Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

КАФЕДРА ФИНАНСОВОГО МОНИТОРИНГА

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-2/1

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

СПЕЦИАЛЬНАЯ ПОДГОТОВКА

Направление подготовки (специальность) — [1] 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/ В	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
5	3	108	0	64	0		44	0	3
Итого	3	108	0	64	0	0	44	0	

АННОТАЦИЯ

Учебная дисциплина формирует у студентов базовые навыки анализа текущего состояния защищенности информационной системы, моделирования процессов протекающих в информационной системе, в том числе процессов циркуляции информации в технических средствах передачи и обработки информации. Кроме того, данная учебная дисциплина формирует у студентов навыки анализа пользователей информационной системы, что позволяет строить модели нарушителя состояния режима конфиденциальности и защиты информации.

Прежде чем рассматривать основные составляющие информационной безопасности и разрабатывать стратегию обеспечения безопасности информации, важно знать степень конфиденциальности обрабатываемой информации, принадлежность организации (ведомственная или коммерческая), а также состав технических средств, предназначенных для обработки такой информации. Данный анализ и определение состава исходных данных необходим для выработки стратегии обеспечения информационной безопасности, так как основные и ключевые требования по защите информации предъявляются государственными органами, контролирующими деятельность в области защиты информации.

По результатам анализа исходных данных строятся модели угроз и нарушителя информационной безопасности, после чего разрабатывается стратегия обеспечения информационной безопасности.

На основании утвержденной стратегии, а также моделей угроз и нарушителя информационной безопасности, принимаются меры по обеспечению безопасности информации с точки зрения системного подхода.

В курсе рассматриваются основные методы моделирования и анализа как направления деятельности в целом, так и применительно конкретно к процессам, связанным с обеспечением безопасности информации. Вместе с тем, в курсе рассматриваются основные положения теории организации, теории управления и организационного поведения (с психологической и социологической точки зрения), так как одним из основных направлений деятельности по защите информации является формирование у исполнителей (работников) высокого уровня персональной ответственности при работе с конфиденциальной (защищаемой) информацией, а также построение и анализ моделей нарушителя и расследование инцидентов информационной безопасности.

В рамках данной дисциплины студенты слушают онлайн-курс «Введение в цифровой инжиниринг». Целью курса «Введение в цифровой инжиниринг» является изучение применения основных информационных технологий в условиях цифровизации промышленности.

В рамках курса рассматриваются такие понятия как сложный инженерный объект, жизненный цикл, цифровые модели и цифровые двойники, даются рекомендации и примеры использования современных технологий цифрового проектирования сложных инженерных объектов.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью изучения дисциплины является формирование у студентов практических навыков анализа состояния защищенности информационной системы, моделирования процессов, протекающих в информационной системе, и построение моделей нарушителя режима конфиденциальности и защиты информации, в том числе процессов циркуляции информации в

технических средствах передачи, обработки и информации для выработки стратегии информационной безопасности на объекте информатизации. Вместе с тем, целью данной учебной дисциплины является формирование у студентов практических навыков анализа пользователей информационной системы с точки зрения организационного поведения и криминологии.

Задачами курса является получение студентами знаний об основных методах моделирования и анализа как направлениях деятельности в целом, так и применительно конкретно к процессам, связанным с обеспечением безопасности информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина опирается на компетенции, знания и навыки, полученные студентами при изучении дисциплин «Информатика (информационные технологии в правоохранительной деятельности)», «Теория информационной безопасности и методологии защиты информации», «Организационная защита информации», «Введение в специальность».

В свою очередь, знание дисциплины «Специальная подготовка» необходимо при изучении таких дисциплин, как:

Инженерно-техническая защита информации;

Технологии защищенного документооборота;

Программно-аппаратная защита информации;

Информационное право;

Специальные информационные технологии в правоохранительной деятельности;

Криптографические методы защиты информации;

Информационно-аналитическое обеспечение правоохранительной деятельности, при прохождении производственной практики (НИР), а также для подготовки выпускной квалификационной работы (ВКР).

