Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Беспалов Владимир Александрович
Должность: Ректор МИЭТ
Дата подписания: 16.07.2024 15:13:05
Уникальный программный ключ:
ef5a4fe6ed0ffdf3f1a49d6ad1b49464dc1bf7354f736d76c8f8bea882b8d602

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____А.Г. Балашов
«27» 02 2024 г.
М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Обеспечение безопасности информационных систем»

Направление подготовки –27.04.08«Управление интеллектуальной собственностью»
Направленность (профиль)– «Правовое обеспечение управления интеллектуальной собственностью»

Москва 2024

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

Компетенция ПК-3 «Способен осуществлять оценку результатов интеллектуальной деятельности в области создания инновационных продуктов» сформулирована на основе профессионального стандарта 40.206 «Специалист по управлению интеллектуальной собственностью и трансферу технологий».

Обобщенная трудовая функция С.Анализ и оценка инновационных проектов в рамках трансфера технологий.

Трудовая функция С/03.*7* Оценка стоимости прав на РИД, созданных или приобретаемых в ходе реализации инновационных проектов для целей дальнейшего использования и/или трансфера технологий.

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения подкомпетенций**
ПК-3.ОБИ Способен осуществлять оценку соответствия продуктов информационной технологии требованиям обеспечения безопасности информации	Контроль обеспечения соответствия товаров и услуг государственным и международным требования в области сертификации	**Знает** нормативную базу и современную методологию в области обеспечения безопасности информации продуктов информационной технологий; **Умеет** применять нормативную базу и современную методологию при разработке требований по обеспечению безопасности информации, разработке продуктов информационной технологии и выполнении требований обеспечения безопасности информации на всех этапах жизненного цикла продуктов информационной технологии; **Имеет опыт** работы с нормативным документами, формирования требований по обеспечению безопасности информации и оценки продуктов информационной технологии на соответствие требованиям обеспечения безопасности информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» образовательной программы.

Входные требования к дисциплине основываются на теоретических знаниях и практических навыках, приобретённых студентами в процессе обучения в бакалавриате и 1 и 2 семестре обучения в магистратуре.

Дисциплина предназначена для окончательного формирования профессиональной компетенции ПК-3 Способен осуществлять оценку результатов интеллектуальной деятельности в области создания инновационных продуктов.

До начала обучения по дисциплине у обучающегося должны быть сформированы следующие подкомпетенции:

УК-1.МНП Способен критически анализировать познавательные проблемные ситуации, на основе методологии науки вырабатывать стратегию действий;

ОПК-1.УИС Способен анализировать и выявлять естественнонаучную сущность проблем управления интеллектуальной собственностью;

ОПК-2.УИС Способен формулировать научные и прикладные задачи управления интеллектуальной собственностью в технических системах и обосновывать методы их решения.

Дисциплина изучается в 3 семестре.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа			Самостоятельная работа (часы)	Промежуточная аттестация
				Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
2	3	3	108	32	-	16	60	За

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторныер аботы (часы)	Практические занятия (часы)		
1. Современная постановка задачи защиты информации	*8*	-	*4*	*6*	*Опрос на практических занятиях. Контроль выполнения онлайн тестов.*
2. Общие критерии оценки безопасности информационных технологий	*6*	-	*2*	*6*	*Опрос на практических занятиях. Контроль выполнения онлайн тестов.*
3. Понятие доверия и обеспечение доверия к информационным технологиям	*6*	-	*2*	*3*	*Опрос на практических занятиях. Контроль выполнения онлайн тестов.*
4.Требования ФСТЭК РФ и ФСБ РФ к обеспечению безопасности информации	*12*	-	*8*	*45*	*Опрос на практических занятиях. Контроль выполнения онлайн тестов. Контроль выполнения индивидуального задания*

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1	2	Взаимосвязь современных понятий в области защиты информации
	2	3	Модели угроз информационным технологиям
	3	3	Риск ориентированный подход к обеспечению безопасности информационных систем
2	4	3	Методология обеспечения безопасности информации в соответствии с общими критериями оценки безопасности информационных технологий

