Индийский филиал Автономной некоммерческой организации высшего образования «Московский университет «Синергия»

РАССМОТРЕНО
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Комплект рабочих программ дисциплин (модулей) по основной профессиональной образовательной программе высшего образования

Направление подготовки:

10.04.01 Информационная безопасность

Направленность (профиль):

Безопасность информационного и программного обеспечения автоматизированных систем

Форма обучения:

очная

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 02A7A1DF009BB38AAF4A2886FA3DCD085A
Владелец: НЕСТЕРОВ МАКСИМ СЕРГЕЕВИЧ
Действителен: с 20.11.2025 до 20.02.2027

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 15E5F2006BB416AB4E8C993599A2EAB4
Владелец: Васильев Артем Игоревич
Действителен: с 16.06.2026 до 16.06.2038

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Управление информационной безопасностью»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 8

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Управление информационной безопасностью» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе во 2 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование теоретических знаний и умений по организации системы менеджмента информационной безопасности в организациях на основе оценки рисков информационной безопасности, реализации и внедрения соответствующих механизмов контроля, распределения ролей и ответственности, обучения персонала, оперативной работы по осуществлению защитных мероприятий и мониторинга функционирования механизмов контроля.

Задачи изучения дисциплины:

– получение студентами знаний в области управления информационной безопасностью корпоративных информационных систем на основе концепции управления PDCA;

– формирование знаний в сфере моделирования процессов управления на основе различных подходов к управлению рисками информационной безопасности;

– обучение методам и технологиям работы с первичными руководящими документами и стандартами в сфере информационной безопасности и управления.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП	Код компетен	Код и наименование	Перечень планируемых результатов обучения по дисциплине	Формы образовательной

(содержание компетенций)	ции	индикатора достижения компетенций	выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	деятельности
Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	**ОПК-5**	ОПК-5.1 Знать: логические методы и приемы научного исследования; о видах экспериментов и методах обработки данных; методы анализа, синтеза, способы математического моделирования в области исследований и разработок, в том числе, организации современных систем управления.	терминологию, основные нормативные акты и стандарты в области управления информационной безопасностью	выполнять идентификацию и оценку информационных активов, идентификацию и анализ рисков; выполнять планирование обработки рисков	построения информационной модели объекта управления; практическим и аспектами процесса оценки выбора и реализации организационных и технических мер защиты информации предприятий транспортной отрасли	Контактная работа: Лекции Лабораторный практикум Самостоятельная работа
		ОПК-5.2 Уметь: осуществлять методологическое обоснование научного исследования; применять на практике различные виды обработки данных.	качественную модель оценивания соответствия защиты информации; основные подходы к проведению идентификации бизнеспроцессов и/или технологических процессов предприятий транспортной отрасли; требования к оформлению результатов оценки соответствия защиты информации	самостоятельно определить область оценки соответствия защиты информации предприятия транспортной отрасли, а также перечень неоцениваемых областей; разрабатывать проекты локальных нормативных актов, регламентирующих работу по защите информации	сбора свидетельств при проведении оценки соответствия защиты информации; навыками формирования отчетной документации по результатам оценки соответствия защиты информации	Контактная работа: Лекции Лабораторный практикум Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Система обеспечения информационной безопасности предприятия транспортной отрасли. Общие положения	6					8				8	Контрольная работа /13
Тема 2. Политика информационной безопасности предприятия транспортной отрасли	6					8				9	Контрольная работа/12
Тема 3. Инвентаризация информационных активов предприятия	6					8				8	Контрольная работа /13
Тема 4. Синтез информационной модели предприятия для целей управления информационной безопасностью	6					8				9	Контрольная работа /12
Тема 5. Управление конфигурацией и администрирование системы обеспечения информационной безопасности предприятия	6					8				8	Контрольная работа /13
Тема 6. Анализ и оценивание рисков безопасности информации. Определение потребностей защиты информации предприятия	6					8				9	Контрольная работа /12
Тема 7. Контроль и совершенствование процессов системы обеспечения	6					8				8	Контрольная работа /13

информационной безопасности предприятия											
Тема 8. Управление инцидентами безопасности информации и непрерывностью функционирования предприятия. Управление информационной безопасностью предприятия в условиях кризиса	6					8				9	Контрольная работа /12
Всего:	**48**					**64**				**68**	**100**
Контроль, час	**36**										**100 Экзамен**
Объем дисциплины (в академических часах)	**216**										
Объем дисциплины (в зачетных единицах)	**6**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Система обеспечения информационной безопасности предприятия транспортной отрасли. Общие положения

Факторы, влияющие на содержание системы защиты информации. Модель безопасности с полным перекрытием. Задачи управления системой защиты информации на предприятии. Концепция системы менеджмента информационной безопасности.

Тема 2. Политика информационной безопасности предприятия транспортной отрасли

Иерархия документов политики информационной безопасности, процедуры безопасности. Рекомендуемый перечень политики информационной безопасности. Разработка политики информационной безопасности. Роли и ответственность

Тема 3. Инвентаризация информационных активов предприятия

Виды активов, связанных с информационными системами. Цели инвентаризации, перечень и детализированная классификация информационных активов. Категории владельцев информационных активов.

Тема 4. Синтез информационной модели предприятия для целей управления информационной безопасностью

Определение ценности информационных активов. Классификатор ущерба. Паспортизация по требованиям ИБ. Операционный контроль в рамках системы обеспечения ИБ. Идентификация бизнес - процессов и требований законодательства. Описание информационно - технологических процессов.

Тема 5. Управление конфигурацией и администрирование системы обеспечения информационной безопасности предприятия

Источники угрозы безопасности информации, профиль угрозы, последствия реализации угроз ИБ. Модель угроз ИБ. Модель многоуровневой защиты. Система оценки уязвимостей. Оценка риска и задача определения потребностей защиты. Составляющие управления риском. Возможные цели менеджмента риска. Коммуникация риска.

Тема 6. Анализ и оценивание рисков безопасности информации. Определение потребностей защиты информации предприятия

Составляющие затрат на обеспечение информационной безопасности. Классификация информационных рисков. Факторы риска и методы оценки риска. Факторы, влияющие на выбор метода оценки рисков. Методология оценки рисков, основные стратегии снижения рисков, возможные факторы принятия рисков. Разработка и реализация плана обработки рисков. Оценивание остаточных рисков.

Тема 7. Контроль и совершенствование процессов системы обеспечения информационной безопасности предприятия

Программные продукты для управления рисками информационной безопасности. Структура документации, необходимая предприятию для управления рисками информационной безопасности. Тестирование полноты реализации технических мер защиты информации, контроль применения организационных мер защиты информации. Фиксация решений о необходимости выполнения корректирующих или превентивных действий в отношении системы обеспечения информационной безопасности.

Тема 8. Управление инцидентами безопасности информации и непрерывностью функционирования предприятия. Управление информационной безопасностью предприятия в условиях кризиса

Нормативная база управления инцидентами и непрерывностью бизнеса. План обеспечения непрерывности бизнеса. Жизненный цикл процесса управления непрерывностью бизнеса. Измерение готовности предприятия к обеспечению непрерывности бизнеса. Идентификация и реагирование на инциденты информационной безопасности. Управление информационной безопасностью предприятия в условиях кризиса

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Зырянова, Т. Ю. Управление информационной безопасностью : учебное пособие / Т. Ю. Зырянова. — Екатеринбург : Уральский государственный университет путей сообщения, 2023. — 96 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/149731/details

2. Овчинникова, Е. А. Основы управления информационной безопасностью : учебное пособие / Е. А. Овчинникова ; под редакцией С. Н. Новикова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2023. — 167 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/138782/details

Дополнительная литература:

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 4-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 210 с. — ISBN 978-5-4497-2408-3. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/133946/details

2. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 4-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL:

https://www.iprbookshop.ru/books/146327/details

3. Управление инцидентами информационной безопасности на объектах информатизации с учетом нейтрализации воздействия человеческого фактора : учебное пособие / О. М. Голембиовская, Е. В. Кондрашова, М. Ю. Рытов [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 121 с. — ISBN 978-5-4497-4323-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/150764/details

4. Борзунов, Г. И. Биоинспирированные алгоритмы и их применение : конспект лекций. Учебное пособие / Г. И. Борзунов, М. А. Куприяшин. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2020. — 184 с. — ISBN 978-5-7262-2699-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/116388/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Ассоциация по вопросам защиты информации	http://bis-expert.ru/
2	Специализированный сайт по тематике информационной безопасности, противодействие вредоносному программному коду	http://z-oleg.com/index.php
4	Электронный фонд правовой и нормативно-технической документации	https://docs.cntd.ru/
5	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/
6	Официальный сайт журнала «Информационная безопасность»	http://www.itsec.ru/main.php

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информатики, технологий и методов программирования

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; оснащена рабочими местами на базе вычислительной техники, подключенными к локальной вычислительной

сети и сети "Интернет", сетевым программным обеспечением, обучающим программным обеспечением

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Контрольная работа	13-10/12-10 – верные ответы составляют более 90% от общего количества; 9-7 – верные ответы составляют 80-50% от общего количества; 6-0 – менее 50% правильных ответов.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

<u>Типовые задания к контрольным работам</u>

Задание 1. Составить реестр информационных активов предприятия, определяемого по заданию преподавателя.

Задание 2. Составить реестр рисков безопасности информации предприятия, определяемого по заданию преподавателя.

Задание 3. Составить перечень технологических процессов предприятия, определяемого по заданию преподавателя.

Задание 4. Разработать технический паспорт объекта информации предприятия, определяемого по заданию преподавателя.

Задание 5. Разработать план обработки рисков безопасности информации предприятия.

Задание 6. Составить электронную форму анкеты-опросника для оценки соответствия выбранных мер защиты информации предприятия

требованиям безопасности информации для технологического процесса, определяемого по заданию преподавателя.

Задание 7. Подготовить отчет по результатам оценки соответствия защиты информации предприятия.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	Критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **-90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо) –** ответ в целом правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно) –** ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично. **-Менее 50 (неудовлетворительно)** – ответы на теоретическую часть неправильные или неполные. Задания не решены

Задания для проведения промежуточной аттестации обучающихся

1. Факторы, влияющие на содержание системы защиты информации. Модель безопасности с полным перекрытием. Требования ФСТЭК по защите информации.

2. Основные направления защиты информации. Состав задач системы обеспечения информационной безопасности предприятия транспортной отрасли.

3. Международные и государственные стандарты в области управления информационной безопасностью. Концепция системы менеджмента информационной безопасности (СМИБ).

4. Функции СМИБ, структура частных менеджментов в составе СМИБ организации. Использование знаний в СМИБ.

5. Понятие политики информационной безопасности (ПИБ) предприятия. Назначение ПИБ предприятия. Иерархия документов, составляющих ПИБ предприятия.

6. Проблема создания системы обеспечения информационной безопасности предприятия. Модель взаимодействия заинтересованных сторон.

7. Разработка политики информационной безопасности предприятия, основные правила и последовательность шагов. Структура разрабатываемых политик безопасности.

8. Формирование ролей, связанных с обеспечением информационной безопасности предприятия.

9. Организационно-распорядительная документация предприятия по вопросам обеспечения информационной безопасности. Требования ГОСТ Р 59795-2021 к содержанию документов, разрабатываемых при создании автоматизированных систем, с решениями по организационному обеспечению.

10. Понятие информационного актива организации. Виды активов, связанных с информационными системами. Способы формирования перечня сведений конфиденциального характера организации.

11. Инвентаризация активов. Владельцы информационных активов и их роль в СМИБ организации. Реестр информационных активов предприятия.

12. Необходимость паспортизации информационной инфраструктуры предприятия по требованиям информационной безопасности. Паспортизация по требованиям информационной безопасности предприятия транспортной отрасли.

13. Измерение ущерба от реализации угроз информационной безопасности и определение ценности информационных активов предприятия. Разработка классификатора потенциального ущерба

предприятия от реализации угроз информационной безопасности.

14. Информационная модель деятельности предприятия, способы формирования. Синтез информационной модели для целей менеджмента ИБ предприятия. Иерархия уровней представления информационной инфраструктуры предприятия.

15. Идентификация информационных технологических процессов предприятия. Синтез информационной модели для целей менеджмента ИБ предприятия.

16. Идентификация и классификация угроз безопасности информации предприятия. Профиль угрозы безопасности информации. Формирование модели угроз.

17. Объекты воздействия угроз ИБ в автоматизированных системах предприятия. Правила описания и оценки уязвимостей.

18. Понятие информационного риска. Составляющие управления риском. Цикл процессов управления рисками безопасности информации предприятия.

19. Классификация информационных рисков. Примеры организаций с высоким уровнем информационных рисков.

20. Факторы риска безопасности информации предприятия. Идентификация рисков безопасности информации предприятия. Оценка риска и методики используемые при оценке риска безопасности информации предприятия.

21. Процесс менеджмента риска безопасности информации. Целевые показатели величины допустимого остаточного риска, связанного с нарушением безопасности информации предприятия.

22. Составляющие затрат на обеспечение информационной безопасности предприятия и возможности по достижению оптимального значения риска безопасности информации.

23. Методы обработки риска безопасности информации предприятия. Формирование плана обработки рисков. Требования к экспертам, привлекаемым для обработки риска безопасности информации предприятия.

24. Основные стратегии снижения рисков безопасности информации. Меры оптимизации рисков безопасности информации предприятия. Выбор и реализация средств управления информационной безопасностью предприятия.

25. Принятие риска. Возможные факторы принятия рисков безопасности информации предприятия. Программные продукты для решения задач управления рисками безопасности информации предприятия.

26. Структура документации, необходимой предприятию для формирования системы обеспечения информационной безопасностью.

27. Контроль процесса функционирования системы обеспечения информационной безопасностью предприятия. Совершенствование процесса функционирования системы обеспечения информационной

безопасностью предприятия.

28. Реагирование на инциденты безопасности информации предприятия. Восстановление и возобновление работоспособности, предупреждение повторных нарушений.

29. Управления непрерывностью функционирования автоматизированных (информационных) систем предприятия. Управление непрерывностью функционирования предприятия как процесс, нормативная база и требования.

30. Управление информационной безопасностью предприятия в условиях кризиса. Создание устойчивости и смягчение уязвимостей безопасности информации предприятия.

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Защищенные информационные системы»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 6

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 10

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Защищенные информационные системы» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе в 3 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – изучение принципов построения алгоритмов и протоколов, обеспечивающих безопасность информации, освоение принципов организации и обеспечения работы шифровальных средств, математические методы криптоанализа, а также знание нормативно-правовой документации в области применения средств криптографической защиты информации.

Задачи изучения дисциплины:

– формирование профессиональной культуры обеспечения информационной безопасности в информационных системах;

– изучение принципов построения защищенных информационных систем;

– ознакомление с уязвимостями, угрозами информационной безопасности и видами деструктивного воздействия, характерными для современных информационных систем;

– изучение подходов и методов обеспечения безопасности информационных систем.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	**ОПК-2**	ОПК-2.1. Знать: основные понятия, используемые при проектировании, создании, модернизации системы защиты информации объектов информатизации; требования к разработке компьютерной системы в защищенном исполнении.	архитектуру, типовую структуру проблемноориентированной компоненты обеспечения информационной безопасности	определять и обосновывать техническую структуру подсистемы для обеспечения информационной безопасности	методами, средствами и протоколами доступа для обеспечения информационной безопасности	Контактная работа: Лекции Практические занятия Лабораторный практикум Самостоятельная работа
		ОПК-2.2. Уметь: определять основные мероприятия по организации разработки системы защиты информации на объектах информатизации; разрабатывать технические проекты, документы, регламентирующие обеспечение информационной безопасности объектов информатизации (подсистемы либо компонента системы).	основные протоколы разработки технических проектов системы обеспечения информационной безопасности в соответствии с нормативно-правовой базой	применять методы и протоколы обеспечения информационной безопасности в соответствии с нормативно-правовой базой	подходами для разработки технического проекта системы обеспечения информационной безопасности в соответствии с нормативно-правовой базой	Контактная работа: Лекции Практические занятия Лабораторный практикум Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Проектирование защищенных информационных систем, проблемы обеспечения безопасности в информационных системах	9	9				14				14	Лабораторный практикум /20
Тема 2. Криптографические протоколы и программное обеспечение	9	9				15				15	Лабораторный практикум/40
Тема 3. Защита информации на уровне подсистемы управления и технологии интеллектуального анализа	10	10				15				15	Лабораторный практикум/40
Всего:	**28**	**28**				**44**				**44**	**100**
Контроль, час	**36**										**100 Экзамен**
Объем дисциплины (в академических часах)	**180**										
Объем дисциплины (в зачетных единицах)	**5**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Проектирование защищенных информационных систем, проблемы обеспечения безопасности в информационных системах

Основные причины реализации угроз информационной безопасности. Классификация по характеру действий, используемых при различного вида атаках. Угрозы безопасности информационных систем, возникающие из-за проблем с сопровождением. Разработка концептуального плана защиты.

Тема 2. Криптографические протоколы и программное обеспечение

Управление ключами. Протоколы распределения криптографических ключей. Модели криптографической инфраструктуры. Протоколы, основанные на идентификационной информации

Тема 3. Защита информации на уровне подсистемы управления и технологии интеллектуального анализа

Управление передачей сообщений по определенным протоколам и каналам. Международные стандарты взаимодействия удаленных элементов сети. Проблемы защиты информации в интеллектуальных системах

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд.. — Саратов : Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/145912/details

2. Газизов, А. Р. Техническая защита информации : учебное пособие / А. Р. Газизов, Д. В. Фатхи. — Ростов-на-Дону : Донской государственный технический университет, 2022. — 108 с. — ISBN 978-5-7890-2053-1. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/130429/details

Дополнительная литература:

1. Ксендзов, А. В. Защищенные системы передачи информации. Ч.1 : учебное пособие / А. В. Ксендзов. — Рязань : Рязанский государственный радиотехнический университет, 2021. — 96 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/137320/details

2. Системы защиты информации в ведущих зарубежных странах :

учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. — Брянск : Брянский государственный технический университет, 2012. — 224 c. — ISBN 978-89838-488-3. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/7007/details

3. Овчинникова, Е. А. Информационная безопасность. Организационно-правовые основы. В 2 частях. Ч. 2 : учебное пособие для СПО / Е. А. Овчинникова, Г. В. Попков. — Саратов : Профобразование, 2024. — 167 c. — ISBN 978-5-4488-1877-6 (ч. 2), 978-5-4488-1883-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/139030/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Официальный сайт сетевой академии Huawei	https://e.huawei.com/en/talent/#/ict-academy/home
2	Специализированный сайт по тематике компьютерных сетей	http://www.citforum.ru
3	Томилова Э.А. Проблемные вопросы построения системы адаптивного управления защитой информации на этапах создания информационной системы в защищенном исполнении	https://elibrary.ru/item.asp?id=83984497

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информатики, технологий и методов программирования

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; оснащена рабочими местами на базе вычислительной техники, подключенными к локальной вычислительной сети и сети "Интернет", сетевым программным обеспечением, обучающим программным обеспечением

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Лаборатория технической защиты информации

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; оснащена специализированным оборудованием по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам; системой виброакустической защиты "Гамма СВАЗ-01", ПЭВМ «Secret»

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Лаборатория программно-аппаратных средств защиты информации

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; оснащена антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации (средствами анализа защищенности компьютерных сетей, аппаратно-программными средствами управления доступом к данным, стендами для изучения проводных и беспроводных компьютерных сетей, включающими абонентские устройства, коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование: оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной

информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	30-26/40-33 – работа выполнена в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы; 25-19/32-25– работа выполнена в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 20-16/26-19 – работа выполнена в срок, в основном самостоятельно, использованы соответствующие формулы; определены соответствующие спецификации, имеются ошибки в расчетах; выбраны совместимые комплектующие необходимые, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 15/20 – обучающийся подготовил работу несамостоятельно или не завершил в срок, описание спецификации содержит незначительные ошибки, выводы и ответы на вопросы отсутствуют.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые задания к лабораторному практикуму

Задание 1. Обнаружение узлов корпоративной сети. Исследуйте подсеть лаборатории (компьютерного класса / лаборатории ГУМРФ

имени адмирала С.О. Макарова), выявите все активные узлы средством запросов TimeStamp Request, Information Request, Netmask Request. Выявите узлы сети, на которых запросы ICMP Echo Request фильтруются; Повторите исследование, используя все рассмотренные в работе утилиты, сравните результаты; Сравните реакцию различных ОС на информационные ICMP-запросы.

Задание 2. Обнаружение узлов корпоративной сети средствами протокола TCP. Исследуйте подсеть лаборатории (компьютерного класса / лаборатории ГУМРФ имени адмирала С.О. Макарова), выявите все активные узлы методом TCP Ping, с использованием TCPпакетов с различным сочетанием флагов (с техникой сканирования методом TCP Ping средствами nmap); Выявите узлы сети, на которых запросы ICMP Echo Request фильтруются; Сравните реакцию различных ОС на информационные ICMP запросы. Необходимо использовать одну из рассмотренных утилит (на выбор). Результаты занесите в таблицу; Исследуйте реакцию узла сети на SYN-запросы, сравните ответы от открытого и закрытого TCP-порта. Все исследования необходимо провести средствами hping3 и nmap.

Задание 3. Обнаружение узлов корпоративной сети средствами протоколов UDP (UDP PING), IP. Идентифицируйте узлы сети, фильтрующие сообщения ICMP Echo Request. Сканирование произведите методом UPD Discovery средствами рассмотренных утилит; Исследуйте реакцию узла сети на UDP-запросы, сравните ответы открытого и закрытого UDP порта. Исследования проведите для различных ОС; Идентифицируйте узлы сети, фильтрующие сообщения ICMP Echo Request, используйте рассмотренные методы протокола IP; Сравните реакцию различных ОС на IP-пакеты с рассмотренными типами ошибок в заголовке.

Задание 4. Обнаружение узлов корпоративной сети средствами протокола ARP (ARP PING). Содержание лабораторной работы. Идентифицируйте узлы сети, фильтрующие сообщения ICMP Echo Request. Произведите сканирование методом ARPing с помощью рассмотренных утилит; Результаты проверки должны выводиться на стандартное устройство и сохраняться в файле.

Задание 5. Методы скрытого сканирования (STEALTH TCP SCANNING METHODS). Исследуйте ответ различных ОС на сканирование методами Stealth scanning. Представьте результаты для различных методов сканирования и состояний TCP-порта (порт открыт, порт закрыт, порт открыт и фильтруется, порт закрыт и фильтруется).

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	Критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **-90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо) –** ответ в целом правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно) –** ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично. **-Менее 50 (неудовлетворительно)** – ответы на теоретическую часть неправильные или неполные. Задания не решены

Задания для проведения промежуточной аттестации обучающихся

1. Подсистемы подтверждения подлинности отправки и получения сообщения.
2. Подсистемы разграничения доступа.
3. Подсистемы идентификации и аутентификации.
4. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы.
5. Подсистемы защиты связи.
6. Требования к подсистемам, предъявляемые в каждом классе

защищенности.

7. Гарантии безопасности компьютерных систем в системе общих критериев.

8. Понятие гарантии безопасности. Уровни гарантий.

9. Гарантии проектирования защищенных информационных систем.

10.Принципы обеспечения гарантий безопасности.

11.Методология анализа гарантий безопасности.

12. Каналы утечки и их анализ в системе общих критериев.

13.Виды каналов утечки информации. Место каналов утечки информации в системе общих критериев безопасности.

14.Методология анализа каналов утечки информации.

15.Безопасное функционирование в системе общих критериев.

16.Управление конфигурацией. Безопасная установка систем защиты информационных технологий.

17.Безопасная модернизация информационных технологий

18. Основные угрозы информации в компьютерных системах.

19.Специфика возникновения угроз в открытых сетях.

20.Особенности защиты информации на узлах компьютерной сети.

21. Системные вопросы защиты программ и данных.

22. Параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера.

23.Основные категории требований к программной и программно-аппаратной реализации средств защиты информации.

24.Модель угроз. Анализ критичных технологий.

25.Требования, предъявляемые к разработке модели угроз.

26.Структура модели угроз безопасности информации.

27.Анализ критичных технологий обработки информации.

28.Система лицензирования и сертификации средств защиты.

29.Структуры в РФ, обеспечивающие лицензирование и сертификацию средств защиты.

30.Нормативная база и ответственность за защиту информации в компьютерных системах.

31. Разработка политик безопасности для защищенных компьютерных систем.

32. Требования, предъявляемые к разработке политик безопасности.

33.Дискреционная и многоуровневая политика безопасности.

34.Политика мандатного доступа.

35. Политика защиты целостности информационных ресурсов.

36. Понятие аттестации защищенных компьютерных систем.

37. Технология ИИ по защите информации.

38.Аутентификация и идентификация компьютеров в сети.

39.Групповая политика и делегирование полномочий.

40.Классификации сетевых уязвимостей, угроз, и атак.

41.Механизмы реализации атак в сетях TCP/IP.

42.Технические и программные меры защиты от сетевых атак.

43.Криптографические протоколы аутентификации и защищенные сетевых приложения.

44. Межсетевое экранирование и системы обнаружения вторжений.

45.Угрозы безопасности БД

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Информационные технологии в науке и производстве»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 6

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 9

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Информационные технологии в науке и производстве» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе в 1 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование компетенций решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и использованием информационных систем с учетом основных требований информационной безопасности.

Задачи изучения дисциплины:

– сформировать представление об информационных технологиях, основах информационной безопасности, средствах информационных компьютерных технологий, основных видах современного прикладного программного обеспечения общего и профессионального назначения;

– развить способность решения стандартных задач профессиональной деятельности с помощью средств информационных технологий;

– научить применять программное обеспечение общего назначения, использовать информационно-поисковые средства глобальной сети Интернет для решения поисковых, образовательных и прикладных задач.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП	Код компетен	Код и наименование	Перечень планируемых результатов обучения по дисциплине	Формы образовательной

(содержание компетенций)	ции	индикатора достижения компетенций	выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	деятельности
Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	**ОПК-4**	ОПК-4.1. Знать: основные перспективы развития науки и техники в области профессиональной деятельности для проведения научных исследований и разработок; методы отыскания оптимальных решений.	знать основные перспективы развития науки и техники в области профессиональной деятельности для проведения научных исследований и разработок; методы отыскания оптимальных решений			Контактная работа: Лекции Лабораторный практикум Самостоятельная работа
		ОПК-4.2. Уметь: осуществлять анализ источников научно-технической информации с целью дальнейшего применения в рамках исследования; применять на практике различные виды обработки данных.		осуществлять анализ источников научно-технической информации с целью дальнейшего применения в рамках исследования; применять на практике различные виды обработки данных		
		ОПК-4.3. Владеть навыками осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов, разработки плана проведения научной и проектной деятельности.			осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов, разработки плана проведения научной и проектной деятельности	

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Введение в информационные технологии в науке	7					7				13	Реферат/25
Тема 2. Технологии математического и имитационного моделирования	7					7				13	Реферат/25
Тема 3. Технологии анализа данных	7					7				13	Реферат/25
Тема 4. Технологии информационного менеджмента	7					7				13	Реферат/25
Всего:	**28**					**28**				**52**	**100**
Контроль, час											**100 Зачет**
Объем дисциплины (в академических часах)	**108**										
Объем дисциплины (в зачетных единицах)	**3**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Введение в информационные технологии в науке

Введение в информационные технологии в науке и производстве. Информационные технологии в оформлении научных публикаций. Разработка плана статьи.

Тема 2. Технологии математического и имитационного моделирования

Технологии математического и имитационного моделирования. Имитационное моделирование в Arena.

Тема 3. Технологии анализа данных

Технологии анализа данных. Анализ информации – основные принципы. Консолидация данных. Трансформация данных.

Тема 4. Технологии информационного менеджмента

Технологии информационного менеджмента. Управление научноисследовательскими инвестиционными проектами.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Тюльпинова, Н. В. Компьютерные и информационные технологии в науке и производстве : учебное пособие для магистров / Н. В. Тюльпинова. — Саратов : Вузовское образование, 2020. — 268 c. — ISBN 978-5-4487-0612-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/88759/details

Дополнительная литература:

1. Методы, алгоритмы и архитектуры распределенной обработки больших данных : учебное пособие / И. В. Никифоров, О. А. Юсупова, Н. В. Воинов, А. Д. Ковалев. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2023. — 194 c. — ISBN 978-5-7422-8461-1. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/147723/details

2. Муромцев, В. В. Информационные технологии в профессиональной деятельности : учебник и практикум / В. В. Муромцев, А. В. Муромцева. — Москва, Вологда : Инфра-Инженерия, 2023. — 383 c. — ISBN 978-5-9729-1299-5. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/133166/details

3. Цифровые ресурсы в научном исследовании : учебное пособие / С. И. Головкина, В. Е. Засенко, Е. А. Афоничкина [и др.]. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2025. — 106 c. — ISBN 978-5-7422-8987-6. — Текст :

электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/152106/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Информационно-аналитический портал	http://www.ixbt.com
2	Microsoft	http://www.microsoft.com/ru-ru/default.aspx
3	1С	http://www.1c.ru/
4	Лаборатория Касперского	http://www.kaspersky.ru/
5	Ассоциация Предприятий Компьютерных и Информационных Технологий	http://apkit.ru/
6	Российский союз ИТ директоров	http://www.rucio.org/

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информационных технологий для проведения лабораторных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения,

электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Реферат	25 - 20 – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению; 19 - 14– основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы; 13 - 8 – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении. 7 - тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы;

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые темы рефератов

1. Обзор современного ПО, используемого для решения задач в профессиональной деятельности.
2. Реализация возможностей систем искусственного интеллекта в профессиональной сфере.
3. Реализация возможностей экспертных систем в профессиональной сфере.
4. Информационные технологии в обработки результатов научного эксперимента.

5. Обзор статистических методов, используемых при обработке данных эксперимента.

6. Охрана интеллектуальной собственности: авторские и смежные права в интернет.

7. Облачные технологии в профессиональной деятельности.

8. Новые производственные технологии, промышленный интернет.

9. Государственная политика РФ в области информационных ресурсов.

10. Технологии машинной графики и визуализации.

11. Нейро-математические и нейро-информационные технологии и сети.

12. Когнитивные технологии в профессиональной деятельности.

13. Технологии информационного реинжиниринга.

14. Объектно-ориентированные технологии, технологии объектно-ориентированного анализа.

15. Своя, согласованная с преподавателем тема.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета

Краткая характеристика оценочного средства	Критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов «Зачтено» – 90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Дайте определение Информационной технологии.
2. Охарактеризуйте ИТ поиска информации.
3. Охарактеризуйте ИТ обработки данных.
4. Охарактеризуйте эмерджентные технологии.
5. Какой сервис используется для определения индекса УДК статьи?
6. Какие сервисы для перевода и транслитерации текста Вам известны?
7. Что показывает показатель Индекс цитирования CI?
8. Что показывает показатель Индекс Хирша?
9. Для чего необходима верификация?
10. Что обозначает научное исследование?
11. Какие бывают виды научных статей?
12. Что такое методология?
13. Что такое машинное обучение?
14. Где применяется машинное обучение?
15. Перечислите способы машинного обучения.
16. Что такое ассоциация, приведите пример.
17. Охарактеризуйте понятие большие данные.
18. Что такое хранилище данных?
19. Дайте понятие производственной системы.
20. Что такое моделирование?
21. Перечислите виды моделирования.
22. Что такое агентное моделирование?
23. Когда модель адекватна?
24. Процесс построения модели, как правило, предполагает…
25. Физическое моделирование – это…
26. Для чего используются самоорганизующие карты?
27. Почему информационный подход к моделированию получил сегодня распространение?
28. Что такое регрессия?
29. Дайте определение базы данных?
30. Что такое структурированные данные?
31. Какие модели БД самые распространенные?
32. Что такое нейронная сеть?
33. Что такое трансформация данных.
34. Для чего используется консолидация данных?
35. Что такое кластеризация данных?
36. Что такое Data Mining?
37. Для чего необходим парсинг?
38. Дайте определение глобальной сети.

39. Что такое промышленный интернет?
40. Что такое интернет вещей?
41. Дайте определение локальной сети.
42. Современная структура интернет.
43. Какие угрозы безопасности информации вы знаете?
44. Что такое цифровая подпись?
45. Что называют анализом данных?
46. Что называется экспертной системой?
47. Что содержит экспертная система?
48. Системы поддержки принятия решений решают ...
49. Что можно считать искусственным интеллектом?
50. К отечественному ПО для анализа и обработки данных относят…

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Иностранный язык в профессиональной сфере»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

СОДЕРЖАНИЕ

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 5

3. ТЕМАТИЧЕСКИЙ ПЛАН 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 10

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 13

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Иностранный язык в профессиональной сфере» составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования - магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Министерства образования и науки РФ от 26.11.2020 № 1455.

Изучение дисциплины «Иностранный язык в профессиональной сфере» является продолжением языкового курса бакалавриата. Она направлена на формирование общей и профессиональной коммуникативной компетенций: развитие у обучающихся навыков чтения, аудирования и письма, изучение основных понятий с целью использования полученных знаний в повседневной жизни и профессиональной деятельности.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в учебные планы по программам подготовки магистров по направлению 10.04.01 Информационная безопасность и входит в обязательную часть Блока 1.

Дисциплина изучается на 1 курсе в 1 семестре.

Цель и задачи дисциплины.

Цель изучения дисциплины – формирование у обучающихся необходимых компетенций для успешного освоения образовательной программы, в частности повышение исходного уровня владения иностранным языком (английский язык), достигнутого на предыдущей ступени образования, и овладение обучающимися необходимым и достаточным уровнем коммуникативной компетенции для решения социально-коммуникативных задач в профессиональной деятельности при общении с зарубежными партнерами, а также для дальнейшего самообразования.

Задачи изучения дисциплины:

- знать методы активного речевого поведения в ситуациях общения при осуществлении профессиональной деятельности;
- знать основные грамматические явления, характерные для деловой речи;
- знать нормы устного общения на деловые профессиональные темы;
- знать нормы деловой профессиональной лексики языка и уметь её использовать;
- знать и иметь практический опыт по осуществлению деловой переписки;
- уметь применять активное речевое поведения в ситуациях общения при осуществлении профессиональной деятельности;
- иметь практический опыт устного общения на деловые профессиональные темы;
- иметь практический опыт по применению основных

грамматических явлений, характерных для деловой речи;

- иметь практический опыт проведения дискуссии на профессиональные темы (задавать вопросы и отвечать на вопросы; комментировать и делать выводы).

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой

Результаты освоения ООП (содержание компетенций)	**Код компетенции**	**Код и наименование индикатора достижения компетенций**	**Перечень планируемых результатов обучения по дисциплине**			**Формы образовательной деятельности**
			должен знать	**должен уметь**	**должен иметь практический опыт**	
Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**УК-4**	УК-4.1. Знает современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации.	современные коммуникативные технологии позволяющие обеспечивающие понимание сути и значения современного менеджмента	использовать современные коммуникативные технологии для осуществления свободного чтения оригинальной литературы на иностранном языке по менеджменту	осуществления поискового, ознакомительного, изучающего и просмотрового чтения как с использованием современных коммуникационных технологий, так и без них.	Контактная работа: Практические занятия Самостоятельная работа
		УК-4.2. Уметь применять на практике коммуникативные технологии, методы и способы делового общения.	современные коммуникативные технологии позволяющие обеспечивающие понимание профессиональной коммуникации; терминологический минимум по специальности, особенности осуществления поиска нужной информации по заданной теме в иноязычных источниках различного типа	использовать современные коммуникативные технологии для осуществления свободного чтения оригинальной литературы на иностранном языке для профессионального взаимодействия; оформлять извлеченную из иностранных источников информацию в виде перевода или резюме	осуществления поискового, ознакомительного, изучающего и просмотрового чтения как с использованием современных коммуникационных технологий, так и без них; четко и логично выражать свои мысли в устной и письменной формах с учетом стилей общения	
		УК-4.3. Владеть методикой межличностного делового общения на государствен	иноязычные лексико-грамматические средства, профессиональные языковые формы,	делать сообщения и доклады на иностранном языке на темы, связанные с научной деятельностью	поиска нужной информации на профессиональную тематику в печатных и электронных источниках	

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			должен знать	должен уметь	должен иметь практический опыт	
		ном и иностранном языках, с применением профессиональных языковых форм и средств.	обеспечивающие понимание профессиональной коммуникации	магистранта; вести беседу на иностранном языке по специальности		
Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	**УК-5**	УК-5.1. Знает сущность, разнообразие и особенности различных культур, их соотношение и взаимосвязь.	межкультурные особенности ведения профессиональной и научной деятельности	преодолевать этно- и культурноцентристкие стереотипы	речевого и невербального поведения в условиях деловой межкультурной коммуникации	Контактная работа: Практические занятия Самостоятельная работа
		УК-5.2. Уметь обеспечивать и поддерживать взаимопонимание между обучающимися – представителями различных культур и навыки общения в мире культурного многообразия.	правила коммуникативного поведения в ситуациях межкультурного делового общения	действовать в соответствии с традициями данного культурного контекста и выполнять стандартные для данной ситуации действия; использовать этикетные формы научно - профессионального общения	использования речевого этикета профессионального общения	

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
1 семестр											
Unit 1. Economics and information systems		1	2							8	Доклад-презентация и участие в дискуссии/5 Тест/3
Unit 2. Economic Systems		1	2							8	Доклад-презентация и участие в дискуссии/5 Тест/3
Unit 3. Corporate Information System (CIS)		1	2							8	Доклад-презентация и участие в дискуссии/5 Тест/3
Unit 4. Making Information Security Strategic to Business		1	2							8	Доклад-презентация и участие в дискуссии/5 Тест/3
Unit 5. System Integration (SI)		2	2							9	Доклад-презентация и участие в дискуссии/5 Тест/3
Unit 6. Customer Relationship Management		2	2							9	Доклад-презентация и участие в дискуссии/5 Тест/3
Unit 7. E-Business (Electronic Business)		2	2							9	Доклад-презентация и участие в дискуссии/5 Тест/3
Unit 8. IT Project Management		2	2							9	Доклад-презентация и участие в дискуссии/5 Тест/3
Unit 9. Intellectual Property: Software Protection		2	1							9	Доклад-презентация и участие в дискуссии/5 Тест/4
Unit 10. Laptops and Tablets in Business Communication		2	1							9	Доклад-презентация и участие в дискуссии/5 Тест/4
Unit 11. Collaboration in Cyberspace and Global Economy		2	1							9	Доклад-презентация и участие в дискуссии/5 Тест/4
Unit 12. Digital Economy		2	1							9	Доклад-презентация и участие в дискуссии/5 Тест/4
Всего:		**20**	**20**							**104**	**100**

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Контроль, час	**36**										**Экзамен**
Объем дисциплины (в академических часах)	**180**										
Объем дисциплины (в зачетных единицах)	**5**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Unit 1. Economics and information systems

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of issues on economics and information systems. Business and technology.

Unit 2. Economic Systems

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of economic systems. Economic Systems. Economic input. Factors of production. Efficiency. Traditional economic system. Market economic system. Mixed economic system.

Unit 3. Corporate Information System (CIS)

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of the Corporate Information System (CIS). Key functions of the corporate information system. SAP ERP.

Unit 4. Making Information Security Strategic to Business

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of Making Information Security Strategic to Business.

Unit 5. System Integration (SI)

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of System Integration (SI). Economic downturn. Economic crisis. Information security. Combat cyber-threats.

Unit 6. Customer Relationship Management

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of Customer Relationship Management. Overview of CRM systems.

Unit 7. E-Business (Electronic Business)

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of E-Business (Electronic Business). E-business model. Advantages of e-business. Types of e-business. Challenges of e-business. Security and risks. E-business vs e-commerce.

Unit 8. IT Project Management

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of IT Project Management. Phases of IT project management. Challenges faced by IT project managers. Types of IT project management tools. Example of an information technology

project. Streamline projects with IT project management software.

Unit 9. Intellectual Property: Software Protection

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of Intellectual Property: Software Protection. Identifying Your Intellectual Property. How to protect software intellectual property. Intellectual Property Theft. Creating Robust Intellectual Property Protections. Strategy to protect your intellectual property.

Unit 10. Laptops and Tablets in Business Communication

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of Laptops and Tablets in Business Communication. The Benefits of Using Telecommunication in Businesses. Benefits of Mobile Technology for Business. What issues do IT departments need to consider when adopting tablets? What are the best ways to use tablets for business?

Unit 11. Collaboration in Cyberspace and Global Economy

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of Collaboration in Cyberspace and Global Economy. International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World.

Unit 12. Digital Economy

Warm-up activities. Reading and translate text. Comprehension. Translate text into Russian/English language. Discussion of Digital Economy. Evolution of the digital economy concept. Main components of the digital economy. Trends in emerging digital technologies. Value in the digital economy. Measuring value in the digital economy. Value creation and capture in the digital economy: A global perspective.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Брискер, М. В. English for computer science : учебное пособие / М. В. Брискер. — Москва, Вологда : Инфра-Инженерия, 2023. — 116 с. — ISBN 978-5-9729-1563-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/133354/details

2. English for Information Technology : учебное пособие для студентов технических направлений подготовки / составители О. И. Тараканова, О.

Ю. Зиско, Е. М. Покровская. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2023. — 82 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/152777/details

Дополнительная литература:

1. English for Master's Course = Английский для магистрантов : учебное пособие / М. Н. Алексеева, И. Н. Галивец, О. В. Иванова [и др.]. — 2-е изд.. — Москва : Российский новый университет, 2023. — 156 с. — ISBN 978-5-89789-212-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/137670/details

2. Никрошкина, С. В. Английский язык для магистрантов: научная деятельность. English for master students: academic activity : учебное пособие / С. В. Никрошкина. — Новосибирск : Новосибирский государственный технический университет, 2023. — 75 с. — ISBN 978-5-7782-5072-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/156039/details

3. Юдина, О. Л. English for postgraduates : учебное пособие / О. Л. Юдина. — Екатеринбург : Уральский институт управления – филиал РАНХиГС, 2021. — 106 с. — ISBN 978-5-8056-0418-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/158003/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1.	Материалы по теме The Digital Economy and Digital Business	https://link.springer.com/chapter/10.1007/978-3-030-91247-5_4
2.	Официальный сайт газеты "FinancialTimes".	http://www.ft.com
3.	Digital economy – статья на английском языке	https://www.ebsco.com/research-starters/technology/digital-economy

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Виды контактной работы, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Доклад-презентация и участие в дискуссии	*Оценка за участие в семинаре состоит из оценки за доклад:* 4 – доклад выполнен в соответствии с требованиями, 10 правильно оформленных слайдов презентации, грамотное использование терминологии, свободное изложение рассматриваемых проблем, докладчик правильные ответил на все вопросы преподавателя и обучающихся. 3 – доклад выполнен в основном соответствии с требованиями,10 не совсем правильно оформленных слайдов презентации, грамотное использование экономической терминологии, в основном свободное изложение рассматриваемых проблем, докладчик частично правильно ответил на все вопросы преподавателя и обучающихся. 2 – доклад выполнен в основном в соответствии с требованиями,10 не совсем правильно оформленных слайдов презентации, докладчик был привязан к тексту, докладчик испытывал затруднения при ответе на вопросы преподавателя и обучающихся. 1 – доклад выполнен не в соответствии с требованиями, 10 не совсем правильно оформленных слайдов презентации, 0 - докладчик был привязан к тексту, докладчик не смог ответить на вопросы преподавателя и обучающихся. *Оценка участия в дискуссии:* 1 – за одно выступление
2.	Тест	4 – верные ответы составляют более 90% от общего количества; 3 – верные ответы составляют 80-50% от общего количества; 2-0 – менее 50% правильных ответов
3.	Тест	3 – верные ответы составляют более 90% от общего количества; 2 – верные ответы составляют 80-50% от общего количества; 1 - 0 – менее 50% правильных ответов

Типовые контрольные задания или иные материалы текущего

контроля успеваемости

Примерные темы докладов-презентаций и дискуссий:

1. Economics and information systems.
2. Business and technology.
3. Factors of production. Efficiency.
4. Traditional economic system
5. Market economic system
6. Mixed economic system
7. Corporate Information System (CIS).
8. Key functions of the corporate information system.
9. SAP ERP
10. Economic downturn.
11. Economic crisis.
12. Information security.
13. Combat cyber-threats
14. System Integration (SI): Types, Approaches, and Implementation Steps.
15. Overview of CRM systems.
16. E-business model.
17. Advantages of e-business.
18. Types of e-business.
19. Challenges of e-business.
20. Security and risks.
21. E-business vs e-commerce.
22. Phases of IT project management.
23. Challenges faced by IT project managers.
24. Types of IT project management tools.
25. Example of an information technology project
26. Streamline projects with IT project management software.
27. Identifying Your Intellectual Property.
28. How to protect software intellectual property.
29. Intellectual Property Theft.
30. Creating Robust Intellectual Property Protections.
31. Strategy to protect your intellectual property.
32. The Benefits of Using Telecommunication in Businesses.
33. Benefits of Mobile Technology for Business.
34. What issues do IT departments need to consider when adopting tablets?
35. What are the best ways to use tablets for business?
36. International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World
37. Evolution of the digital economy concept.
38. Main components of the digital economy.
39. Trends in emerging digital technologies.
40. Value in the digital economy.
41. Measuring value in the digital economy.

42. Value creation and capture in the digital economy: a global perspective.

Примерные тестовые задания

Задание 1

Choose the best verb.

1. To turn on the computer, _____ the "Start" button.

a. touch b. press c. switch

2. The printer has _____ of ink.

a. finished b. ended c. run out

3. Unfortunately, my scanner isn't _____ at the moment.

a. working b. going c. doing

4. Please _____ the CD ROM.

a. insert b. introduce c. inject

5. The projector isn't working because it isn't _____.

a. plugged b. plugged in c. plugged into

6. The batteries in my digital camera are nearly dead. They need _____.

a. to change b. exchanging c. changing

7. I have to _____ a computer screen for eight hours a day.

a. see b. look at c. watch

8. Switch off your computer, and _____ it from the wall socket.

a. de-plug b. unplug c. non-plug

9. I turned off the photocopier and _____ the plug.

a. pulled out b. extracted c. took away

10. _____ any key to continue.

a. Kick b. Smash c. Hit

Задание 2.

1. Governments ... information systems to provide services to citizens.

a) move

Ь) deploy

c) !ay

2. Infon11ation systems have quickened the ... of daily activities.

a) pace

Ь) rack

c) scale

3. Android is designed primarily for ... moЬile devices such as smart-phones and taЬIet computers.

a) optic-fiber

Ь) touchscreen

c) soft-touch

4. Avirtual keyboard is a ... compoпent that allows a user to enter characters.

a) routiпe

Ь) package

c) software

5. A ... keyboard can usually be operated with multiple input devices.

a) virtual

Ь) image

c) moral

6. Despite being primarily ... for touchscreen input, Android also has been llsed iп game coпsoles, digital cameras, regular PCs and other electro пics.

a) spen t

Ь) designed

c) elaborated

7. A ... operating system is an operating system for devices st1ch as a smartphone, taЬlet, PDA, or other moЬile devices.

a) resilient

Ь) fast-moving

c) mobile

8. Mobile operating systems ... features of a personal computer opera t-ing system with other features useful for mobile or handheld use.

a) compact

Ь) combine

c) claster

9. We find ourselves in an age of digital ... where information is put at risk every day.

a) warfare

Ь) inconsequence

c) irrationality

10. And information ... has a critical role to play in tl1e drive toward in-novation.

a) security

Ь) consistency

c) regularity

Задание 3.

I. Прочитайте и письменно переведите оригинальный текст с английского на русский язык.

A traveller who had been riding in the rain and was wet through, arrived at a small hotel in the country. There was only one fireplace in the hall and a lot of people around it. The traveller thought of a plan how to get warm. He asked the hotel owner to take some fish to his horse. The hotel owner was surprised but the traveller insisted and the hotel owner did as he was asked. All the people rushed out to see the horse eat fish. The traveller had the fireplace all to himself and felt comfortable. When the hotel owner returned he said, "I was sure horses do not eat fish."— "Then why did you take it to my horse?"

Вопросы:

1. Why did the hotel owner try to feed the horse with fish?

2. Why did the traveller ask him to do it?

II. Поставьте вопрос к подчеркнутому члену предложения.

The traveller thought of a plan how to get warm.

III. Раскройте скобки, употребив правильную глагольную форму.

Once John Smith and his wife Mary who (1 — live) in a small house in the mountains, (2 — find) a dog. Though the dog (3 — be) weak and hungry, he (4 — not eat) anything in the presence of his new masters. Several days later the dog (5 — disappear). John and Mary (6 — leave) alone. But one day when Smith (7 — travel) in a train, he (8 — see) his dog running along the road. He (9 — get) off the train at the next station, (10 — buy) a piece of meat, (11 — catch) the dog and (12— bring) him home again. There the dog (13 — tie) up for a week.

The dog (14— escape) several times and each time he (15— run) north. At last the dog (16 — decide) to stay at the cottage but a long time (17 — pass) before Smith and his wife (18 — can) touch him. They (19 - call) him Wolf.

One summer a stranger (20 — come) to the cottage. As soon as the dog (21 — see) him, he (22— rush) to the stranger and (23 — lick) his hands. Then the stranger (24 - say): "His name (25 - be) not Wolf. It (26 - be) Brown. He (27 - be) my dog." Mary (28 - ask) to leave the dog with them. But the stranger (29 — refuse) and (30 — say) that the dog (31 — must) decide it himself. "I (32 — say) goodbye and (33 — go) away. If he (34 — want) to stay, let him stay." For some time Wolf (35 — watch) the man go. Then he (36 — rush) after him and (37 - try) to stop him. Then the dog (38 - run) back to Smith and his wife (39 - try) to drag Smith after the stranger. He (40 – want) to be at the same time with the old and the new master. Finally the dog (41 — lie) down at the feet of Smith. Mary (42 — be) happy.

IV. Выберите правильный вариант.

1.I... glasses since I was a child,

a) wear, b) wore, c) am wearing, d) have been wearing.

2. When the phone rang, I... dinner.

a) cook, b) was cooking, c) had been cooking, d) have been cooking.

3. He usually had dinner at 4 p.m., ... ?

a) had he, b) hadn't he, c) did he, d) didn't he.

4. He works ... and makes good progress.

a) hard, b) hardly, c) good, d) badly.

5. He reminds me ... someone I knew in the army.

a) of, b) to, c) from, d) about.

6. Mary is here. Where are ... ?

a) other, b) others, c) the others, d) another.

7. What ... bad weather we are having today!

a) the, b) a, c) an, d) — .

8. Did you read ... English books at school?

a) some, b) many, c) much, d) none.

9. I want to know what ...,

a) are you doing, b) were you doing, c) will you do, d) you are doing.

10. I've made ... mistakes now than I made last time.

a) few, b) a few, c) fewer, d) less.
11. Can ... of you help me?
a) some, b) any, c) somebody, d) anybody.
12. This translation is twice as ....
a) easy, b) easier, c) the easiest, d) much easier.
13. We ... two compositions this month.
a) write, b) wrote, c) were writing, d) have written.
14. I had a feeling that somebody ... there before.
a) is, b) was, c) has been, d) had been.
15. She won't see him ... he phones her.
a) except, b) after, c) unless, d) because.
16. ... only one theatre and two cinemas in this city ten years ago.
a) there is, b) there was, c) there are, d) there were.
17. My watch....
a) stops, b) has stopped, c) have stopped, d) stop.
18. Do you know when he ... ?
a) comes, b) will come, c) shall come, d) come.
19. I don't have any pets. Neither ....
a) she does, b) does she, c) is she, d) does she have.
20. His parents didn't let him ... TV late.
a) to watch, b) watch, c) watching, d) watched.

V. Переведите на английский язык.

1. Москва была основана Юрием Долгоруким.
2. Небо темное, может пойти дождь.
3. Мы не знали, что он собирается нас навестить.
4. Кто знает прогноз погоды на завтра?
5. Нам не пришлось долго ждать их.

VI. Выберите правильный ответ.

1. What's the name of the most famous clock in Britain?
a) Big Albert, b) Big Stephen, c) Big Wren, d) Big Ben.
2. What's tartan?
a) a dish, b) a pattern of the kilt, c) a bird, d) a dance.
3. Where is Glasgow situated?
a) in Scotland, b) in Wales, c) in England, d) in Northern Ireland.
4. What's the name of the London underground?
a) Metro, b) Tube, c) Subway, d) Underground,
5. What is the nickname of the Liberal Party?

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета в 1 семестре и экзамена во 2 семестре.

Процедура оценивания	**Шкала и критерии оценки, балл**

Процедура оценивания	Шкала и критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета, включающего в себя: Задание №1 – теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень владения обучающимся принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними; Задание №2 – задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности; Задание №3 – задание на проверку умений и опыта, полученных в результате освоения дисциплины	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **-90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые формулы, использована профессиональная лексика. Задача решена правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо)–** ответ в целом правильный, логически выстроен, приведены необходимые формулы, использована профессиональная лексика. Ход решения задачи правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно)–** ответ в основном правильный, логически выстроен, приведены не все необходимые формулы, использована профессиональная лексика. Задача решена частично. **-Менее 50 (неудовлетворительно)**– ответы на теоретическую часть неправильные или неполные. Задача не решена

Типовые задания для проведения промежуточной аттестации обучающихся

1 семестр

Задания 1-го типа

1. Economics and information systems.
2. Business and technology.
3. Factors of production. Efficiency.
4. Traditional economic system
5. Market economic system
6. Mixed economic system
7. Corporate Information System (CIS).
8. Key functions of the corporate information system.
9. SAP ERP
10. Economic downturn.
11. Economic crisis.
12. Information security.
13. Combat cyber-threats
14. System Integration (SI): Types, Approaches, and Implementation Steps.
15. Overview of CRM systems.
16. The roles of information in the economic system.
17. Rational theory of information acquisition.
18. The market as information: theory.

19. The market as information: in practice.
20. General equilibrium with markets for future and uncertainty.
21. Electronic business. Basic definitions and concepts
22. E-commerce. Basic definitions and concepts
23. Internet entrepreneurship. Kinds
24. Internet entrepreneurship. Development prospects
25. Team management in IT project management
26. E-business model.
27. Advantages of e-business.
28. Types of e-business.
29. Challenges of e-business.
30. Security and risks.
31. E-business vs e-commerce.
32. Phases of IT project management.
33. Challenges faced by IT project managers.
34. Types of IT project management tools.
35. Example of an information technology project
36. Streamline projects with IT project management software.
37. Identifying Your Intellectual Property.
38. How to protect software intellectual property.
39. Intellectual Property Theft.
40. Creating Robust Intellectual Property Protections.
41. Strategy to protect your intellectual property.
42. The Benefits of Using Telecommunication in Businesses.
43. Benefits of Mobile Technology for Business.
44. What issues do IT departments need to consider when adopting tablets?
45. What are the best ways to use tablets for business?
46. International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World
47. Evolution of the digital economy concept.
48. Main components of the digital economy.
49. Trends in emerging digital technologies.
50. Value in the digital economy.
51. Measuring value in the digital economy.
52. Value creation and capture in the digital economy: a global perspective.

Задания 2-го типа

1. What are the main challenges of AI development? Justify the answer.
2. Analyze the main differences between mass communication and interpersonal communication.
3. Describe the main risks of the introduction of artificial intelligence technologies. Justify the answer.
4. Analyze the main differences in the features of negotiating in Japan and in India.

5. Analyze the main features of AI regulation.

6. How, in your opinion, should the development, implementation and use of artificial intelligence technologies be regulated? Justify the answer.

7. What are the differences between a micro-project and a small project? Justify the answer.

8. Compare the four types of information culture. What are the differences? Explain the answer.

9. What tasks, in your opinion, should the regulation of artificial intelligence solve? Justify the answer.

10. 10 What are the main key aspects of AI regulation and their implementation in Russia? Justify the answer.

11. Compare different types of IP and the principles of their creation. What are the differences? Justify the answer.

12. Analyze global trends in the development and evaluation of the Russian market.

13. What is the human factor in the formation of the AI era? Justify the answer.

14. Describe the main differences between integral and positional negotiations. What are the differences? Justify the answer.

15. Analyze the main characteristics of higher education in the digital economy.

16. Analyze the main differences between the two communication models. Aristotle's model. The Lasswell model. What are the differences? Justify the answer.

17. Compare the characteristics of the standard of digital services in the UK and in Russia. What are the differences? Justify the answer.

18. Analyze the labor market and human resources competencies in the digital age. What changes have occurred compared to the pre-digital era? Justify the answer.

19. Project management standards: private and public. What are the differences? Justify the answer. Analyze the main differences between the types of information system architecture: non-integrated (distributed), poorly integrated, and highly integrated. What are the differences?

20. Describe the main differences between nonverbal and verbal business communication. What are their differences? Justify the answer.

21. What is the difference between the effect and the effectiveness of the project, how are these concepts related to each other? Justify the answer.

22. Analyze the impact of digital technologies on the labor market.

23. Classification of software protection systems. What are the differences? Justify the answer

24. Describe the social assessment system in China.

25. Compare the characteristics of the digital services standard in Germany and in Japan. What are the differences? Justify the answer.

26. Analyze the prerequisites for the development of artificial intelligence science.

27. Analyze the main differences between mass communication and interpersonal communication.

28. Describe the main risks of the introduction of artificial intelligence technologies. Justify the answer.

29. Analyze the main differences in the features of negotiating in Japan and in India.

30. Analyze the main features of AI regulation in Russia.

31. How, in your opinion, should the development be regulated, introduction and use of artificial intelligence technologies in higher education? Justify the answer.

32. Analyze the biological modeling of artificial intelligence.

33. Compare the four types of information culture. What are the differences? Explain the answer.

34. What tasks, in your opinion, should the regulation of artificial intelligence solve? Justify the answer.

35. 10 Analyze the main risks of the introduction of artificial intelligence in the healthcare sector.

36. Analyze the main risks of the introduction of artificial intelligence in the field of national defense.

37. Analyze the main risks of the introduction of artificial intelligence in banking.

38. What is the human factor in the formation of the AI era? Justify the answer.

39. Describe the main differences between integral and positional negotiations. What are the differences? Justify the answer.

40. Analyze the main disadvantages of artificial intelligence.

41. Analyze the main differences between the two communication models. Aristotle's model. The Lasswell model. What are the differences? Justify the answer.

42. Compare the characteristics of the standard of digital services in the USA and in Russia. What are the differences? Justify the answer.

43. Analyze the labor market and human resources competencies in the digital age. How does the situation in Russia differ from Western countries? Justify the answer.

44. Project management standards: private and public. What are the advantages and disadvantages? Justify the answer.

45. Describe the main differences between nonverbal and verbal business communication. What are their differences? Justify the answer.

46. Analyze the problems and risks of AI in the field of civil aviation.

47. Analyze the impact of digital technologies on the labor market.

48. Classification of software protection systems. What are the differences? Justify the answer

49. Analyze the problems and risks of AI in the field of railway transport.

50. Give a description of the social assessment system in China.

51. Compare the characteristics of the digital services standard in the EU

and in the USA. What are the differences? Justify the answer.

Задания 3-го типа

Задание №1.

Прочитайте и перескажите текст на английском языке.

Среди представителей профессий, отличающихся высокой вероятностью полной автоматизации и замены роботизированными или программными решениями, в первую очередь те, что связаны с выполнением формализованных повторяющихся операций. Например, развитие автоматизированных вопросноответных систем и голосовой биометрии способствует полному вытеснению сотрудников служб поддержки, которые помогают клиентам решать наиболее часто встречающиеся вопросы. В перспективе работники, выполняющие простые умственные операции, будут задействованы только в нестандартных ситуациях, с которыми не справился ИИ. С развитием технологий машинного перевода, распознавания речи в будущем исчезнет профессия переводчика и оператора колл-центра, даже живые экскурсоводы скорее станут экзотикой — их заменят нейронные сети, способные производить адаптивный контент для каждого конкретного пользователя. В числе «исчезающих» профессий — агент-туроператор, аналитик общего профиля, архивариус, аудитор, банковский операционист, делопроизводитель, инженер по эксплуатации зданий, кассир, клиентский менеджер, кредитный менеджер, нотариус, охранник административных зданий, рекрутер, телемаркетолог, трейдер, юридический консультант. Развитие технологий, цифровая трансформация компаний, рост конкуренции за рабочие места, увеличение продолжительности жизни приводят работников к необходимости менять сферу профессиональной деятельности несколько раз в течение жизни, приобретая новые компетенции и навыки. Чтобы оставаться востребованным на рынке труда, человек должен получать новые знания быстрее, чем это было ранее. Пересматриваются подходы к обучению, трансформируются образовательные модели. К ключевым задачам, которые стоят сегодня перед образованием, относятся создание учебного контента, отвечающего требованиям динамично изменяющегося рынка труда и потребностям человека, а также сокращение расходов за счет использования технологий [Global Education Futures Report, 2018]. Среди наиболее актуальных трендов в образовании: непрерывное обучение или обучение в течение всей жизни, омниобучение (обучение с использованием всех возможных каналов коммуникации), социальное обучение, микрообучение, адаптивное обучение, нейрообучение, дистанционное обучение, менторство, смешанное обучение, проектно-ориентированное обучение, «самообучающиеся» организации, EdTech-стартапы и др.

Задание №2.

Прочтите и переведите текст устно.

В наибольшей степени осведомлены о современных цифровых

технологиях сотрудники научно-исследовательских организаций (для большинства терминов доля знающих в НИИ выше, чем в вузах и организациях неакадемического сектора). Лучше знакомы с цифровой терминологией молодые ученые: разница в уровне знаний между группой в возрасте до 29 лет и средним значением по всей выборке по отдельным технологиям достигает 10–15 п.п. В условиях цифровой экономики владение продвинутыми цифровыми навыками (способность быстро осваивать новые IT-инструменты и навыки программирования) становится актуальным, например, для маркетологов (в целях оптимизации управления рекламой и прогнозирования эмоциональной реакции пользователей на рекламу), юристов (для автоматизации анализа материалов, подготовки к судебному процессу и т.д.), геологов (для картирования сложных месторождений полезных ископаемых, анализа сейсмических данных) и многих других специалистов. Для инженеров профессиональные цифровые навыки, прежде всего программирование, являются неотъемлемой частью требуемого работодателем набора навыков. Во всех отраслях экономики ожидается стремительный рост спроса на специалистов по данным (data scientists), способных структурировать данные и извлекать из них добавленную стоимость. Их ключевые востребованные компетенции: глубокое понимание математической статистики, теории вероятностей, аналитические способности, навыки решения нестандартных задач, умение эффективно представить результаты работы, любознательность и склонность к работе с данными. Профессия исследователя данных становится межотраслевой, и характерные для нее навыки придется осваивать широкому кругу специалистов. Поскольку инструментарий киберпреступников непрерывно эволюционирует, становится более изощренным и сложным, то усиливается спрос на специалистов в области кибербезопасности.

Задание №3.

Составьте деловое письмо-предложение о сотрудничестве (внедрение РПА-роботов в банк) с учетом социокультурных особенностей потенциальных клиентов (Казахстан).

Задание №4.

Прочтите и переведите текст устно.

It can be argued that Digital is the same as IT or software project management. In fact, as we mentioned above, the many different understandings of the term have led certain individuals to use the three project management fields interchangeably.

And in many ways, the three namely digital, IT, and software project management are similar if not the same.

Project management in the digital sense can be seen as a spin-off or type of the other two, software and IT project management. With digital being more specific in context. This specific context is often marketing related.

Project management in the digital sense can be seen the have a faster turnaround and smaller budgets than the other two. The projects also often have a direct consumer focus.

With digital agencies focusing more often on focusing on strategy, advertising, communications, or marketing projects.

Digital and IT project management both can deal with projects that have large, technical, and complex builds. The latter deals more typically with larger-scale budgets and are often into the more hardcore enterprise market.

Software project management deals with project management aspects related to software and web projects. Project management in software engineering does however have a unique lifecycle process. This process requires numerous rounds of testing, updating, as well as customer feedback.

Задание № 5. Переведите текст на русский язык письменно.

Artificial intelligence (AI) is intelligence demonstrated by machines, unlike the natural intelligence displayed by humans and animals, which involves consciousness and emotionality. The distinction between the former and the latter categories is often revealed by the acronym chosen. 'Strong' AI is usually labelled as artificial general intelligence (AGI) while attempts to emulate 'natural' intelligence have been called artificial biological intelligence (ABI). Leading AI textbooks define the field as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of achieving its goals. Colloquially, the term "artificial intelligence" is often used to describe machines that mimic "cognitive" functions that humans associate with the human mind, such as "learning" and "problem solving".

As machines become increasingly capable, tasks considered to require "intelligence" are often removed from the definition of AI, a phenomenon known as the AI effect. A quip in Tesler's Theorem says "AI is whatever hasn't been done yet." For instance, optical character recognition is frequently excluded from things considered to be AI, having become a routine technology. Modern machine capabilities generally classified as AI include successfully understanding human speech, competing at the highest level in strategic game systems (such as chess and Go),]and also imperfect-information games like poker, self-driving cars, intelligent routing in content delivery networks, and military simulations.

Artificial intelligence was founded as an academic discipline in 1955, and in the years since has experienced several waves of optimism,] followed by disappointment and the loss of funding (known as an "AI winter"), followed by new approaches, success and renewed funding.] After AlphaGo defeated a professional Go player in 2015, artificial intelligence once again attracted widespread global attention. For most of its history, AI research has been divided into sub-fields that often fail to communicate with each other.] These sub-fields are based on technical considerations, such as particular goals (e.g. "robotics" or "machine learning")] the use of particular tools ("logic" or artificial neural networks), or deep philosophical differences.] Sub-fields have also been

based on social factors (particular institutions or the work of particular researchers).

Задание №6.

Переведите текст на английский язык письменно.

Техническая основа ИТ и ИС управления представлена совокупностью взаимосвязанных единым управлением автономных технических средств сбора, накопления, обработки, передачи, вывода и представления информации, средств обработки документов и оргтехники, а также средств связи для осуществления информационного обмена между различными техническими средствами. Достижение эффективной работы ИС предполагает выполнение некоторого набора требований, предъявляемых к комплексу технических средств (КТС), основными из которых являются следующие:

• минимизация трудовых и стоимостных затрат на решение всего комплекса задач системы;

• реализация интегрированной обработки информации за счет информационной, технической и программной совместимости различных технических устройств;

• обеспечение пользователей связью через терминальные устройства с распределенной базой данных; высокая надежность;

• наличие защиты информации от несанкционированного доступа;

• реализуемость КТС, т.е. возможность его создания за счет типовых средств, выпускаемых отечественной промышленностью;

• гибкость структуры КТС, т.е. перспектива включения в его состав новых, более совершенных технических средств по мере освоения их промышленностью;

• минимизация капитальных затрат на приобретение КТС и их текущую эксплуатацию.

Эффективное функционирование ИС базируется на комплексном использовании современных технических средств обработки информации и методов организации технологических процессов решения задач. Основой дальнейшего развития автоматизации управленческой деятельности в различных отраслях экономики является новая, прогрессивная информационная технология, ориентированная на использование последних достижений электронной техники, в частности, высокопроизводительных, быстродействующих компьютеров и современных средств связи. Создание новой технологии требует учета особенностей структуры экономических систем.

Задание №7.

Составьте ответ на деловое письмо-предложение услуг компании в области внедрения ИС в поликлинике в соответствии с нормами письменного этикета английского языка.

Задание №8.

Письменно подготовьте презентацию цифрового аналитического сервиса с применением технологий искусственного интеллекта (предназначен для выявления и анализа долгосрочных отраслевых и кроссотраслевых трендов) с сфере телекоммуникаций.

Задание №9. Перескажите текст на английском языке.

Проблематика машинного обучения касается процесса самостоятельного получения знаний интеллектуальной системой в процессе её работы. Это направление было центральным с самого начала развития ИИ. В 1956 году, на Дартмундской летней конференции, Рей Соломонофф написал отчёт о вероятностной машине, обучающейся без учителя, назвав её: «Индуктивная машина вывода».

Обучение без учителя — позволяет распознать образы во входном потоке. Обучение с учителем включает также классификацию и регрессионный анализ. Классификация используется, чтобы определить, к какой категории принадлежит образ. Регрессионный анализ используется, чтобы в рядах числовых примеров входа/выхода и обнаружить непрерывную функцию, на основании которой можно было бы прогнозировать выход. При обучении агент вознаграждается за хорошие ответы и наказывается за плохие. Они могут быть проанализированы с точки зрения теории решений, используя такие понятия как полезность. Математический анализ машинных алгоритмов изучения — это раздел теоретической информатики, известный как вычислительная теория обучения (англ. Computational learning theory).

К области машинного обучения относится большой класс задач на распознавание образов. Например, это распознавание символов, рукописного текста, речи, анализ текстов. Многие задачи успешно решаются с помощью биологического моделирования (см. след. пункт). Особо стоит упомянуть компьютерное зрение, которое связано ещё и с робототехникой.

Задание №10. Переведите текст на русский язык устно.

A scanner is a peripheral that reads images and converts them into electronic codes which can be understood by a computer. The paper with the image is placed face down on a glass screen, as with a photocopier. Beneath the glass are the lighting and measurement devices. Once the scanner is activated, it reads the image as a series of dots and then generates the digitized image that is sent to the computer and stored as a file. The scanner operates by using three rotating lamps, each of which has a different coloured filter: red, green and blue. The resulting three separate images are combined into one by appropriate software.

There are different types of scanners: Image scanner, which digitizes a two-dimensional image. 3D scanner, which digitizes the three-dimensional shape of a real object. Motion picture film scanner, which scans original film for storage

as a digital file. Laser scanner, which guides a laser beam along a path, sometimes combined with a measurement. Stepper is a part of the photolithography process. A biometric scanner is an electronic device with a sensor to read patterns or images from faces, irises and finger pads to create

a biological template or profile. Flatbed is built like a photocopier and is for use on a desktop; it can capture text, colour images and even small 3D objects.

A flatbed scanner is an optical scanner which makes use of a flat surface for scanning documents. The scanner is capable of capturing all elements on the document and does not require movement of the document. Flatbed scanners are effective scanners for delicate materials such as vintage photographs, papers and other documents which are fragile

Задание №11.

Подготовьте устную презентацию CMS WordPress используя необходимый лингвистический инструментарий изучаемого языка.

Задание №12.

Письменно подготовьте презентацию операционной системы Lunix используя необходимый лингвистический инструментарий изучаемого языка.

Задание №13. Перескажите текст на английском языке.

Быстро развивающаяся область электроники привела к созданию первого универсального электронного компьютера в 1946 году в Университете штата Пенсильвания Это был электронный числовой интегратор и компьютер, или ЭНИ-АК, устройство содержало 18 000 вакуумных ламп, а его скорость была несколько миллионов математических операций в минуту. Его программа была записана на процессоре и изменялась вручную.

Позже появились транзисторы. Это способствовало появлению меньших по размеру, более быстрых элементов, которые невозможно было создать с помощью ламповых машин. Поскольку транзисторы используют намного меньше электроэнергии и имеют намного более длинный срок службы, сами компьютеры стали более совершенными. Если не принимать во внимание размер и форму, все современные цифровые вычислительные машины созданы на основе одной и той же концепции. Однако, исходя из их стоимости и характеристик, они могут быть разделены на несколько категорий. Первая категория — это персональный компьютер, или микрокомпьютер, — относительно дешевая машина, обычно настольного размера. Некоторые называют их лэптопами- Он достаточно малого размера, чтобы поместиться в портфель. Вторая категория — автоматизированное рабочее место, микрокомпьютер с улучшенной графикой и способностями для обмена информацией, что делает его особенно полезным для работы в офисе. И третья категория —

компьютеры-серверы, мощная, дорогостоящая машина с ресурсом обслуживания потребностей больших предприятий, ведомств, научных исследовательских учреждений. Самые большие и мощные из них называются суперкомпьютерами.

Говоря р центральном вычислительном устройстве, или сердце компьютера, я хотел бы добавить, что существовало несколько поколений микропроцессоров. Первое поколение было представлено вычислительным устройством Intel 8086. Второе поколение было представлено вычислительным устройством Intel 80286, которое использовалось в компьютере IBM PC AT 286. Третье поколение было представлено процессором Intel 80386, который использовался в компьютере IBM PC AT 386. Микропроцессоры четвертого поколения использовались в компьютерах IBM PC AT 486. Также существуют процессоры пятого поколения, используемые в компьютерах Пентиум 60 и Пентиум 66, центральные вычислительные устройства шестого поколения, которые использовались в компьютерах Пентиум 75, 90,100 и 133. Несколько лет назад появились процессоры седьмого и восьмого поколений.

Задание №14

Подготовьте презентацию CMS Joomla.

Задание №8

Подготовьте письменный перевод текста.

По мере развития ИИ от исследовательских лабораторий и офисных отделов ИТ до популярной технологии люди и машины начинают сотрудничать более тесно, а возможности трансформации, которые ИИ обеспечивает бизнесу и обществу, огромны. Некоторые отрасли, рынки и отдельные компании продвинулись дальше других, однако некоторые останутся позади. Сейчас самое начало пути, перед каждым открыто множество возможностей. В конце концов, интеллектуальную экономику будут составлять интеллектуальные компании, и, независимо от размера и географического положения, каждая организация получит возможность вырваться вперед в этом соревновании. Успешные компании, возможно, выделят следующие подходы: Эксперимент. Подход, основанный на определении небольших быстрых побед, заложит основу внедрения инноваций и реализации стратегий по устранению рисков для более масштабного развертывания в будущем. Организации будут обращаться к ИИ, чтобы лучше понять нужды клиентов и граждан, а затем разрабатывать новые продукты, службы и бизнес-модели, которые отличаются большей устойчивостью к неопределенностям будущей экономики и нарушениям конкурентоспособности. Повышение квалификации. Сотрудники, которые четко понимают преимущества ИИ для себя и обладают навыками, нужными для максимально эффективного использования этой технологии, получат новые возможности не только для увеличения производительности, но и для карьерного роста.

Предусмотрительные работодатели предоставят возможности обучения и развития соответственно. Управление. Организации в частном и государственном секторах создадут соответствующие механизмы управления и контроля для оценки социального влияния ИИ. Они будут уделять особое внимание укреплению доверия к решениям на базе ИИ, обеспечивая надежность и беспристрастность лежащей в основе алгоритмов логики, которую при этом можно будет легко объяснить клиентам, сотрудникам и надзорным органам. Таким образом бизнес-лидеры могут внести собственный вклад в построение завтрашней интеллектуальной экономики не только в своих интересах, но и в интересах своих сотрудников и общества в целом.

Задание №15

Переведите на русский язык.

Since its beginning, artificial intelligence has come under scrutiny from scientists and the public alike. One common theme is the idea that machines will become so highly developed that humans will not be able to keep up and they will take off on their own, redesigning themselves at an exponential rate.

Another is that machines can hack into people's privacy and even be weaponized. Other arguments debate the ethics of artificial intelligence and whether intelligent systems such as robots should be treated with the same rights as humans.

Self-driving cars have been fairly controversial as their machines tend to be designed for the lowest possible risk and the least casualties. If presented with a scenario of colliding with one person or another at the same time, these cars would calculate the option that would cause the least amount of damage.

Another contentious issue many people have with artificial intelligence is how it may affect human employment. With many industries looking to automate certain jobs through the use of intelligent machinery, there is a concern that people would be pushed out of the workforce. Self-driving cars may remove the need for taxis and car-share programs, while manufacturers may easily replace human labor with machines, making people's skills more obsolete.

Задание №16. Переведите на английский язык.

Начиная с 2000-х годов ИКТ входят в круг приоритетных направлений государственной политики в России. Еще в 2002 г. была принята федеральная целевая программа «Электронная Россия (2002–2010 годы)». На смену ей пришла государственная программа «Информационное общество (2011–2020 годы)». В 2008 г. была принята Стратегия развития информационного общества в Российской Федерации. Действовавшие до 2019 г. инструменты поддержки можно отнести к двум группам. Во-первых, это меры поддержки «традиционных» цифровых технологий и закупки готовых решений в госсекторе (электронные правительство, госуслуги и др.), а также обеспечение развития

информационной инфраструктуры и широкополосного доступа к сети Интернет (для социально значимых объектов, малых населенных пунктов). Во-вторых, это множество мер прямой финансовой поддержки разработки и внедрения ИКТ в рамках научно-технической и инновационной политики. К началу 2019 г. их насчитывалось около 30 — преимущественно гранты и субсидии разработчикам технологий, венчурные инвестиции и льготные займы. Часть мер прямо фокусируется на цифровых технологиях, многие из них введены в течение последних двух-трех лет в связи с усилением «цифровой повестки», а также запуском Национальной технологической инициативы, в рамках ко- 57 торой определены сквозные технологии (для нескольких рынков), практически полностью совпадающие со сквозными цифровыми технологиями национальной программы «Цифровая экономика Российской Федерации». Многие другие меры позволяют поддерживать цифровые технологии в составе более широкого спектра тематик. 71. Запуск национальной программы «Цифровая экономика Российской Федерации» и включение ускоренного внедрения цифровых технологий в число национальных целей развития до 2024 г. согласно Указу № 204 подняли цифровую повестку на самый высокий политический уровень. Более того, это один из первых примеров национальных целей, реализуемых на основе принципов проектного управления и подкрепленных значительными дополнительными бюджетными средствами (410 млрд руб. средств федерального бюджета и около 535 млрд руб. внебюджетных средств на 2019–2021 гг.).

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Планирование эксперимента и обработка данных»

Направление подготовки:10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 6

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 8

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 12

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Планирование эксперимента и обработка данных» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе в 1 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование знаний, умений и навыков в решении задач планирования научного эксперимента.

Задачи изучения дисциплины:

– освоение специфической терминологии математической теории планирования эксперимента;

– развитие навыков построения математических моделей сложных стохастических систем, оценки их статистической достоверности и интерпретации;

– практическое использование полученных математических моделей для оптимизации принимаемых решений безопасности автоматизированных систем.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	**ОПК-4**	ОПК-4.1. Знать: основные перспективы развития науки и техники в области профессиональной деятельности для проведения научных исследований и разработок; методы отыскания оптимальных решений.	принципы, методы и средства сбора, обработки и анализа профессиональной информации	осуществлять сбор научнотехнической информации по теме исследования, обрабатывать и анализировать собранную информацию, выделять в ней главное	методикой сбора, обработки и анализа профессиональной информации	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа
		ОПК-4.2. Уметь: осуществлять анализ источников научно-технической информации с целью дальнейшего применения в рамках исследования; применять на практике различные виды обработки данных.	теоретические основы подготовки планов и программ проведения научных исследований и технических разработок	разрабатывать планы и программы проведения научных исследований и технических разработок	методикой подготовки планов и программ проведения научных исследований и технических разработок	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа
Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	**ОПК-5**	ОПК-5.1. Знать: логические методы и приемы научного исследования; о видах экспериментов и методах обработки данных; методы анализа, синтеза, способы математического моделирования в области исследований и разработок, в том числе, организации современных систем управления.	современные инструменты и методы для проведения научных исследований	выбирать современные инструменты и методы для проведения научных исследований	методикой применения на практике современных инструментов и методов для проведения научных исследований	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа

		ОПК-5.2. Уметь: осуществлять методологическое обоснование научного исследования; применять на практике различные виды обработки данных.	порядок, правила составления оформления и представления научно-технических отчетов, обзоров, научных докладов и статей	оформлять и представлять научно-технические отчеты, обзоры, научные доклады и статьи	навыками оформления и представления научно-технической документации, научных докладов и статей	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Введение в теорию планирования эксперимента	4	5				5				10	Лабораторный практикум/15
Тема 2. Регрессионный анализ. Разложение функции отклика в степенной ряд, кодирование факторов	4	5								10	Контрольная работа/25
Тема 3. Планы первого порядка	5	5				6				10	Лабораторный практикум/15
Тема 4. Обработка экспериментальных данных	5	5				6				10	Лабораторный практикум/15
Тема 5. Крутое восхождение по поверхности отклика	5	4				6				10	Лабораторный практикум/15
Тема 6. Планы второго порядка	5	4				5				10	Лабораторный практикум/15
Всего:	**28**	**28**				**28**				**60**	**100**
Контроль, час											**100 Зачет**
Объем дисциплины (в академических часах)	**144**										
Объем дисциплины (в зачетных единицах)	**4**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Введение в теорию планирования эксперимента

Введение в теорию планирования эксперимента. Особенности использования результатов эксперимента при решении научных и прикладных задач. Основные понятия и определения теории планирования эксперимента. Факторы и факторное пространство. Функция отклика и поверхность отклика. Разложение функции отклика в степенной ряд. Активный и пассивный эксперимент. Основные принципы планирования эксперимента.

Тема 2. Регрессионный анализ. Разложение функции отклика в степенной ряд, кодирование факторов

Основные понятия математической статистики. Основные понятия регрессионного анализа. Метод наименьших квадратов. Кодирование факторов (нормирование значений факторов). Центр эксперимента. Матричные преобразования при обработке результатов эксперимента. Факторное пространство. Опыт. Матрица эксперимента. Примеры.

Тема 3. Планы первого порядка

Планы первого порядка. Назначение и особенности планов первого порядка. Полный факторный эксперимент. Матрица планирования эксперимента и способы её построения. Свойства матрицы планирования полного факторного эксперимента. Избыточность полного факторного эксперимента. Дробный факторный эксперимент. Дробные реплики. Матрица планирования дробного факторного эксперимента и способы её построения. Смешанные оценки. Разрешающая способность реплики. Генерирующее соотношение и определяющий контраст. Принципы выбора генерирующего соотношения. Реплики высокой дробности. Обобщающий определяющий контраст. Минимально допустимая степень дробности реплики. Линейные насыщенные планы. Сравнительная характеристика планов первого порядка.

Тема 4. Обработка экспериментальных данных

Погрешности измерений. Причины возникновения и классификация погрешностей. Случайная величина. Числовые характеристики случайной величины. Законы распределения случайной величины. Нормальный закон распределения и его параметры. Дублирование опытов. Общая схема обработки результатов при дублировании опытов. Алгоритм обработки результатов при равномерном дублировании. Алгоритм обработки результатов при неравномерном дублировании. Алгоритм обработки результатов при отсутствии дублирования. Выявление резко выделяющихся результатов. Уровень значимости. Оценка однородности ряда дисперсий. Критерии Фишера, Кохрена, Бартлетта. Оценка уравнения регрессии методом наименьших квадратов. Оценка значимости коэффициентов. t-критерий Стьюдента. Оценка адекватности модели. Возможные причины неадекватности модели и

способы их устранения.

Тема 5. Крутое восхождение по поверхности отклика

Оптимизация, постановка задачи, основные понятия, классификация методов оптимизации. Задача оптимизации в экспериментальных исследованиях. Планирование экстремальных экспериментов. Градиентные и неградиентные методы поиска. Симплексный метод поиска. Метод крутого восхождения по поверхности отклика. Примеры.

Тема 6. Планы второго порядка

Планы второго порядка. Оценка значимости квадратичных членов. Назначение и классификация планов второго порядка. Симметричные планы второго порядка. Несимметричные планы второго порядка. Центральные композиционные планы. Способы построения центральных композиционных планов. Звёздные точки. Ортогональный центральный композиционный план (ОЦКП). Способы построения и свойства матрицы планирования ОЦКП. Определение параметров ОЦКП. Ротатабельный ортогональный центральный композиционный план (РОЦКП). Матрица планирования РОЦКП. Определение параметров РОЦКП. Ротатабельный центральный композиционный план (РЦКП). Способы построения и свойства матрицы планирования РЦКП. Определение параметров РЦКП. Униформ-ротатабельное планирование. Планы второго порядка с единичной областью планирования. Сравнительная характеристика планов второго порядка.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Солдатов, А. А. Методы обработки экспериментальных данных : учебное пособие / А. А. Солдатов. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2024. — 108 с. — ISBN 978-5-7262-3035-1. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/141180/details

2. Мойзес, Б. Б. Статистические методы контроля качества и обработка экспериментальных данных : учебное пособие / Б. Б. Мойзес, И. В. Плотникова, Л. А. Редько ; под редакцией Б. И. Капранова. — 2-е изд.. — Москва : Ай Пи Ар Медиа, 2024. — 118 с. — ISBN 978-5-4497-1238-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/147299/details

Дополнительная литература:

1. Хохлов, С. С. Основные методы анализа экспериментальных данных : учебное пособие / С. С. Хохлов, А. Н. Дмитриева. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2025. — 126 с. — ISBN 978-5-7262-3149-5. — Текст : электронный //

Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/156787/details

2. Методы обработки экспериментальных данных : учебное пособие / С. А. Гордин, А. А. Соснин, И. В. Зайченко, В. Д. Бердоносов ; под редакцией С. А. Гордина. — Комсомольск-на-Амуре : Комсомольский-на-Амуре государственный университет, 2022. — 75 с. — ISBN 978-5-7765-1501-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/122763/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Бурумов В.А. Программа обработки и графического анализа многопараметрических экспериментальных данных	https://elibrary.ru/item.asp?id=89290223
2	Вишняков В.И. Программный комплекс для сбора и обработки экспериментальных данных	https://elibrary.ru/item.asp?id=76405996
3	Иванищев Ю.Г., Давыдов В.М. Планирование эксперимента и автоматизированная обработка данных	https://elibrary.ru/item.asp?id=69214700

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информационных технологий для проведения лабораторных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование: оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	15-13 – работа выполнена в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы; 12-10 – работа выполнена в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 9-7 – работа выполнена в срок, в основном самостоятельно, использованы соответствующие формулы; определены соответствующие спецификации, имеются ошибки в расчетах; выбраны совместимые комплектующие необходимые, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 6-4 – обучающийся подготовил работу несамостоятельно или не завершил в срок, описание спецификации содержит незначительные ошибки, выводы и ответы на вопросы отсутствуют.
2.	Контрольная работа	25-20 – верные ответы составляют более 90% от общего количества; 19-14 – верные ответы составляют 80-50% от общего количества; 13-0 – менее 50% правильных ответов.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые задания к лабораторным практикумам

1. Планирование активного эксперимента

Разработать приложение с графическим интерфейсом, позволяющее вычислять время переходного процесса для заданной динамической системы, отображать полученный результат на графике и сохранять полученные результаты в файл.

2. Полный факторный эксперимент

Сформировать план полного факторного эксперимента и получить с его помощью факторную модель в предположении, что величина функции отклика известна абсолютно точно.

3. Обработка результатов при равномерном дублировании

Построить факторную модель при равномерном дублировании опытов.

4. Обработка результатов при неравномерном дублировании

Построить факторную модель при неравномерном дублировании опытов.

5. Дробный факторный эксперимент

Сформировать план дробного факторного эксперимента и получить с его помощью факторную модель

6. Ортогональный центральный композиционный план

Сформировать ортогональный центральный композиционный план и получить с его помощью факторную модель.

Типовые задания для контрольной работы

1. Процедура выбора числа и условий проведения опытов, необходимых и достаточных для построения факторной модели это

1) методика, 2) методология, 3) планирование эксперимента, 4) программа.

2. Матрица планирования эксперимента - это ...

1) таблица, обеспечивающая рандомизацию экспериментальных исследований, 2) таблица, задающая общее число экспериментов, 3) таблица, задающая последовательность проведения отдельных экспериментов, 4) таблица, включающая условия проведения отдельных экспериментов.

3. Критерий Фишера используется для оценки…

1) оценки значимости коэффициентов факторной модели, 2) оценки однородности дисперсий, 3) оценки адекватности факторной модели.

4. Критерий Кохрена используется для…

1) оценки значимости коэффициентов факторной модели, 2) оценки однородности дисперсий, 3) оценки адекватности факторной модели.

5. Определить коэффициенты линейной регрессии: $y = a_o + a_1 x$ методом наименьших квадратов для экспериментальных данных.

6. Дана таблица значений функции y=f(x). Используя метод наименьших квадратов, подобрать для заданных значений x и y линейную функцию квадратичную функцию y=a0+a1*x+a2*x*x. Построить график этой функции.

7. С помощью полного факторного эксперимента найти математическое описание некоторого процесса, в котором осуществлялось измерение y, зависящего от двух факторов x1 и x2 (%) в окрестности точки факторного пространства с координатами: x01 и x02. Результаты измерений y приведены в таблице.

8. Даны значения функции отклика для ПФЭ 2^2 (y1=5, y1=10, y1=7, y1=12). Построить матрицу планирования эксперимента, найти коэффициенты линейной регрессии, оценить их значимость и проверить модель на адекватность.

9. Осуществить проверку правильности выполненных расчетов средствами пакета Matlab.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	Критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов «Зачтено» – 90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Классификация математических моделей.
2. Построение математической модели на основе экспериментальных данных. Факторная модель.
3. Пассивный эксперимент. Активный эксперимент.
4. Нормирование факторов.
5. Полный факторный эксперимент.
6. Свойства матрицы планирования полного факторного эксперимента. Геометрическая интерпретация полного
факторного эксперимента. Коэффициенты модели при полном факторном эксперименте.
7. Эффекты взаимодействия факторов.
8. Дробный факторный эксперимент. Особенности дробного факторного эксперимента.
9. Регулярные и нерегулярные реплики.
10. Смешанные оценки. Генерирующее соотношение и определяющий контраст.
11. Разрешающая способность реплики.
12. Коэффициенты модели при дробном факторном эксперименте.
13. Реплики высокой дробности. Обобщающий определяющий контраст.
14. Метод крутого восхождения по поверхности отклика.
15. Планы второго порядка.
16. Центральные композиционные планы.
17. Ортогональный центральный композиционный план. Параметры ортогонального центрального
композиционного плана. Коэффициенты модели для ортогонального центрального композиционного плана.
18. Ротатабельный ортогональный центральный композиционный план. Параметры ротатабельного ортогонального центрального композиционного плана. Коэффициенты модели для ротатабельного
ортогонального центрального композиционного плана.
19. Ротатабельный центральный композиционный план. Параметры ротатабельного центрального
композиционного плана. Коэффициенты модели для ротатабельного центрального композиционного плана.
20. Причины возникновения погрешностей при активном эксперименте.
21. Классификация погрешностей.
22. Дублирование опытов.
23. Обработка результатов эксперимента при равномерном дублировании опытов.
24. Обработка результатов эксперимента при неравномерном дублировании опытов.

25. Обработка результатов эксперимента при отсутствии дублирования опытов.
26. Выявление промахов.
27. Критерии однородности дисперсий.
28. Оценка значимости коэффициентов модели.
29. Проверка адекватности факторной модели.
30. Возможные причины неадекватности модели и способы их устранения.

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Обеспечение безопасности компьютерных систем»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 7

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Обеспечение безопасности компьютерных систем» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе в 1 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование компетенций по основным разделам теоретических и практических основ безопасности компьютерных систем, получение опыта противодействия киберугрозам, практических навыков в различных областях информационной безопасности, таких как: анализ защищенности, расследование инцидента и устранение уязвимостей.

Задачи изучения дисциплины:

– изучение методов реверс-инжиниринга;

– ознакомление со способами анализа действий злоумышленников;

– ознакомление с методами устранения уязвимостей;

– изучение методов защиты серверов с запущенными веб-приложениями от множественных атак;

– изучение принципов выявления уязвимых мест путем атак.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	**ОПК-1**	ОПК-1.1. Знать: принципы функционирования автоматизированных систем, в том числе поддержки документооборота, и обеспечения их безопасности; методы и средства управления информационной безопасностью; содержание нормативных документов, регламентирующих требования к системе обеспечения информационной безопасности.	методы и средства управления информационной безопасностью; содержание нормативных документов. регламентирующих требования к системе обеспечения информационной безопасности	проводить оценку соответствия объекта требованиям нормативных документов и стандартам по информационной безопасности	анализа и подготовки содержания нормативно-распорядительных и иных документов для обоснования и поддержки безопасного функционирования объектов; разработки требований информационной безопасности к объектам информатизации	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Информационная безопасность в системе национальной безопасности РФ	3	4				4				7	Контрольная работа/13
Тема 2. Расчет вероятности проникновения злоумышленника на объект хранения информации	4	3				3				8	Контрольная работа/12
Тема 3. Понятие угрозы безопасности информации, коррелирующие с этим понятием термины	3	4				4				7	Контрольная работа/13
Тема 4. Модели дискреционного управления доступом Харрисона-РуззоУльмана.Модель доступа БеллаЛаПаддула	4	3				3				8	Контрольная работа/12
Тема 5. Построение систем защиты от угроз нарушения конфиденциальности информации.	3	4				4				7	Контрольная работа/13
Тема 6. Развертывание SNS в автономном режиме	4	3				3				8	Контрольная работа/12
Тема 7. Построение систем защиты от угроз нарушения целостности	3	4				4				7	Контрольная работа/13
Тема 8. Установка СУБД Microsoft SQL	4	3				3				8	Контрольная работа/12

Server											
Всего:	**28**	**28**				**28**				**60**	**100**
Контроль, час											**100** **Зачет**
Объем дисциплины (в академических часах)	**144**										
Объем дисциплины (в зачетных единицах)	**4**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Информационная безопасность в системе национальной безопасности РФ

Понятие государственной тайны и иных охраняемых законом тайн, сведений конфиденциального характера.

Тема 2. Расчет вероятности проникновения злоумышленника на объект хранения информации

Преобразование аналоговых телефонных сообщений (скремблеры)

Тема 3. Понятие угрозы безопасности информации, коррелирующие с этим понятием термины

Основные меры противодействия угрозам безопасности (методы защиты информации) и их классификация.

Тема 4. Модели дискреционного управления доступом Харрисона-Руззо Ульмана. Модель доступа Белла Ла Паддула

Описание моделей. Программная реализация моделей.

Тема 5. Построение систем защиты от угроз нарушения конфиденциальности информации.

