ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 29.01.2022

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины В.1.05 Практикум по виду профессиональной деятельности
для направления 10.03.01 Информационная безопасность
уровень бакалавр **тип программы** Бакалавриат
профиль подготовки Безопасность автоматизированных систем
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 01.12.2016 № 1515

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 29.01.2022

А. Н. Соколов

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Баринов А. Е.
Пользователь: barinovae
Дата подписания: 27.01.2022

А. Е. Баринов

Челябинск

1. Цели и задачи дисциплины

Цели: Получение практических навыков научно-исследовательской и проектно-конструкторской деятельности в лабораторных и производственных условиях путем непосредственного участия студентов в решении актуальных производственных и научно-технических задач с раскрытием индивидуальных особенностей и способностей. Задачи: Подготовка студентов к самостоятельной работе в сфере информационной безопасности. Применение студентами знаний и умений, полученных при изучении дисциплин специальности для решения междисциплинарных задач в сфере информационной безопасности. Овладение навыками анализа имеющихся ресурсов и управления ими для решения поставленных задач обеспечения защиты информации.

Краткое содержание дисциплины

Практикум предполагает решение задач полного цикла обеспечения информационной безопасности объекта информатизации, начиная от аналитико-синтетической обработки информации по виду профессиональной деятельности до анализа угроз и построения комплексной системы защиты. При этом обучающиеся вовлекаются во все аспекты обеспечения ее информационной безопасности: организационные, программно-аппаратные и технические

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПСК-4.4 способностью участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Знать:Знать:безопасные сетевые технологии, в которых используются программно-аппаратные средства обеспечения информационной безопасности автоматизированных систем
	Уметь:
	Владеть: Владеть:навыками применения программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
ПК-11 способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Знать:Знать:методики расчета и инструментального контроля показателей технической защиты информации
	Уметь:Уметь: использовать методики расчета и инструментального контроля показателей технической защиты информации
	Владеть:Владеть:методами расчета и инструментального контроля показателей технической защиты информации
ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Знать:Знать:принципы формирования политики информационной безопасности в информационных (автоматизированных) системах
	Уметь:Уметь:разрабатывать частные политики информационной безопасности

	информационных (автоматизированных) систем
	Владеть:Владеть:методами управления информационной безопасностью информационных (автоматизированных) систем
ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знать:Знать:программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях
	Уметь:Уметь:проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированных систем с целью обеспечения требуемого уровня ее защищенности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	Владеть:
ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Знать:Знать:основные угрозы безопасности информации и модели нарушителя в информационных (автоматизированных) системах
	Уметь:Уметь:анализировать и оценивать угрозы информационной безопасности информационных (автоматизированных) систем
	Владеть:Владеть:методами мониторинга угроз информационной безопасности информационных (автоматизированных) систем
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знать:Знать:отечественные и зарубежные стандарты в области информационной безопасности
	Уметь:Уметь:применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
	Владеть:Владеть: навыками использования отечественныхи зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Знать:Знать:принципы организации информационных систем в соответствии с требованиями по защите информации
	Уметь:Уметь:формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
	Владеть:Владеть:формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их

	основе
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Знать:информационные ресурсы разных видов и форм по виду профессиональной деятельности
	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
	Владеть:технологиями поиска и аналитико-синтетической обработки информационных ресурсов по виду профессиональной деятельности
ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знать:Знать:принципы организации информационных систем в соответствии с требованиями по защите информации
	Уметь:Уметь:разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем
	Владеть:Владеть:навыками выбора и обоснования критериев эффективности функционирования защищенных информационных (автоматизированных) систем
ПСК-4.1 способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	Знать:Знать:организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы
	Уметь:Уметь:осуществлять управление и администрирование защищенных автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем
	Владеть:Владеть:навыками разработки политик информационной безопасности автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
В.1.06 Безопасность операционных систем, Б.1.16 Основы информационной безопасности, В.1.07 Безопасность сетей электронных вычислительных машин	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования

В.1.06 Безопасность операционных систем	Знать основные виды и классы операционных систем, методологически и практические подходы к обеспечению безопасности ОС, основные программно-аппаратные средства защиты информации в ОС. Уметь использовать на практике базовые средства безопасности ОС различных классов.
Б.1.16 Основы информационной безопасности	Знать структуру комплексной системы защиты информации, состав видов защиты информации, основное действующее законодательство в области защиты информации. Уметь определять структуру КСЗИ, формулировать требования и состав к конкретной КСЗИ.
В.1.07 Безопасность сетей электронных вычислительных машин	Знать структуру и способы организации сетей, уметь строить карту сетей различных классов, владеть навыками использования программных средств и методов обеспечения безопасности сетей ЭВМ.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 6 з.е., 216 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах		
		Номер семестра		
		6	7	8
Общая трудоёмкость дисциплины	216	72	72	72
Аудиторные занятия:	132	64	32	36
Лекции (Л)	0	0	0	0
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	132	64	32	36
Лабораторные работы (ЛР)	0	0	0	0
Самостоятельная работа (СРС)	84	8	40	36
Поиск и аналитико-синтетическая обработка информации по проблемам ИБ	48	8	40	0
Изучение уязвимостей бинарных приложений и основных стандартов тестирования компьютерных систем на проникновение.	36	0	0	36
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет	зачет	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность)	64	0	64	0
2	Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность)	32	0	32	0