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
аналитический			
Получение и обработка	Информационные технологии и	ПК-6 [1] - Способен формировать и	З-ПК-6[1] - знать основные

поступающей информации; анализ и отбор данных и сведений для формирования информационных ресурсов; обработка акустических и видеозаписей, фотоматериалов с целью получения информации, необходимой для формирования ресурсов и оперативного реагирования; формирование автоматизированных, в том числе справочных, оперативно-розыскных, криминалистических учетов; осуществление информационного и оперативно-аналитического поиска; осуществление оперативно-розыскного анализа, идентификации, диагностики и прогнозирования, криминалистической диагностики; информационно-аналитическое обеспечение оперативно-розыскных мероприятий и следственных действий; информационно-психологическое обеспечение оперативно-розыскных мероприятий и	системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства	поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы *Основание:* Профессиональный стандарт: 06.011	информационно-поисковые и логико-аналитические системы и принципы работы с ними, а также теоретические основы баз данных, структуру баз данных, системы управления базами данных для информационных систем различного назначения, архитектуру баз данных, физические и логические уровни представления данных, основы моделей данных, основы проектирования баз данных ; У-ПК-6[1] - уметь формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические; В-ПК-6[1] - владеть принципами разработки и создания автоматизированных баз и банков данных, а также принципами их использования

следственных действий; противодействие деструктивным и негативным информационно-психологическим воздействиям.	ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		
Получение и обработка поступающей информации; анализ и отбор данных и сведений для формирования информационных ресурсов; обработка акустических и видеозаписей, фотоматериалов с целью получения информации, необходимой для формирования ресурсов и оперативного реагирования; формирование автоматизированных, в том числе справочных, оперативно-розыскных, криминалистических учетов; осуществление информационного и оперативно-аналитического поиска; осуществление оперативно-розыскного анализа,	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы	ПК-8 [1] - Способен применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование *Основание:* Профессиональный стандарт: 06.022	З-ПК-8[1] - знать ключевые методы аналитической разведки, методику проведения оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования ; У-ПК-8[1] - уметь применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; В-ПК-8[1] - владеть навыками определения необходимых механизмов для проведения аналитической разведки, осуществления оперативно-аналитического

идентификации, диагностики и прогнозирования, криминалистической диагностики; информационно-аналитическое обеспечение оперативно-розыскных мероприятий и следственных действий; информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий; противодействие деструктивным и негативным информационно-психологическим воздействиям.	управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования с учетом задач профессиональной деятельности
правоохранительный			
Обеспечение законности и правопорядка; предупреждение, выявление, пресечение, участие в раскрытии преступлений и иных правонарушений; информационно-аналитическое и информационно-психологическое обеспечение оперативно-	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного	ПК-10 [1] - Способен участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и	З-ПК-10[1] - знать основы уголовного, уголовно-процессуального права, криминалистики, криминологии ; У-ПК-10[1] - уметь оказывать содействие выявлению, предупреждению, пресечению, раскрытию и расследованию преступлений в

розыскных мероприятий и следственных действий.	уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового	эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений *Основание:* Анализ опыта: Выполнение деятельности в области выявления, предупреждения, пресечения, раскрытия и расследования преступлений.	качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений; В-ПК-10[1] - владеть навыками получения информации, ее анализа, оценки и использования в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений

	мониторинга в субъектах первичного финансового мониторинга.		
организационно-управленческий			
Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов; разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности; организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач.	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-	ПК-11 [1] - Способен осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов *Основание:* Профессиональный стандарт: 06.031	З-ПК-11[1] - знать основные нормативно-правовые акты и основы организационной деятельности в области получения, накопления, обработки, анализа, использования информации и защиты объектов информатизации, информационных технологий и ресурсов основы организационной деятелньос ; У-ПК-11[1] - уметь осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов; В-ПК-11[1] - владеть навыками осуществления организационно-правового обеспечения деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации,

	аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		информационных технологий и ресурсов
Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов; разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности; организация работы малых групп и коллективов исполнителей,	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в	ПК-12 [1] - Способен планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов, принимать управленческие решения *Основание:* Профессиональный стандарт: 08.021	З-ПК-12[1] - знать основные принципы и методы управления персоналом, принципы и методы принятия и реализации управленческих решений в сфере профессиональной деятельности ; У-ПК-12[1] - уметь планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов, принимать управленческие решения; В-ПК-12[1] - владеть методологией управления персоналом в сфере профессиональной

сформированных для решения конкретных профессиональных задач в сфере финансового мониторинга.	правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		деятельности

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за	Использование воспитательного потенциала дисциплин профессионального модуля для формирования у студентов

	профессиональный выбор, профессиональное развитие и профессиональные решения (В18)	ответственности за свое профессиональное развитие посредством выбора студентами индивидуальных образовательных траекторий, организации системы общения между всеми участниками образовательного процесса, в том числе с использованием новых информационных технологий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры финансовой безопасности (В44)	1.Использование воспитательного потенциала дисциплин профессионального модуля для формирование базовых навыков финансовой безопасности через изучение типологий финансовых махинаций, освоение механизмов обеспечения кибербезопасности в кредитно-финансовой сфере в соответствии с нормативными документами ЦБ РФ, изучение рисков и угроз в рамках процедур кредитования, инвестирования и других механизмов экономической деятельности. 2.Использование воспитательного потенциала дисциплин профессионального модуля для развития коммуникативных компетенций, навыков делового общения, работы в гибких командах в условиях быстроменяющихся внешних факторов за счет изучения учащимися возможностей, методов получения информации, ее обработки и принятии решения в условиях оценки многофакторных ситуаций, решения кейсов в области межличностной коммуникации и делового общения. 3.Использование воспитательного потенциала дисциплин профессионального модуля для формирования нравственных и правовых норм.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ориентации на неукоснительное соблюдение нравственных и правовых норм в профессиональной деятельности (В45)	1.Использование воспитательного потенциала дисциплин профессионального модуля для формирование базовых навыков финансовой безопасности через изучение типологий финансовых махинаций, освоение механизмов обеспечения кибербезопасности в кредитно-финансовой сфере в

		соответствии с нормативными документами ЦБ РФ, изучение рисков и угроз в рамках процедур кредитования, инвестирования и других механизмов экономической деятельности. 2.Использование воспитательного потенциала дисциплин профессионального модуля для развития коммуникативных компетенций, навыков делового общения, работы в гибких командах в условиях быстроменяющихся внешних факторов за счет изучения учащимися возможностей, методов получения информации, ее обработки и принятии решения в условиях оценки многофакторных ситуаций, решения кейсов в области межличностной коммуникации и делового общения. 3.Использование воспитательного потенциала дисциплин профессионального модуля для формирования нравственных и правовых норм.

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	5 Семестр						
1	Организационные структуры. Построение модели угроз информационной безопасности	1-8	0/32/0	Зд-2 (2),Зд-4 (2),Зд-6 (2)	25	КИ-8	З-ПК-6, У-ПК-6, В-ПК-6, З-ПК-8, У-ПК-8, В-ПК-8, З-ПК-10, У-ПК-10, В-ПК-10, З-ПК-11,