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
	5	3	Функциональные требования безопасности информации в соответствии с общими критериями оценки безопасности информационных технологий
3	6	3	Понятие доверия к информационным технологиям. Методология обеспечения доверия к информационным технологиям
	7	3	Требования доверия в соответствии с общими критериями оценки безопасности информационных технологий
4	8	2	Система нормативных документов по защите информации. Основные отечественные, зарубежные и международные документы
	9	2	Средства криптографической защиты информации и требования к ним
	10	2	Классификация информационных систем в соответствии с документами ФСТЭК РФ
	11	3	Требования по обеспечению безопасности информации в ИСПДн
	12	3	Требования по обеспечению безопасности информации в объектах КИИ

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование занятия
1	1	2	Разработка модели угроз безопасности информационных систем
	2	2	Оценка рисков информационной безопасности
2	3	2	Разработка функциональных требований безопасности в соответствии с общими критериями оценки безопасности информационных технологий
3	4	2	Формирование требований доверия
4	5	2	Разработка требований безопасности к СКЗИ
	6	2	Разработка требований обеспечения безопасности информации в соответствии с документами ФСТЭК РФ
	7	2	Особенности обеспечения безопасности информации в ИСПДн
	8	2	Особенности обеспечения безопасности информации в объектах КИИ

4.3. Лабораторные работы

Не предусмотрены.

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	2	Подготовка к практическим занятиям
	4	Изучение лекций 1- 3 онлайн курса «Академия Microsoft: Анализ и управление рисками в информационных системах на базе операционных систем Microsoft» и выполнение онлайн тестов
2	1	Подготовка к практическому занятию
	5	Изучение лекций 2, 3, 5 - 7 онлайн курса «Стандарты информационной безопасности» и выполнение онлайн тестов
3	1	Подготовка к практическому занятию
	2	Изучение лекции 4 онлайн курса «Стандарты информационной безопасности» и выполнение онлайн тестов
4	4	Подготовка к практическим занятиям
	4	Изучение лекций 1 - 6 онлайн курса «Общие вопросы технической защиты информации» и выполнение онлайн тестов
	9	Изучение лекции онлайн курса «Обеспечение безопасности персональных данных» и выполнение онлайн тестов
	28	Выполнение индивидуального задания и подготовка к его защите

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС// URL: , http://orioks.miet.ru/):

Сценарий обучения по дисциплине «Обеспечение безопасности информационных систем», реализуемой с использованием технологии электронного обучения;

Модуль 1 «Современная постановка задачи защиты информации»:

✓ *Презентации к лекциям, учебная литература по дисциплине, нормативные документы по Модулю 1.*

Модуль 2 «Общие критерии оценки безопасности информационных технологий»:

✓ *Презентации к лекциям, учебная литература по дисциплине, нормативные документы по Модулю 2.*

Модуль 3 «Понятие доверия и обеспечение доверия к информационным технологиям»:

✓ *Презентации к лекциям, учебная литература по дисциплине, нормативные документы по Модулю 3.*

Модуль 4 «Требования ФСТЭК РФ и ФСБ РФ к обеспечению безопасности информации»:

✓ *Презентации к лекциям, учебная литература по дисциплине, нормативные документы по Модулю 4;*

✓ *Методические рекомендации по выполнению индивидуального проекта по дисциплине.*

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Основы информационной безопасности: Учеб. пособие / В.А. Галатенко. - 2-е изд. - М. : ИНТУИТ, 2016. - 266 с. - URL: https://e.lanbook.com/book/100295 (дата обращения: 15.12.2023). - ISBN 978-5-94774-821-5
2. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков ; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - Имеется электронная версия издания. - ISBN 978-5-7256-0973-8
3. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учеб. пособие / П.Н. Девянин. - М.: Горячая линия-Телеком, 2012. - 320 с. - URL: https://e.lanbook.com/book/5150 (дата обращения: 15.12.2023). - ISBN 978-5-9912-0147-6.
4. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : Учеб. пособие / Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - [2-е изд., стер.]. - Москва : Горячая линия-Телеком, 2012. - 550 с. - URL: https://e.lanbook.com/book/5114 (дата обращения: 15.12.2023). - ISBN 978-5-9912-0257-2