3	Организация и управление безопасностью компьютерных систем организации (проектно-конструкторская деятельность)	36	0	36	0

5.1. Лекции

Не предусмотрены

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Методика НИР: основные этапы	6
2	1	Поиск и формулировка проблемы ИБ, составление перечня ключевых слов.	6
3	1	Поиск научной литературы в русскоязычных электронных ресурсах	6
4	1	Поиск научной литературы в зарубежных электронных ресурсах	6
5	1	Поиск экспертной информации по проблеме	6
6	1	Поаспектная систематизация и отбор выявленной литературы	6
7	1	Поаспектное реферирование выявленной литературы	6
8	1	Аналитико-синтетическая переработка информации	6
9	1	Подготовка обзора по научной проблеме ИБ	6
10	1	Оформление текста и Списка использованной литературы, подготовка Презентации.	6
11	1	Защита НИР	4
12	2	Изучение системы нормативных правовых документов по ПД: ФЗ, постановления правительства РФ.	4
13	2	Изучение системы нормативных правовых документов по ПД: документы ФСТЭК РФ.	6
14	2	Изучение системы нормативных правовых документов по ПД: документы ФСБ РФ.	4
15	2	Определение актуальных угроз безопасности ИСПДн	6
16	2	Разработка Модели угроз безопасности ГИС (МИС)	6
17	2	Определение актуальных угроз безопасности по отраслевым стандартам	6
18	3	Изучение основных уязвимостей бинарных приложений	4
19	3	Написание shellcode	4
20	3	Написание эксплойтов под основные уязвимости бинарных приложений	4
21	3	Изучение средств тестирования на проникновение	4
22	3	Практика применения средств тестирования на проникновение	4
23	3	Организационные аспекты организации тестирования на проникновение	4
24	3	Комплексная задача по тестированию на проникновение	4
25	3	Изучение формата исполняемых файлов операционных систем семейства Microsoft Windows	4
26	3	Изучение формата исполняемых файлов Unix-подобных операционных систем	4

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Изучение стандартов по тестированию компьютерных систем на проникновение	Комплекс БР ИББС, PCI DSS и др. нормативных документов	42
Поиск и аналитико-синтетическая обработка информации по проблеме	1.Артемова С.Г., Душко О.В., Сомова К.В. Основы научных исследований. – Волгоград: Волгоградский государственный технический университет., 2021.– 106с 2.Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательств и защиты от манипуляций : учебное пособие / Э. П. Теплов, Ю. А. Гатчин, А. П. Нырков, В. В. Сухостат. — Санкт-Петербург : НИУ ИТМО, 2016. — 120 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91381 (дата обращения: 24.09.2021). — Режим доступа: для авториз. пользователей. 3. Дмитриева, И.Н. Основы научных исследований: учебное пособие / И.Н. Дмитриева, А.Ф. Черненко. –Челябинск: Издательский центр ЮУрГУ, 2020. –52с. 4. Информационные ресурсы НБ ЮУрГУ	42

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Проектные технологии обучения	Практические занятия и семинары	Проектирование информационной модели проблемной области ИБ	32

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Проблемное обучение	Выявление проблем ИБ и путей их решения в России и за рубежом (1 раздел)

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов	Контролируемая компетенция ЗУНы	Вид контроля	№№

дисциплины		(включая текущий)	заданий
Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность)	ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Защита отчета по НИР	1-8
Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность)	ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	Защита отчета по практической работе	1-11
Комплексное исследование безопасности информационной инфраструктуры (научно-исследовательская деятельность)	ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Защита отчета по практической работе	1-11
Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность)	ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Защита отчета по практической работе	12-17
Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность)	ПК-11 способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Защита отчета по практической работе	12-17
Организация и управление безопасностью ИТ инфраструктуры и документирование процедур (проектно-конструкторская деятельность)	ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Защита отчета по практической работе	12-17
Организация и управление безопасностью компьютерных систем организации (проектно-конструкторская деятельность)	ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Защита отчета по практической работе	18-23
Организация и управление безопасностью компьютерных систем	ПСК-4.4 способностью участвовать в разработке аппаратных и программных средств в составе автоматизированных	Защита отчета по практической работе	18-23

организации (проектно-конструкторская деятельность)	систем, связанных с обеспечением информационной безопасности		
Все разделы	ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Бонус-рейтинг	1-23
Все разделы	ПСК-4.1 способностью учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	Посещаемость занятий	1-23