							У-ПК-11, В-ПК-11, З-ПК-12, У-ПК-12, В-ПК-12
2	Организационные мероприятия по обеспечению информационной безопасности	9-16	0/32/0	Зд-10 (2),Зд-12 (2),Зд-14 (2),к.р-15 (5)	20	КИ-16	З-ПК-6, У-ПК-6, В-ПК-6, З-ПК-8, У-ПК-8, В-ПК-8, З-ПК-10, У-ПК-10, В-ПК-10, З-ПК-11, У-ПК-11, В-ПК-11, З-ПК-12, У-ПК-12, В-ПК-12
3	Третий раздел: онлайн-курс «Введение в цифровой инжиниринг»	8-16	0/0/0	Т-16 (5)	5	Т-16	З-ПК-6, У-ПК-6, В-ПК-6, З-ПК-8, У-ПК-8, В-ПК-8, З-ПК-10, У-ПК-10, В-ПК-10, З-ПК-11, У-ПК-11, В-ПК-11, З-ПК-12, У-ПК-12, В-ПК-12
	Итого за 5 Семестр		0/64/0		50		
	Контрольные мероприятия за 5 Семестр				50	З	З-ПК-6, У-ПК-6, В-ПК-6, З-ПК-8, У-ПК-8, В-ПК-8, З-ПК-10, У-ПК-10, В-ПК-10, З-ПК-11, У-ПК-11, В-ПК-11, З-ПК-12, У-ПК-12, В-ПК-12

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
Т	Тестирование
КИ	Контроль по итогам
Зд	Задание (задача)
к.р	Контрольная работа
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	5 Семестр	0	64	0
1-8	**Организационные структуры. Построение модели угроз информационной безопасности**	0	32	0
1 - 2	**Организационные структуры** Сущность организации как системы. Сущность структурного подхода к изучению организации. Система управления организацией. Жизненный цикл организации. Организационные коммуникации. Организационные структуры правоохранительных органов и силовых структур.	Всего аудиторных часов		
		0	8	0
		Онлайн		
		0	0	0
3 - 4	**Анализ информации** Анализ информации - Степени конфиденциальности информации; - Качество и свойства информации; - Методы обработки и хранения информации; - Процессы циркуляции информации в системе коммуникаций конкретной организации относительно ее организационно-штатной структуры, в том числе в структурах правоохранительных органов и силовых структурах; - Обеспечение информационной безопасности.	Всего аудиторных часов		
		0	8	0
		Онлайн		
		0	0	0
5 - 6	**Моделирование** Моделирование - Классификация моделей; - Свойства моделей; - Методы моделирования угроз информационной безопасности и построение моделей нарушителя режима конфиденциальности и защиты информации.	Всего аудиторных часов		
		0	8	0
		Онлайн		
		0	0	0
7 - 8	**Угрозы информационной безопасности** Угрозы информационной безопасности - Анализ защищенности информационной системы; - Идентификация угроз по всем направлениям защиты; - Построение модели угроз информационной безопасности.	Всего аудиторных часов		
		0	8	0
		Онлайн		
		0	0	0

9-16	**Организационные мероприятия по обеспечению информационной безопасности**	0	32	0
9 - 10	**Организационные мероприятия, направленные на достижение информационной безопасности** Организационные мероприятия, направленные на достижение информационной безопасности - Государственные органы Российской Федерации, контролирующие деятельность в области режима конфиденциальности и защиты информации. Основные руководящие документы; - Формирование и поддержание персональной ответственности за нарушения в области защиты информации и режима конфиденциальности; - Личность нарушителя режима конфиденциальности и защиты информации; - Построение и анализ модели нарушителя режима конфиденциальности и защиты информации.	Всего аудиторных часов		
		0	8	0
		Онлайн		
		0	0	0
11 - 12	**Организационные мероприятия, направленные на достижение информационной безопасности** - Личность нарушителя режима конфиденциальности и защиты информации; - Построение и анализ модели нарушителя режима конфиденциальности и защиты информации.	Всего аудиторных часов		
		0	8	0
		Онлайн		
		0	0	0
13 - 14	**Организация контроля за обеспечением режима конфиденциальности и защиты информации** Организация контроля за обеспечением режима конфиденциальности и защиты информации - Технические методы и инструменты контроля информационной безопасности; - Методы выявления нарушений режима конфиденциальности и защиты информации.	Всего аудиторных часов		
		0	8	0
		Онлайн		
		0	0	0
15 - 16	**Расследование нарушений режима конфиденциальности и защиты информации** Расследование нарушений режима конфиденциальности и защиты информации - Оперативное реагирование на инцидент информационной безопасности; - Оценка последствий инцидента информационной безопасности; - Привлечение к ответственности нарушителя режима конфиденциальности и защиты информации.	Всего аудиторных часов		
		0	8	0
		Онлайн		
		0	0	0
8-16	**Третий раздел: онлайн-курс «Введение в цифровой инжиниринг»**	0	0	0
8 - 16	**Онлайн-курс «Введение в цифровой инжиниринг»** Тема 1. Введение. Предпосылки Четвертой индустриальной революции. Элементы и технологии индустрии 4.0. Понятие цифровых технологий и цифровой экономики. Информационный продукт как результат цифровой экономики. Основные технологии цифровой трансформации. Сквозные цифровые технологии в материальном производстве, сфере услуг и государственном управлении.	Всего аудиторных часов		
		0	0	0
		Онлайн		
		16	16	0