Нормативная литература

1. ГОСТ Р 51898 – 2002 Аспекты безопасности. Правила включения в стандарты;
2. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий, Введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187;
3. ГОСТ Р 51897-2011 Менеджмент риска. Термины и определения;
4. ГОСТ Р ИСО/МЭК 31000-2010 Менеджмент риска. Принципы и руководство;
5. ГОСТ Р ИСО/МЭК 31010-2011 Методы оценки риска;
6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности;
7. Методика определения актуальных угроз безопасности персональных данных при их обработке и информационных системах персональных данных (утвержден заместителем директора ФСТЭК России 14 февраля 2008 г.);
8. ГОСТ Р 50922-2006 “Защита информации. Основные термины и определения”;
9. Рекомендации по стандартизации Р 50.1.056 – 2005 “Техническая защита информации. Основные термины и определения”;

10. ISO/IEC 19790:2012 Information technology – Security techniques – Security requirements for cryptographic modules;
11. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель;
12. ГОСТ Р ИСО 7498-2-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

Периодические издания

1. БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.spels.ru/index.php/bit (дата обращения: 15.12..2023). - Режим доступа: свободный. - ISSN 2074-7128 (Print)
2. ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ : научный журнал / Научно-производственное объединение Эшелон. - Москва : НПО Эшелон, 2013 - . - URL: https://cyberrus.info/ (дата обращения: 15.12.2023). - Режим доступа: свободны
3. ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ : научно-практический журнал / ФГУП "Научно-технический центр оборонного комплекса "Компас". - Москва : ФГУП НТЦ оборонного комплекса Компас, 1974 - . - URL: https://eivis.ru/browse/publication/93931 (дата обращения: 15.12.2023). - Режим доступа: по подписке

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. ФСТЭК России / Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации: сайт. – URL: https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii (дата обращения 25.12.2023)
2. Лань : Электронно-библиотечная система Издательства Лань. - СПб., 2011-. - URL: https://e.lanbook.com (дата обращения: 15.12.2023). - Режим доступа: для авторизированных пользователей МИЭТ.
3. Юрайт : Электронно-библиотечная система : образовательная платформа. - Москва, 2013 - . - URL: https://urait.ru/ (дата обращения : 15.12.2023); Режим доступа: для авторизированных пользователей МИЭТ.
4. eLIBRARY.RU: научная электронная библиотека: сайт. – Москва, 2000. – URL: https://elibrary.ru (дата обращения: 15.12.2023). – Режим доступа: для зарегистрированных пользователей.
5. Росстандарт: сайт. – URL: https://www.rst.gov.ru/portal/gost/home/standarts (дата обращения 25.12.2023).

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, основанное на В ходе реализации обучения, используются **смешанное обучение,** основанное на

интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий формами и видами взаимодействия в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: раздел ОРИОКС «Домашние задания» и электронная почта.

В процессе обучения при проведении занятий и для самостоятельной работы используются **внутренние электронные ресурсы** в форме презентаций лекций.

При проведении занятий и для самостоятельной работы используются **внешние электронные ресурсы:**

- Негосударственное образовательное частное учреждение дополнительного профессионального образования «Национальный Открытый Университет «ИНТУИТ», Курс «Академия Microsoft: Анализ и управление рисками в информационных системах на базе операционных систем Microsoft», [режим доступа - свободный], URL: https://intuit.ru/studies/courses/531/387/info, (дата обращения: 15.12.2023);
- Негосударственное образовательное частное учреждение дополнительного профессионального образования «Национальный Открытый Университет «ИНТУИТ», Курс «Стандарты информационной безопасности», [режим доступа - свободный], URL: https://intuit.ru/studies/courses/30/30/info, (дата обращения: 15.12.2023);
- Негосударственное образовательное частное учреждение дополнительного профессионального образования «Национальный Открытый Университет «ИНТУИТ», Курс «Общие вопросы технической защиты информации», [режим доступа - свободный], URL: https://intuit.ru/studies/courses/30/30/info, (дата обращения: 15.12.2023);
- Негосударственное образовательное частное учреждение дополнительного профессионального образования «Национальный Открытый Университет «ИНТУИТ», Курс «Обеспечение безопасности персональных данных», [режим доступа - свободный], URL: https://intuit.ru/studies/courses/697/553/info, (дата обращения: 15.12.2023).