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Защита отчета по практической работе	Защита отчета о выполнении задания осуществляется индивидуально. Студентом предоставляет выполненное задание. Оценивается качество правильность выводов и ответы на вопросы (задаются минимум 2 вопроса). При оценивании результатов используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей (за каждое задание): полностью выполнили базовую часть задания (1 балл), выполнили дополнительную часть задания (1 балл). Если студент в обозначенный срок не сдает работу минимум на базовую часть, то дополнительная часть становится обязательной и максимальный балл за задание становится (1 балл)	Зачтено: рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: рейтинг обучающегося за мероприятие менее 60 %.
Посещаемость занятий	Не оценивается	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %.
Бонус-рейтинг	Студент представляет копии документов, подтверждающие победу или участие в научных конференциях по тематике дисциплины При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Максимально возможная величина бонус-рейтинга +15 %.	Зачтено: +15 % за победу в научной конференции международного уровня +10 % за победу в научной конференции российского уровня +5 % за победу в научной конференции университетского уровня +1 % за участие в научной конференции. Не зачтено: -

Защита отчета по НИР	Защита отчета о выполнении задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 2 вопроса). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей (за каждое задание): - приведены методики выполнения работы – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 1 балл Максимальное количество баллов – 5. Весовой коэффициент мероприятия (за каждое задание) – 0,1.	Зачтено: рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: рейтинг обучающегося за мероприятие менее 60 %.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Защита отчета по практической работе	1) Используя уязвимость переполнения буфера в стеке выполнить произвольный код в программе 2) Реализовать атаку на DHCP-сервер 3) Реализовать загрузчик PE-файла 4) Реализовать загрузчик ELF-фалйа
Посещаемость занятий	.
Бонус-рейтинг	
Защита отчета по НИР	Темы НИР: 1.Обеспечение целостности информации в ИС: отечественные и зарубежные технологии. 2. Обеспечение доступности информации в ИС: отечественные и зарубежные технологии. 3. Обеспечение конфиденциальности информации в ИС: отечественные и зарубежные технологии. 4.Правовая защита информации в России и за рубежом. 5.Организационная защита информации в России и за рубежом. 6.Аппаратная защита информации в России и за рубежом 7.Программная защита информации в России и за рубежом. 8.Инженерно-техническая защита информации в России и за рубежом и др.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Астахова Л.В._Практикум_Методическое пособие
2. Баринов А.Е. Методические указания по практикуму по научно-исследовательской деятельности(в локальной сети кафедры)

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Астахова Л.В._Практикум_Методическое пособие
2. Баринов А.Е. Методические указания по практикуму по научно-исследовательской деятельности(в локальной сети кафедры)

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Персональные данные в государственных информационных ресурсах / М.Ю. Брауде-Золотарёв, Е.С. Сербина, В.С. Негородов, И.Г. Волошкин. — Москва : Дело РАНХиГС, 2016. — 56 с. — ISBN 978-5-7749-1121-9. — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/74913
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Сабанов, А.Г. Защита персональных данных в организациях здравоохранения : учебное пособие / А.Г. Сабанов, В.Д. Зыков, Р.В. Мещеряков. — Москва : Горячая линия-Телеком, 2012. — 206 с. — ISBN 978-5-9912-0243-5. — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/5194
3	Основная литература	Электронно-библиотечная система издательства Лань	Тумбинская, М.В. Защита информации на предприятии : учебное пособие / М.В. Тумбинская, М.В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/130184
4	Основная литература	Электронно-библиотечная система издательства Лань	Петренко, В.И. Защита персональных данных в информационных системах. Практикум : учебное пособие / В.И. Петренко, И.В. Мандрица. — Санкт-Петербург : Лань, 2019. — 108 с. — ISBN 978-5-8114-3311-7. — — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/111916
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Каширская, Е. Н. Защита информации в информационно - управляющих системах : учебное пособие / Е. Н. Каширская, М. А. Макаров. — Москва : РТУ МИРЭА, 2020. — 67 с. https://e.lanbook.com/book/167621
6	Основная литература	eLIBRARY.RU	Артемова С.Г., Душко О.В., Сомова К.В. Основы научных исследований. – Волгоград: Волгоградский государственный технический университет., 2021.– 106с https://elibrary.ru/item.asp?id=45577821
7	Основная литература	Электронно-библиотечная система издательства Лань	Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательств и защиты от манипуляций : учебное пособие / Э. П. Теплов, Ю. А. Гатчин, А. П. Ныркова, В. В. Сухостат. — Санкт-Петербург : НИУ ИТМО, 2016. — 120 с. — Режим

			доступа: для авториз. пользователей. https://e.lanbook.com/book/91381
8	Дополнительная литература	eLIBRARY.RU	Дмитриева, И.Н. Основы научных исследований: учебное пособие / И.Н. Дмитриева, А.Ф. Черненко. –Челябинск: Издательский центр ЮУрГУ, 2020. –52с. https://elibrary.ru/item.asp?id=44821588

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. -База данных polpred (обзор СМИ)(бессрочно)
2. -Стандартинформ(бессрочно)
3. -База данных ВИНИТИ РАН(бессрочно)
4. -Информационные ресурсы ФИПС(бессрочно)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows 10, MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net Studio 8.5; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2