	Тема 2. Сложный инженерные объект. Понятие сложного инженерного объекта. Иерархия компонент сложных инженерных объектов. Общекультурный подход, функционально-балансовый подход, инженерно-технический подход, подход системного анализа. Примеры, характеристики, существенные черты инженерных объектов. Тема 3. Жизненный цикл сложного инженерного объекта. Понятие жизненного цикла объекта. Этапы жизненного цикла сложного инженерного объекта. Понятия ввода в эксплуатацию, нормальной эксплуатации, вывода из эксплуатации. Нормативные требования, связи между этапами жизненного цикла. Возможности использования современных информационных технологий. Жизненный цикл сложного инженерного объекта, технического изделия и продукта. Аналогии и особенности. Современный цифровой инструментарий управления жизненным циклом. Понятие PLM-подхода. Тема 4. Цифровые модели и двойники. Понятия цифровой модели. История и современные подходы, технология BIM-моделирования. MULTI-D моделирование. Разнородность цифрового инструментария. Разнородность данных и процессов при описании одного объекта. Накопление и онлайн-доступность данных за всю историю объекта. Современная информационная модель как предшественник цифрового двойника СИО. Понятие цифрового двойника, связь с жизненным циклом инженерного объекта. Цифровое документирование жизненного цикла объекта. Основные цифровые технологии. Цифровые двойники и модели для сложных бизнес-процессов и объектов. Проблемы системной работы с цифровой информацией. Тема 5. Цифровое проектирование и конструирование. Понятие цифрового проектирования и конструирования. Базовые подходы, понятия, навыки и инструменты. Классификация цифровых инструментов проектирования и конструирования. Атрибуты и атрибутивная информация. Иерархия уровней моделирования. Инструменты и техники цифрового моделирования инженерно-физических процессов. Цифровая модель инженерной деятельности, инструментарий и цифровой продукт. Организация работы проектной группы. Проблемы и технология совместимости данных, обмена данными и сохранности данных в цифровом проектировании. Тема 6. Цифровое производство. Общие принципы организации производственной деятельности в цифровой экономике. Информационные процессы в технологической сфере. "Умное" оборудование. Бесшовная интеграция цифровой проектной деятельности и "умного производства". Кастомизация продуктов при цифровом производстве. Классификация типов цифровых			

	производств в отраслях индустрии. Современные цифровые производственные технологии. Аддитивные технологии. Эффективность цифрового производства. Тема 7. Технологии промышленного интернета вещей. Введение в проектирование и реализацию систем IoT. Понятийный аппарат Интернета вещей. Архитектура, технологии и приложения промышленного интернета вещей в индустрии и бизнесе. Рынок производителей и пользователей решений IoT. Открытые проблемы в разработке, реализации и эксплуатации систем «интернета вещей». Перспективы технологии IoT. Тема 8. Виртуальная и дополненная реальности в промышленности. Принципы и методы цифровых 3D моделирования, визуализации и анимации. Технологии построения виртуальной реальности со стыковкой проектных данных и отображения реальных объектов. Понятие дополненной реальности и технологии ее построения. Приложения виртуальной и дополненной реальности в индустрии и бизнесе. Тема 9. Системы управления проектами. Понятие системной инженерии. Проектный и процессный подходы. Цифровые системы управления проектами. Мировые и российские продукты. Управление ресурсами, цифровые ERP-системы. Связь изучаемого курса с типовой иерархией задач системного инженера. Тема 10. Заключение. Принципы гибкой интеграции основных видов деятельности цифровой инженерии в индустрии и экономики. Эффекты цифровой трансформации инженерной деятельности в сферах материального производства, услуг и государственного управления. Формирование сквозной цифровой среды инженерной деятельности. Перспективы перестройки рынка труда в инженерной сфере в ходе цифровой трансформации.			

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	5 Семестр

1 - 2	**Тема 1.** Построение организационной структуры и анализ существующей организационной структуры в совокупности с коммуникационной системой организации.
3 - 4	**Тема 2.** Анализ информации в системе коммуникаций конкретной организации и определение класса защищенности информационной системы.
5 - 6	**Тема 3.** Построение модели угроз информационной безопасности информационной системы
7 - 8	**Тема 4.** Качественный анализ информационной системы на предмет идентификации угроз информационной безопасности
9 - 10	**Тема 5.** Построение модели нарушителя режима конфиденциальности и защиты информации
11 - 12	**Тема 6.** Оценка уровня зрелости процессов информационной безопасности организации
13 - 14	**Тема 7.** Организация контроля за обеспечением режима конфиденциальности и защиты информации
15 - 16	**Тема 8.** Расследование нарушений режима конфиденциальности и защиты информации

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Учебно-материальная база курса включает нормативные документы высшего профессионального образования, нормативные документы в области информации, информатизации и защиты информации, сборники лекций и другую учебно-методическую литературу, специализированные компьютерные классы и технические средства обучения.

Современные образовательные технологии при преподавании дисциплины напрямую связаны с гуманизацией образования, способствующей самоактуализации и самореализации личности. В данном курсе применяются следующие образовательные технологии:

- беседа — форма организации занятия, при которой ограниченная дидактическая единица передается в интерактивном информационном режиме для достижения локальных целей воспитания и развития. В зависимости от чередования направлений информационных потоков во времени, различается несколько разновидностей беседы: с параллельным контролем, с предконтролем, с постконтролем и другие;

- исследовательские методы в обучении - дает возможность студентам самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения.

- практическое занятие - метод репродуктивного обучения, обеспечивающий связь теории и практики, содействующий выработке у студентов умений и навыков применения знаний, полученных на лекции и в ходе самостоятельной работы;

- система задач — совокупность заданий к блоку уроков по изучаемой теме, удовлетворяющая требованиям: полнота, наличие ключевых задач, связность, возрастание трудности в каждом уровне, целевая ориентация, целевая достаточность, психологическая комфортность;

- проблемное обучение - создание в учебной деятельности проблемных ситуаций и организация активной самостоятельной деятельности учащихся по их разрешению, в результате

чего происходит творческое овладение знаниями, умениями, навыками, развиваются мыслительные способности;

- тестирование - контроль знаний с помощью тестов, которые состоят из условий (вопросов) и вариантов ответов для выбора (самостоятельная работа студентов). Тестирование применяется как форма контроля знаний студентов по всем темам, предусмотренным для изучения, как в рамках самостоятельной работы студентов, так и на практических занятиях. Тесты состоят из условий и вариантов ответов для выбора.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-10	З-ПК-10	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	У-ПК-10	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	В-ПК-10	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
ПК-11	З-ПК-11	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	У-ПК-11	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	В-ПК-11	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
ПК-12	З-ПК-12	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	У-ПК-12	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	В-ПК-12	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
ПК-6	З-ПК-6	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	У-ПК-6	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	В-ПК-6	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
ПК-8	З-ПК-8	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	У-ПК-8	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	В-ПК-8	З, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.</td></tr>
</table>

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Т 83 Защита информации на предприятии : учебное пособие, Петровский М. В., Тумбинская М. В., Санкт-Петербург: Лань, 2020

2. ЭИ П 84 Информационная безопасность и защита информации : учебник для вузов, Прохорова О. В., Санкт-Петербург: Лань, 2023

3. ЭИ Т 83 Комплексное обеспечение информационной безопасности на предприятии : учебник для вузов, Петровский М. В., Тумбинская М. В., Санкт-Петербург: Лань, 2022

4. ЭИ Ж91 Основы противодействия инсайдерским угрозам : учебное пособие для вузов, Журин С.И., Москва: НИЯУ МИФИ, 2013

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

1. офисные технологии (MS Word, MS Excel, MS PowerPoint, MS Access)

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. на национальной платформе «Открытое образование»: (https://openedu.ru/course/mephi/mephi_digital_engineering/)

2. Научная электронная библиотека «КиберЛенинка» (http://cyberleninka.ru)

3. ИНТУИТ Национальный открытый университет (https://intuit.ru/)

4. Образовательный портал GeekBrains (https://gb.ru)

5. Обучающие статьи о Computer Science и использование классических алгоритмов и структур данных в реше (https://tproger.ru/tag/algorithms/)

https://online.mephi.ru/

http://library.mephi.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. Лаборатория системного анализа

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

При изучении дисциплины необходимо акцентировать внимание как на основных положениях теоретической части программы, так и на выполнении практических и лабораторных заданий.

Следует руководствоваться материалами аудиторных занятий, примерами, предложенными преподавателем, а также информацией, имеющейся в рекомендованной литературе.

Целесообразно прорабатывать самостоятельно материалы каждого аудиторного занятия, чтобы прояснить для себя связь между темами программы, четко представлять особенности методов и технологий, рассмотренных в темах.

Важно всякий раз сопоставлять преимущества и недостатки, ограничения, которые вытекают из рассматриваемых методов при применении каждого из методов и подходов к решению практических задач.

Нужно учиться объяснять ход решения практических задач, используя материалы рассмотренных примеров.

При изучении дисциплины следует уделять внимание тщательному анализу комплекса примеров, имеющихся в материалах по дисциплине, и применять сделанные выводы при выборе задания для самостоятельной работы из числа предложенных преподавателем в виде тем индивидуальной проработки в рамках программы по дисциплине.

Проработка выбранной темы способствует ориентации студента при решении практических задач, и в дальнейшей самостоятельной работе по специальности.

Типовыми заданиями являются блоки вопросов к основным разделам дисциплины. Рекомендуется при работе по освоению материала руководствоваться рекомендуемой литературой по дисциплине.

При освоении дополнительных материалов следует концентрировать внимание на возможных ошибках при использовании теоретического материала в ходе решения практических задач.

Для выполнения самостоятельной работы следует использовать материал, изложенный в учебниках, методические указания, основную и дополнительную литературу по курсу, а также следует пользоваться интрасетью кафедры, средствами портала университета.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебная программа и календарно-тематический план позволяют ориентировать студентов на системное изучение материалов дисциплины.

Основными видами учебных занятий в процессе преподавания дисциплины являются семинарские (практические) занятия.

Целью семинарских занятий является закрепление теоретических знаний, а также выработка у них самостоятельного творческого мышления, приобретение и развитие студентами навыков публичного выступления и ведения дискуссии, применения теоретических знаний на практике.

Семинарское занятие может быть проведено в форме:

1. Опроса;
2. Диспута;
3. Викторины;
4. Круглого стола.