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Специализированная мебель (место преподавателя, посадочные места для студентов) Материально-техническое оснащение: Моноблок, LED телевизоры 75 дюймов, LED телевизоры 65 дюймов, система видео отображения, PTZ-камера, устройство записи и трансляции, радиосистема с петличным микрофоном, двухполосная	LibreOffice 6.0.1.1 Интернет броузер (IE, MF или другой)

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	акустическая система, подавитель обратной связи, микшер, одноканальный трансляционный усилитель, система звукоусиления, конференц-система	
Учебная аудитория	Специализированная мебель (место преподавателя, посадочные места для студентов) Материально-техническое оснащение: Доска настенная раскрывающаяся, электронная печатная доска Panasonic UB-5815, мультимедиа-проектор NEC V230X, экран настенный для мультимедиа-проектора, программно-технический комплекс на 20 учебных мест по направлению "Инфокоммуникационные технологии и системы связи" с функцией удаленного дистанционного управления и контроля, моноблоки Dell Inspirion 3227(Intel Core i3-713U 2.7Ghz/4096Mb/1000Gb/23.8) с беспроводной клавиатурой и мышью, ПЭВМ преподавателя Intel Core i7, высокопрецизионный аттенюатор R&S, генератор ВЧ-сигналов IFR 2023 A Aerofiex/IFR, генератор сигналов GFC-3015, генератор Agilent 33220A, генератор сигналов НЧ Г3-121, измеритель фликера ,колебаний напряжения и гармонических состав.тока ИФГ20,1, испытательный генератор колебаний напряжения измен.частоты гармоник напряжения .ИГУ, измеритель проходной мощности NRT-Z44, измеритель L,C,R цифровой Е7-12, испытательный генератор наносек импульсн полей, ИГН-2.1, испытательный генератор импульсного магнитного поля ИГИ 1,1, испытательный генератор кондуктивных помех в полосе частот 0-150кГц ИГВ 16,1, испытательный генератор микросекундных импульсных помех большой энергии 1/50мкс, испытательный генератор микросекундных импульсных помех большой энергии6,5/700мкс, испытательный генератор наносекундных импульсных помех ИГН4,1м, испытательный генератор	LibreOffice 6.0.1.1 Интернет броузер (IE, MF или другой) Sumatra pdf WireShark 3.3.3 Kleopatra, версия Gpg4win-3.1.15 Code::Blocks 17.12 Far Manager 3.0.5151 GostCrypt 1.3.1 OpenVPN 11.15.0.0 Oracle VM VirtualBox 6.1.8

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	тока промышленной частоты ИГП 1,1 с индукционной катушкой ИК 1,1, испытательный генератор электростатических разрядов ИГЭ 15,2, испытательный генератор ИГЭ 8.2, испытательный генератор динамических изменений напряжения ИГД 8,1м, испытательный генератор колебательных затухающих помех ИГС 1,1, прибор для измерения показателей качества электр. энергии "ПРОРЫВ-КЭ, источник питания GPS-183OD, линейные источники питания GPS-3030DD, осциллограф 2-х канальный GOS-620, осциллограф Le Croy WaveJet WJ322, серверы Kraftway Express ISP ES12, серверы Kraftway Express LSP модель ES12, сервер Kraftway Express 200 модель EDL12, коммутатор Cisco Catalist 2960 24порта, коммутатор Cisco Catalist 3560 24-10/100/1000-4SFP, мини АТС Cisco 2851, дисковое хранилище Promise VTrak M500i, переключатель KVM switch DMK-580-15 на 8 устройств, аппаратный файервол ASA 5510, модуль Cisco для подключ. аналоговых телефонов, ИБП APC Smart UPS XL 2200VA RM 3U 230V, ИБП Smart-UPS 3000 XL RM, усилитель мощности BSA 0101-7.5 с опцией USB и набором кабелей, беспроводная точка доступа Zyxel G-3000EE, устройство связи - развязки УСРН 20,1, устройство связи-развязки УСР М2Н-10,1, устройство связи-развязки УСРМ 20,1, устройство связи-развязки УСРН 25,3, устройство связи-развязки-УСР М2С-5,1, эквивалент сети ENV 216, емкостные клещи ЕК-4, лабораторный комплекс для измерения напряженности, лабораторная установка "Исследов. характеристик направлен. симметричного вибратора, лаб. установка "Исследов. характеристик напр. и диапазонных свойств телев. антенн, лаб. установка "Исследование входного сопрот. и диаграммы напр. антенны, лабораторная установка "Исследование линейной антенной решетки спир. излучателей,	

