.ru/13880.html.
2. **Управление информацией и знаниями в компании**: Учебник / С.Н. Селетков, Н.В. Днепровская. - М.: НИЦ ИНФРА-М, 2014. - 208 с., http://znanium.com/catalog.php?bookinfo=406126.
3. **Экономика и коммерциализация интеллектуальной собственности**: учебник / В.И. Мухопад. - М.: Магистр, НИЦ ИНФРА-М, 2016. - 496 с., http://znanium.com/catalog.php?bookinfo=527713.

Дополнительная литература:

1. Жуков Е.А. Право интеллектуальной собственности [Электронный ресурс]: учебное пособие/ Жуков Е.А.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2011.— 227 с., http://www.iprbookshop.ru/44823.html.Резепова В.Е. Право интеллектуальной собственности [Электронный ресурс]: учебное пособие/ Резепова В.Е.— Электрон. текстовые данные.— Саратов: Ай Пи Эр Медиа, 2009., http://www.iprbookshop.ru/1463.html.
2. Зенин И.А. Интеллектуальная собственность и ноу-хау [Электронный ресурс]: учебное пособие/ Зенин И.А.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2009.— 328 с.,http://www.iprbookshop.ru/10676.html.
3. Резепова В.Е. Право интеллектуальной собственности [Электронный ресурс]: учебное пособие/ Резепова В.Е.— Электрон. текстовые данные.— Саратов: Ай Пи Эр Медиа, 2009.http://www.iprbookshop.ru/1463.html.

Периодические издания: «Литейное производство», «Литейщик России», «Цветная металлургия» (библиотека ВлГУ).

Программное и коммуникационное обеспечение

http://www.de.vlsu.ru:81/umk → Кафедра «Технологии функциональных и конструкционных материалов» → (вход для зарегистрированных пользователей).

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации образовательного процесса по дисциплине используются мультимедийные аудитории кафедры «Технологии функциональных и конструкционных материалов». Кафедра располагает компьютерным классом с современным программным обеспечением, локальной вычислительной сетью и доступом в интернет для работы с Интернет-ресурсом по изучаемой дисциплине.

При проведении занятий используются:

- «Компьютерный класс ИМиАТ», площадь 52 м^2, оснащение: компьютерный класс с 15 рабочими станциями Athlon 64 3000+ и Core 2 Quad, с выходом в Internet, на которых установлено коммерческое лицензионное программное обеспечение: математические пакеты Mathcad 14, MATLAB R14, , CAD/CAM/CAE-система Pro/ENGINEER Wildfire 4 (включая Pro/MECHANICA), КОМПАС 3D v.12; и программное обеспечение со свободными лицензиями: GIMP, Gthumb, ufraw, ImageJ, Inkspace, Dia, Sribus, Maxima, SAGE, qalculate, Scilab, Axiom, GNU Octave, SDDS, GNU R, gnuplot, OpenDX, Elmer, Calculix, Impact, WARP3D, Code_Aster, OpenFOAM, OpenCalphad, QCad, BRL CAD, gCAD3D, FreeCAD, OpenSCAD, T- FLEX CAD, Eclipse, MS Visual Studio Express, Free Pascal Compiler.
- «Учебная аудитория» № 211 корпуса 2, площадь 54 м2 , оснащение: Мультимедийный проектор Benq DLP, экран Seha, ноутбук

Научно-техническая библиотека ВлГУ располагает обширным фондом научно-технической литературы.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 22.03.01 «Материаловедение и технологии материалов»

Рабочую программу составил

Доцент кафедры ТФ и КМ, к.т.н. Д.В. Сухоруков _____

Рецензент главный технолог ООО «Казанское литейно-инновационное объединение» _____Е.В.Середа

Программа рассмотрена и одобрена на заседании кафедры ТФ и КМ протокол № 4а от 17.12.2015 года

Заведующий кафедрой ТФ и КМ _____ В.А. Кечин

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 22.03.01 «Материаловедение и технологии материалов»

протокол № 4 от 17.12.2015 года

Председатель комиссии _____ В.А. Кечин

Программа переутверждена:

на _____ учебный год, протокол №____ от_____

Зав. кафедрой ТФ и КМ_____

на _____ учебный год, протокол №____ от_____

Зав. кафедрой ТФ и КМ_____

на _____ учебный год, протокол №____ от_____

Зав. кафедрой ТФ и КМ_____

на _____ учебный год, протокол №____ от_____

Зав. кафедрой ТФ и КМ_____

на _____ учебный год, протокол №____ от_____

Зав. кафедрой ТФ и КМ_____

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 2020/2021 учебный год

Протокол заседания кафедры № 1 от 28.08.20 года

Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой _____