

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 № 545-1

от 30.08.2021 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	44	0	

## АННОТАЦИЯ

Учебная дисциплина «Специальная подготовка» 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 «Специальная подготовка» 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 безопасностью информации.

## **2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО**

Дисциплина «Специальная подготовка» относится к базовым дисциплинам общепрофессионального модуля Блока С1 «Дисциплины» образовательной программы специалитета «Информационно-аналитическое обеспечение правоохранительной деятельности» по направлению 10.05.05 «Безопасность информационных технологий в правоохранительной сфере».

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 соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	Объект или область знания	Код и наименование профессиональной компетенции;	Код и наименование индикатора достижения
--	---------------------------	--	--

		Основание (профессиональный стандарт-ПС, анализ опыта)	профессиональной компетенции
<p>Обеспечение законности и правопорядка; предупреждение, выявление, пресечение, участие в раскрытии преступлений и иных правонарушений; информационно-аналитическое и информационно-психологическое обеспечение оперативно-розыскных мероприятий и следственных действий.</p>	<p>правоохранительный</p> <p>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</p>	<p>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 эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений</p> <p><i>Основание:</i> Анализ опыта: Выполнение деятельности в области выявления, предупреждения, пресечения, раскрытия и расследования преступлений;</p>	<p>3-ПК-10[1] - знать основы уголовного, уголовно-процессуального права, криминастики, криминологии ; У-ПК-10[1] - уметь оказывать содействие выявлению, предупреждению, пресечению, раскрытию и расследованию преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений;</p> <p>В-ПК-10[1] - владеть навыками получения информации, ее анализа, оценки и использования в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений</p>

	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.		
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	организационно-управленческий	ПК-11 [1] - Способен осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов  <i>Основание:</i> Профессиональный стандарт: 06.031	3-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 деятельности ; У-ПК-11[1] - уметь осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу,



<p>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 в сфере финансового мониторинга.</p>	<p>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 ПОД/ФТ; системы государственного финансового</p>	<p>осуществлять контроль и учет ее результатов, принимать управленческие решения</p> <p><i>Основание:</i> Профессиональный стандарт: 08.021</p>	<p>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 деятельности</p>
---	--	---	---

	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, идентификации, диагностики и	аналитический 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,	ПК-6 [1] - Способен формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы  <i>Основание:</i> Профессиональный стандарт: 06.011	3-ПК-6[1] - знать основные 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

<p>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.</p>	<p>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.</p>		<p>принципами разработки и создания автоматизированных баз и банков данных, а также принципами их использования</p>
<p>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</p>	<p>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,</p>	<p>ПК-8 [1] - Способен применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование</p> <p><i>Основание:</i> Профессиональный стандарт: 06.022</p>	<p>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</p>

<p>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 следственных действий; противодействие деструктивным и негативным информационно-психологическим воздействиям.</p>	<p>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 мониторинга в</p>		<p>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 поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования с учетом задач профессиональной деятельности</p>
---	--	--	---

	субъектах первичного финансового мониторинга.		
--	---	--	--

#### 4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (В18)	Использование воспитательного потенциала дисциплин профессионального модуля для формирования у студентов 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 принятия решения в условиях оценки многофакторных ситуаций, решения кейсов в области межличностной коммуникации и делового общения. 3.Использование воспитательного потенциала

Профессиональное воспитание	Создание условий, обеспечивающих, формирование ориентации на неукоснительное соблюдение нравственных и правовых норм в профессиональной деятельности (В45)	<p>дисциплин профессионального модуля для формирования нравственных и правовых норм.</p> <p>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 принятия 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.</p>
-----------------------------	--	--

## 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
<i>5 Семестр</i>							
1	Организационные структуры. Построение модели угроз информационной безопасности	1-8		Зд-2 (2), Зд-4 (2), Зд-6 (2)	25	КИ-8	З-ПК-10, У-ПК-10, В-ПК-10, З-ПК-11, У-ПК-11, В-ПК-11, З-ПК-6, У-ПК-6, В-ПК-6, З-ПК-8, У-ПК-8, В-ПК-8, З-ПК-1.1, У-ПК-1.1, В-ПК-1.1, З-ПК-1.3, У-ПК-1.3, В-ПК-

							1.3, 3-ПК- 12, У- ПК- 12, В- ПК- 12
2	Организационные мероприятия по обеспечению информационной безопасности	9-16		Зд-10 (2),Зд- 12 (2),Зд- 14 (2),к.р- 15 (5)	20	КИ-16	3-ПК- 10, У- ПК- 10, В- ПК- 10, 3-ПК- 11, У- ПК- 11, В- ПК- 11, 3-ПК- 6, У- ПК-6, В- ПК-6, 3-ПК- 8, У- ПК-8, В- ПК-8, 3-ПК- 1.1, У- ПК- 1.1, В- ПК- 1.1, 3-ПК- 1.3, У- ПК- 1.3, В- ПК-

							1.3, 3-ПК- 12, У- ПК- 12, В- ПК- 12	
3	Третий раздел: онлайн-курс «Введение цифровой инжиниринг»	в	8-16		T-16 (5)	5	T-16	3-ПК- 10, У- ПК- 10, В- ПК- 10, 3-ПК- 11, У- ПК- 11, В- ПК- 11, 3-ПК- 6, У- ПК-6, В- ПК-6, 3-ПК- 8, У- ПК-8, В- ПК-8, 3-ПК- 1.1, У- ПК- 1.1, В- ПК- 1.1, 3-ПК- 1.3, У- ПК- 1.3, В- ПК-

						1.3, 3-ПК- 12, У- ПК- 12, В- ПК- 12
	<i>Итого за 5 Семестр</i>	0/64/0		50		
	<b>Контрольные мероприятия за 5 Семестр</b>			50	3	3-ПК- 10, У- ПК- 10, В- ПК- 10, 3-ПК- 11, У- ПК- 11, В- ПК- 11, 3-ПК- 6, У- ПК-6, В- ПК-6, 3-ПК- 8, У- ПК-8, В- ПК-8, 3-ПК- 1.1, У- ПК- 1.1, 3-ПК- 1.3, У- ПК- 1.3, В- ПК- 1.3, 3-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:

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

## КАЛЕНДАРНЫЙ ПЛАН

Недел и	Темы занятий / Содержание	Лек., час.	Пр./сем. , час.	Лаб., час.
	<i>5 Семестр</i>	0	64	0
1-8	<b>Организационные структуры. Построение модели угроз информационной безопасности</b>		32	
1 - 2	<b>Организационные структуры</b> 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		
			8	
		Онлайн		
3 - 4	<b>Анализ информации</b> 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		
			8	
		Онлайн		
5 - 6	<b>Моделирование</b> Моделирование - Классификация моделей; - Свойства моделей;	Всего аудиторных часов		
			8	
		Онлайн		

	<ul style="list-style-type: none"> <li>- Методы моделирования угроз информационной безопасности и построение моделей нарушителя режима конфиденциальности и защиты информации.</li> </ul>			
7 - 8	<p><b>Угрозы информационной безопасности</b></p> <p>Угрозы информационной безопасности</p> <ul style="list-style-type: none"> <li>- Анализ защищенности информационной системы;</li> <li>- Идентификация угроз по всем направлениям защиты;</li> <li>- Построение модели угроз информационной безопасности.</li> </ul>	<p>Всего аудиторных часов</p> <p>8</p> <p>Онлайн</p>		
9-16	<b>Организационные мероприятия по обеспечению информационной безопасности</b>		32	
9 - 10	<p><b>Организационные мероприятия, направленные на достижение информационной безопасности</b></p> <p>Организационные мероприятия, направленные на достижение информационной безопасности</p> <ul style="list-style-type: none"> <li>- Государственные органы Российской Федерации, контролирующие деятельность в области режима конфиденциальности и защиты информации. Основные руководящие документы;</li> <li>- Формирование и поддержание персональной ответственности за нарушения в области защиты информации и режима конфиденциальности;</li> <li>- Личность нарушителя режима конфиденциальности и защиты информации;</li> <li>- Построение и анализ модели нарушителя режима конфиденциальности и защиты информации.</li> </ul>	<p>Всего аудиторных часов</p> <p>8</p> <p>Онлайн</p>		
11 - 12	<p><b>Организационные мероприятия, направленные на достижение информационной безопасности</b></p> <ul style="list-style-type: none"> <li>- Личность нарушителя режима конфиденциальности и защиты информации;</li> <li>- Построение и анализ модели нарушителя режима конфиденциальности и защиты информации.</li> </ul>	<p>Всего аудиторных часов</p> <p>8</p> <p>Онлайн</p>		
13 - 14	<p><b>Организация контроля за обеспечением режима конфиденциальности и защиты информации</b></p> <p>Организация контроля за обеспечением режима конфиденциальности и защиты информации</p> <ul style="list-style-type: none"> <li>- Технические методы и инструменты контроля информационной безопасности;</li> <li>- Методы выявления нарушений режима конфиденциальности и защиты информации.</li> </ul>	<p>Всего аудиторных часов</p> <p>8</p> <p>Онлайн</p>		
15 - 16	<p><b>Расследование нарушений режима конфиденциальности и защиты информации</b></p> <p>Расследование нарушений режима конфиденциальности и защиты информации</p> <ul style="list-style-type: none"> <li>- Оперативное реагирование на инцидент информационной безопасности;</li> <li>- Оценка последствий инцидента информационной безопасности;</li> <li>- Привлечение к ответственности нарушителя режима конфиденциальности и защиты информации.</li> </ul>	<p>Всего аудиторных часов</p> <p>8</p> <p>Онлайн</p>		
8-16	<b>Третий раздел: онлайн-курс «Введение в цифровой инжиниринг»</b>			
8 - 16	<b>Онлайн-курс «Введение в цифровой инжиниринг»</b>	Всего аудиторных часов		

	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	Онлайн	16	16
--	---	--------	----	----

	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>		
--	---	--	--

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

<b>Недели</b>	<b>Темы занятий / Содержание</b>
	<i>5 Семестр</i>
1 - 2	<b>Тема 1.</b> Построение организационной структуры и анализ существующей организационной структуры в совокупности с коммуникационной системой организации.
3 - 4	<b>Тема 2.</b> Анализ информации в системе коммуникаций конкретной организации и определение класса защищенности информационной системы.
5 - 6	<b>Тема 3.</b> Построение модели угроз информационной безопасности информационной системы
7 - 8	<b>Тема 4.</b> Качественный анализ информационной системы на предмет идентификации угроз информационной безопасности
9 - 10	<b>Тема 5.</b> Построение модели нарушителя режима конфиденциальности и защиты информации
11 - 12	<b>Тема 6.</b> Оценка уровня зрелости процессов информационной безопасности организации
13 - 14	<b>Тема 7.</b> Организация контроля за обеспечением режима конфиденциальности и защиты информации
15 - 16	<b>Тема 8.</b> 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	3-ПК-12	3, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	У-ПК-12	3, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	В-ПК-12	3, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
ПК-6	3-ПК-6	3, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, к.р-15
	У-ПК-6	3, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	В-ПК-6	3, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
ПК-8	3-ПК-8	3, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, к.р-15
	У-ПК-8	3, КИ-8, КИ-16, Т-16, Зд-2, Зд-4, Зд-6, Зд-10, Зд-12, Зд-14, к.р-15
	В-ПК-8	3, 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:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – «отлично»	A	Оценка «отлично» выставляется студенту, если он глубоко иочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89		B	
75-84		C	
70-74	4 – «хорошо»	D	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе

			на вопрос.
65-69			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.
60-64	3 – «удовлетворительно»	E	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.
Ниже 60	2 – «неудовлетворительно»	F	

Оценочные средства приведены в Приложении.

## **8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

### **ОСНОВНАЯ ЛИТЕРАТУРА:**

1. ЭИ Т 83 Защита информации на предприятии : учебное пособие, Санкт-Петербург: Лань, 2020
2. ЭИ П 84 Информационная безопасность и защита информации : учебник, Санкт-Петербург: Лань, 2020
3. ЭИ Ж91 Основы противодействия инсайдерским угрозам : учебное пособие для вузов, Москва: НИЯУ МИФИ, 2013

### **ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:**

1. ЭИ Т 83 Комплексное обеспечение информационной безопасности на предприятии : учебник, Санкт-Петербург: Лань, 2019

### **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/](https://openedu.ru/course/mephi/mephi_digital_engineering/))

<https://online.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 литературой по дисциплине:

### **ОСНОВНАЯ ЛИТЕРАТУРА:**

1. Экономическая безопасность [Текст] : энциклопедия / рук. работы : А. Г. Шаваев. - М. : Пра-вовое просвещение, 2001. - 512 с. - ISBN 5-93485-004-0.

2. Живетин, В.Б. Риски и безопасность экономических систем (математическое моделирование) [Текст] / В. Б. Живетин. - изд. 4-е, испр. и доп. - Москва : Изд-во Ин-та проблем риска. Т. 8. - [Б. м.], 2008. - 431 с. - (Риски и безопасность человеческой деятельности). - ISBN 978-5-98664-035-8. - ISBN 978-5-903140-32-9.

3. Совершенствование системы экономической безопасности и защиты активов. [Текст] : учеб. пособие / Под ред. В. Ф. Шалаева, В.В. Харитонова. - Москва : НИЯУ МИФИ, 2016. - 167 с. - ISBN 978-5-7262-2326-1.

### **ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:**

Не требуется

### **ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:**

Специальное программное обеспечение не требуется

## **ИНТЕРНЕТ-РЕСУРСЫ:**

1. Книги, статьи, учебные материалы МИФИ (<http://neo-chaos.narod.ru/books.htm>)
2. Каталог образовательных ресурсов (Федерация Интернет образования) (<http://www.catalog.alledu.ru/predmet/econom>)
3. Научная электронная библиотека (<http://www.scholar.ru/>)

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**

Лектору, а также преподавателям, ведущим практические и лабораторные занятия, рекомендуется использовать следующие учебники, учебные пособия, методические и справочные материалы.

В качестве основной литературы:

### **ОСНОВНАЯ ЛИТЕРАТУРА:**

1. Экономическая безопасность [Текст] : энциклопедия / рук. работы : А. Г. Шаваев. - М. : Правовое просвещение, 2001. - 512 с. - ISBN 5-93485-004-0.
2. Живетин, В.Б. Риски и безопасность экономических систем (математическое моделирование) [Текст] / В. Б. Живетин. - изд. 4-е, испр. и доп. - Москва : Изд-во Ин-та проблем риска. Т. 8. - [Б. м.], 2008. - 431 с. - (Риски и безопасность человеческой деятельности). - ISBN 978-5-98664-035-8. - ISBN 978-5-903140-32-9.
3. Совершенствование системы экономической безопасности и защиты активов. [Текст] : учеб. пособие / Под ред. В. Ф. Шалаева, В.В. Харитонова. - Москва : НИЯУ МИФИ, 2016. - 167 с. - ISBN 978-5-7262-2326-1.

В случае необходимости дополнительную информацию по вопросам, затрагиваемым в Программе по дисциплине, можно получить, используя следующие интернет-источники:

1. Книги, статьи, учебные материалы МИФИ (<http://neo-chaos.narod.ru/books.htm>)
2. Каталог образовательных ресурсов (Федерация Интернет образования) (<http://www.catalog.alledu.ru/predmet/econom>)
3. Научная электронная библиотека (<http://www.scholar.ru/>)

### **ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:**

Специального программного обеспечения не требуется.

Важно понимать, что целью изучения дисциплины «Специальная подготовка» 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. При этом основной целью курса также является освоение области научного знания, в рамках которого студенты

изучают состояние экономики, а именно при котором обеспечивается достаточно высокий и устойчивый рост экономических показателей; эффективное удовлетворение экономических потребностей; контроль государства за движением и использованием национальных ресурсов; защита экономических интересов страны на национальном и международном уровнях то есть экономическая безопасность, что является неотъемлемой частью общей стратегии обеспечения безопасности предприятия.

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 экономической и информационной безопасности.

Актуализация знаний студентов проводится в ходе мероприятий текущего контроля, при обсуждении материалов творческих работ.

В результате освоения дисциплины студенты должны:

Знать:

3-1) основные методы и технологии моделирования процессов и анализа состояния и процессов экономической безопасности применительно к конкретной организации;

3-2) жизненный цикл систем и уровни зрелости процессов экономической безопасности;

3-3) методики оценки уровня зрелости процессов экономической безопасности применительно к конкретному объекту;

3-4) основные методы и технологии построения и анализа моделей нарушителя экономической безопасности;

3-5) основные методики расследования нарушений в области экономической безопасности.

Уметь:

У-1) строить модели процессов циркуляции информационных потоков в экономических системах;

У-2) анализировать реальные процессы экономической безопасности и выявлять уязвимости;

У-3) применять основные методики расследования нарушений в части касающейся нарушений процессов и состояний экономической безопасности.

Владеть:

В-1) профессиональной терминологией в предметной области.

Особое внимание в процессе обучения необходимо уделять взаимосвязи разделов программы по дисциплине и реализации конкретных проектов.

Желательно тематику примеров связать с предметными задачами отрасли, представить перспективу применения полученных знаний и навыков при самостоятельном решении конкретных задач на условном рабочем месте.

По результатам обсуждения изучаемого материала, выполнения творческих работ желательно формулировать рекомендации по расширенному изучению тем календарного плана Программы, если студент проявил заинтересованность в изучении дисциплины.

Автор(ы):

Рычков Вадим Александрович