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	лабораторная установка "Исследование рупорных антенн", лабораторная установка "Исследование зеркальной параболической антенны", кондиционер сплит система, монитор LED Iiyama ProLite B1906S, монитор LED Samsung S23B370B, мониторы View Sonic, клавиатуры, принтер HP Laser Jet 1022n A4 1200,тестер Master 890B+	
Помещение для самостоятельной работы (компьютерный класс библиотеки)	Материально-техническое оснащение: 17 компьютеров, объединенных в сеть, с выходом в Интернет и обеспечением доступа в электронную информационно-образовательную среду МИЭТ	Операционная система Microsoft Windows от 7 версии и выше, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Crome); Acrobat reader DC

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции **ПК-3.ОБИ** «Способен осуществлять оценку соответствия продуктов информационной технологии требованиям обеспечения безопасности информации».

Фонд оценочных средств представлен отдельным документом и размещен в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/**.**

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Особенности организации процесса обучения

В рамках изучения дисциплины учащиеся должны выполнить индивидуальный проект. Индивидуальный проект выполняется в рамках СРС 4-го модуля обучения. Задание на выполнение индивидуальных проектов выдается учащимся не позднее 11-ой недели обучения. Примерные тематики индивидуальных проектов, требования к отчетным материалам индивидуального проекта, рекомендуемая литература и другие

источники информации для выполнения индивидуального проекта представлены в методических рекомендациях по выполнению индивидуального проекта.

Методические рекомендации по выполнению индивидуального проекта представлены отдельным документом и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система. Баллами оцениваются выполнение каждого контрольного мероприятия в семестре.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (в сумме 40 баллов), выполнение индивидуального проекта (до 30 баллов) и зачет (30 баллов).

В течении семестра контрольные мероприятия (в виде опроса и проверки результатов онлайн тестов) осуществляются на практических занятиях (всего 8 практических занятии). За контрольное мероприятие в рамках практического занятия учащийся может получить от 0 до 5 баллов. Контрольным мероприятием в течении семестра является защита индивидуального проекта. По результатам выполнения и защиты индивидуального проекта учащийся может получить от 0 до 30 баллов. Дополнительные балы выставляются при получении зачета, от 0 до 30 баллов.

По сумме баллов выставляется итоговая оценка. Структура и график контрольных мероприятий доступен в ОРИОКС// URL: http://orioks.miet.ru/.

РАЗРАБОТЧИК:

Доцент кафедры Телекоммуникационные системы, к.т.н. _____/А.В. Шарамок/

Рабочая программа дисциплины «Обеспечение безопасности информационных систем» по направлению подготовки 27.04.08 «Управление интеллектуальной собственностью», направленности (профилю) «Правовое обеспечение управления интеллектуальной собственностью» разработана на кафедре ТКС и утверждена на заседании кафедры 22.02. 2024 года, протокол № 8

Заведующий кафедрой ТКС /А.А. Бахтин /

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа согласована с Институтом ВП СГН

Директор Института ВП СГН /Л.В. Бертовский/

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества

Начальник АНОК /И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ

Директор библиотеки /Т.П.Филиппова /