Возможно и сочетание различных форм проведения семинарских занятий. Педагогическая практика не исключает также и реализацию других подходов в данной области.

Наиболее распространенным является проведение семинара-опроса, в ходе которого студентами осуществляется творческое обсуждение ответов на вопросы, заданные преподавателем, взаимный обмен мнениями обучающихся с последующим подведением итогов преподавателем по каждому учебному вопросу (подвопросу). В результате этого у студентов вырабатывается единое мнение, систематизируются знания, полученные в ходе лекции и самостоятельной работы.

Семинар-диспут предполагает дискуссию, коллективное обсуждение вопросов занятия, особенно проблемных, в целях их объективного разрешения. Такой семинар способствует не только глубокому усвоению учебного материала, но и формированию навыков аргументированного ведения дискуссии, отстаивания собственной точки зрения, что очень важно для будущего специалиста.

Проведение семинара-диспута требует наличия у обучающихся определенной базовой подготовки. В основном выносимые на семинар-диспут вопросы должны носить проблемный и дискуссионный характер.

Одной из разновидностей семинара-диспута является реферативная форма. По важнейшим вопросам сформулированной преподавателем проблемы назначенные студенты готовят рефераты (доклады). В содержании рефератов должны отражаться различные точки зрения на исследуемые вопросы.

На семинаре-викторине преподавателем осуществляется постановка ряда вопросов по тематике занятий, которые требуют конкретных ответов в устной или письменной форме. Оценка ответов производится на конкурсной основе. При проведении данной разновидности семинара на базе учебной группы заранее необходимо создать 2-3 соперничающих команды. Каждая команда выбирает лидера, который и осуществляет руководство коллективом команды в ходе занятия. Для оценки ответов команд из числа наиболее подготовленных студентов можно сформировать жюри. Ход викторины и её результаты постоянно отражаются на классной доске.

Проведение семинара в виде круглого стола подразумевает выступление студентов с актуальными сообщениями по важным разделам темы семинара и последующими ответами докладчиков на поставленные вопросы. Определяются несколько студентов, которые готовят проблемное сообщение. Остальные студенты задают им вопросы. При подготовке этой разновидности семинара преподавателю целесообразно заранее подготовить несколько студентов с вопросами, способными вызвать оживленную и интересную дискуссию по рассматриваемой теме.

Во время выступления студентов преподаватель контролирует содержание, последовательность, обоснованность и логичность их ответов, делает необходимые пометки. Не рекомендуется прерывать выступления отвечающих, если только они не допускают грубых ошибок или не уводят обсуждение вопроса в сторону. К исправлению допущенных студентами во время выступления ошибок преподавателю целесообразно сначала привлекать других обучающихся, а затем, подводя итог, сделать это самому. Если докладчик не укладывается в отведенный для выступления временной интервал, то преподавателю следует тактично его прервать и предложить кратко изложить основные моменты из неосвещенного ещё материала, либо отказаться от дальнейшего заслушивания.

На каждом семинарском (практическом) занятии преподаватель обязан обеспечивать выполнение контролирующей функции данного вида занятий. Основные цели контроля на семинарах - определение степени готовности учебной группы, ориентирование студентов на систематическую работу по овладению предметом, усиление обратной связи преподавателя с обучающимися, выявление отношения к дисциплине, внесение при необходимости корректив в содержание и методику обучения.

От преподавателя требуется сформировать у студентов правильное понимание значения самостоятельной работы, обучить их наиболее эффективным приемам самостоятельного поиска и творческого осмысления приобретенных знаний, привить стремление к самообразованию.

Изучение курса заканчивается итоговой аттестацией. Перед итоговй аттестацией преподаватель проводит консультацию. На консультации преподаватель отвечает на вопросы студентов по темам, которые оказались недостаточно освоены ими в процессе самостоятельной работы. Итоговый контроль проводится в форме ответов на вопросы билетов по всему материалу курса.

Автор(ы):

Рычков Вадим Александрович