Криптографические методы обеспечения конфиденциальности информации

Тема 6. Развертывание SNS в автономном режиме

Подготовка к централизованному развертыванию SNS

Тема 7. Построение систем защиты от угроз нарушения целостности

Схема системы защиты от угроз нарушения доступности. Организационные меры защиты информации в компьютерных системах

Тема 8. Установка СУБД Microsoft SQL Server

Установка сервера. Развертывание инструментов управления

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Макаренко, С. И. Защита компьютерных сетей и телекоммуникаций : учебное пособие / С. И. Макаренко. — Санкт-Петербург : Наукоемкие технологии, 2024. — 312 с. — ISBN 978-5-907618-79-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/157433/details

2. Полтавцева, М. А. Организационные и правовые аспекты информационной безопасности : учебное пособие / М. А. Полтавцева. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2023. — 145 с. — ISBN 978-5-7422-8431-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/147727/details

Дополнительная литература:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд.. — Саратов : Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/145912/details

2. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 3-е изд.. — Саратов : Профобразование, 2024. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/145909/details

3. Джонс, К. Д. Инструментальные средства обеспечения безопасности : учебное пособие / К. Д. Джонс, М. Шема, Б. С. Джонсон. — 4-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 913 с. — ISBN 978-5-4497-0871-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/146346/details

4. Басыня, Е. А. Сетевая информационная безопасность : учебник / Е. А. Басыня. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/132693/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Ассоциация по вопросам защиты информации	http://bis-expert.ru/
4	Сметанкина Г.И., Дорохов И.А. К вопросу о создании системы обеспечения информационной безопасности компьютерной сети	https://elibrary.ru/item.asp?id=67289201
5	Официальный сайт Лаборатории Касперского	http://www.kaspersky.ru/
6	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/
7	Официальный сайт журнала «Информационная безопасность»	http://www.itsec.ru/main.php

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного

оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория Схемотехники

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; учебно-лабораторные стенды и контрольно-измерительная аппаратура для измерения частотных свойств, форм и временных характеристик сигналов, средства для измерения параметров электрических цепей, средства генерирования сигналов, TBS1072C, Осциллограф цифровой, 2 канала х 70 МГц (Госреестр РФ)

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Лаборатория сетей и систем передачи информации

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; оснащена рабочими местами на базе вычислительной техники, стендами сетей передачи информации с коммутацией пакетов и коммутацией каналов, структурированной кабельной системой, стойками с телекоммуникационным оборудованием, системой питания и вентиляции, эмулятором (эмуляторами) активного сетевого оборудования, специализированным программным обеспечением для настройки телекоммуникационного оборудования, (стендами для исследования параметров сетевого трафика

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Лаборатория технической защиты информации

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; оснащена специализированным оборудованием по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам; системой виброакустической защиты "Гамма СВАЗ-01", ПЭВМ «Secret»

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к

сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Контрольная работа	12-11/13-11 – верные ответы составляют более 90% от общего количества; 10-7 – верные ответы составляют 80-50% от общего количества; 6-0 – менее 50% правильных ответов.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

<u>Типовые задания для контрольной работы</u>

1. Не подлежит отнесению к конфиденциальной информации: (Выберите 2 и более ответов)

1) информация, касающаяся актов, затрагивающих права, свободы и обязанности человека и гражданина;

2) сведения о состоянии окружающей среды;

3) информация о деятельности государственных органов и органов местного самоуправления;

4) сведения и документы как полученные, так и составленные в рамках аудиторской деятельности;

5) сведения, которые стали известны нотариусу в связи с осуществлением им профессиональной деятельности.

2. Соотнесите определения и понятия, к которым они относятся (ГОСТ ИСО/МЭК 13335-1):

1) Угроза

2) Инцидент ИБ

А) любое непредвиденное или нежелательное событие, которое может нарушить деятельность организации или информационную безопасность: нарушение правил доступа, физических мер защиты, сбои ПО, отказы ТС, утрата услуг и т.д.

Б) потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьимлибо интересам в рамках информационного процесса

3. Поставьте в соответствие классификационные признаки и

соответствующие им типы угроз информационной безопасности автоматизированных систем (АС):

1) По способу доступа к ресурсам АС

2) По конечному результату реализации угрозы

3) По степени (характеру) воздействия на АС

А) активные

Б) несанкционированное получение пароля путём подкупа, шантажа, угроз или физического насилия по отношению к законному обладателю.

В) Угрозы нарушения целостности информации, к которым относится любое злонамеренное искажение информации, обрабатываемой с использованием АС

Г) пассивные

Д) Угрозы нарушения доступности информации, возникающие в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется.

Е) использование недекларированных возможностей средств защиты.

4. Распределите примеры средств и систем по группам:

А) основные технические средства и системы;

Б) вспомогательные технические средства и системы

1) средства вычислительной техники, обрабатывающие конфиденциальную информацию,

2) средства и системы охранной и пожарной сигнализации;

3) информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи защищаемых

данных,ПО, отказы ТС, утрата услуг и т.д.

4) технические средства приема, передачи и обработки конфиденциальной информации;

5) контрольно-измерительная аппаратура;

6) средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения

5. Соотнесите определения и понятия, к которым они относятся:

А) идентификация

Б) аутентификация

В) авторизация

1) процесс распознавания субъектов путем проверки принадлежности субъекту доступа предъявленного им

идентификатора и подтверждение его подлинности

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета

Краткая характеристика оценочного средства	Критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов «Зачтено» – 90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Что такое информация, субъекты информационных отношений?
2. Компьютерная система-это…
3. Раскройте терм информационная безопасность
4. Что такое информационная безопасность компьютерных систем?
5. Понятия ущерба, риска и угрозы.
6. Что такое уязвимость?
7. Какую информацию относят к секретной, конфиденциальной?
8. Что такое система физической защиты объекта?
9. Какие требования предъявляются к комплексной системе безопасности объекта?
10. Аналоговый, дискретный сигнал.
11. Спектр. Спектр аналогового и дискретного сигнала.
12. Скремблер. Принцип действия скремблера.
13. Условие для выбора n (число мелких интервалов в пределах T).
14. Виды скремблирования. Достоинства и недостатки.
15. Полосовой фильтр. Как он используется при скремблировании, в каком из видов скремблирования.
16. Инверсия частотного спектра сообщения. Для чего применяется?
17. Какие модели доступа Вам известны? Раскройте их сущность.
18. К каким криптосистемам относится данный шифр?
19. Алгоритм шифрования по данному методу.
20. Какие организационные меры обеспечения безопасности Вы знаете?

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины
«Межкультурное взаимодействие в современном мире»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 8

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Межкультурное взаимодействие в современном мире» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе в 1 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование у студентов знаний о взаимодействии и управлении людьми, о методах социальных исследований и навыков их применения в профессиональной деятельности, а также знакомство с исследовательской литературой и информационными ресурсами.

Задачи изучения дисциплины:

– способствовать освоению основных категорий межкультурной коммуникации;

– развивать умение толерантно воспринимать специфику межкультурного разнообразия с соблюдением этических и межкультурных норм с учетом социально-исторического и философского контекста;

–формировать навыки межкультурного взаимодействия на основе анализа философских и исторических фактов, оценки явлений культуры и социальных конфликтов в межкультурной коммуникации.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	**УК-5**	УК-5.2. Уметь обеспечивать и поддерживать взаимопонимание между обучающимися – представителями различных культур и навыки общения в мире культурного многообразия.	закономерности и особенности социально-исторического развития различных культур; особенности межкультурного разнообразия общества; правила и технологии эффективного межкультурного взаимодействия	понимать и толерантно воспринимать межкультурное разнообразие общества; анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	эффективного межкультурного взаимодействия	Контактная работа: Лекции Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Культура и цивилизация	3	4								6	Реферат/13
Тема 2. Типология культуры	4		3							7	Тест/12
Тема 3. Разнообразие культурных форм и сложное строение культуры	3	4								6	Реферат/13
Тема 4. Феномен русской культуры	4		3							7	Тест/12
Тема 5. Освоение культуры: социализация и инкультурация	3	4								6	Реферат/13
Тема 6. Межкультурное взаимодействие в глобализирующемся мире	4		3							7	Тест/12
Тема 7. Этнонациональные особенности межкультурного взаимодействия	3	4								6	Реферат/13
Тема 8. Господствующие в современном мире религиозные системы и их взаимодействие	4		3							7	Тест/12
Всего:	**28**	**16**	**12**							**52**	**100**
Контроль, час											**100 Зачет**
Объем дисциплины (в академических часах)	**108**										
Объем дисциплины (в зачетных единицах)	**3**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Культура и цивилизация

Понятие и сущность культуры. Культура как система, единство образующих ее элементов. Понятие культуры, структура и функции. Деятельностный системный, ценностный подходы. Обыденное понимание культуры. Культура как предмет философского анализа. Культура как универсальная категория. Культура и цивилизация: соотношение понятий и динамика их развития. Понятие «культурное взаимодействие». Основные подходы к понятию цивилизации. Противопоставление культуры и цивилизации. Цивилизация как технологический аспект культуры. Становление и развитие культуры: культурогенез, динамика культуры. Языки, символы, коды культур

Тема 2. Типология культуры

Матриархальные и патриархальные типы культур (И.Я. Бахофен, Л. Фробениус). «Аполлоническое» и «дионисическое» начала в типологии Ф. Ницше. Дихотомия Восток -Запад. Место России в этой системе. Историческая типология культур: глобальная и локальная культуры. Традиционная, индустриальная и постиндустриальная культуры. Постфигуративные, кофигуративные и префигуративные культуры (М. Мид). Высококонтекстные и низкоконтекстные культуры (Эдвард Холл). Моноактивные, полиактивные и реактивные культуры (Р. Льюис). Культурные размерности Г.Хофстеде: индивидуализм коллективизм, избегание неопределенности, дистанция власти, соревновательность (маскулинность), конфуцианский динамизм. Современные психологические исследования индивидуализма-коллективизма в различных культурах.

Тема 3. Разнообразие культурных форм и сложное строение культуры

Феномен массовой культуры. Элитарная и массовая культуры. Доминирующая культура и субкультура. Молодежная культура. Контркультура. Маргинальные культуры. Локальные культуры. Тенденции культурной универсализации в мировом современном процессе.

Тема 4. Феномен русской культуры

Генезис русской культуры: истоки и интенция развития. Проблема власти: идея симфонии духовной и светской власти. Эволюция отечественной культуры в контексте проблемы «Восток – Запад». Духовные искания русского человека. Модернизирующаяся Россия. Национальный эстетический идеал

Тема 5. Освоение культуры: социализация и инкультурация.

Культура и личность. Обучение и научение культуре, социализация и инкультурация. Межпоколенная трансмиссия культуры. Психологические механизмы инкультурации. Влияние социокультурной среды на инкультурацию. Понятие этническая культурная идентичность.

Культурная идентичность. «Свой» и «чужой» в культуре. Этническое сознание и самосознание. Теории этнической идентичности. Структура и формирование этнической идентичности. Кризис и трансформация идентичности. Влияние культурной и этнической идентичности на межкультурную коммуникацию. Аккультурация. Проблемы межкультурного взаимодействия. Механизм развития «культурного шока». Национальные особенности и их учет конфликтной ситуации. Урегулирование этнических конфликтов

Тема 6. Межкультурное взаимодействие в глобализирующемся мире

Сравнительный анализ премодерна, модерна и постмодерна в работах А. Г.Дугина, А. В. Костиной. Э. Тоффлер о ситуации постмодерна. У.Бек, З. Бауман, М. Фуко – исследование трёх эпистем и дискурсивных практик. Взаимосвязь и взаимовлияние различных культур. Международные связи в области науки и образования. Кризис классических и традиционных ценностей в эпоху постмодерна. Культура древовидная и ризомная. Поздняя современность - постиндустриальная цивилизация и её противоречия. А. Гидденс. Этапы глобализациии ее противоречия. Глобальное и локальное. Мультикультурализм и этнокультурные процессы в современном мире. «Soft skills в контексте образовательного процесса. Коммуникативная компетентность. Надпрофессиональные навыки как основа успешной профессиональной деятельности»

Тема 7. Этнонациональные особенности межкультурного взаимодействия

Понятия «этнос» и «этническая идентичность». Культурная и языковая картины мира, этнокультурные стереотипы. Компоненты этнической самоидентификации: этноним, историческое прошлое, этническая территория, язык, религия, культура. Этнодифференциация «свой» и «чужой». Межкультурная коммуникация и проблемы национальной идентичности. Диагностика надпрофессиональных компетенций (Soft skills). Принципы и типы взаимодействия культур. Оппозиция свой-чужой во взаимодействии культур. Этноцентризм и его проявления. Типы взаимодействия: геноцид, ассимиляция, сепарация, маргинализация, интеграция. Культурная антропология и её достижения: функционализм (культурный релятивизм), диффузионизм. Европоцентризм

Тема 8. Господствующие в современном мире религиозные системы и их взаимодействие

Христианство. Конфессии и деноминации. Католицизм: институт папской власти и его участие в международных культурных процессах. Протестантизм, разнообразие деноминаций. Фундаментальное значение традиционной этики кальвинизма для системы ценностей современного западного общества. Разные течения восточного христианства (в частности, Православие), их влияние на ментальность и роль в мировом

культурном процессе. Ислам. Основные течения и вызовы. «Гражданские» религии: предыстория, содержание, адепты. Секуляризация. Атеизм в истории на новом этапе. «Новый атеизм»

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Филиппов, С. И. Стратегии повседневной и профессиональной межкультурной коммуникации в контексте цивилизационного многообразия современного мира : учебно-методическое пособие / С. И. Филиппов. — Новосибирск : Новосибирский государственный университет, 2024. — 103 с. — ISBN 978-5-4437-1507-0. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/148530/details

Дополнительная литература:

1. Дзялошинский, И. М. Медиатизация культуры в цифровой цивилизации : учебное пособие / И. М. Дзялошинский. — Москва : Ай Пи Ар Медиа, 2022. — 477 с. — ISBN 978-5-4497-1594-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/119113/details

2. Мельникова, Е. А. Межкультурная коммуникация в современном мире : учебное пособие / Е. А. Мельникова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2025. — 105 с. — ISBN 978-5-7410-3427-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/153202/details

3. Формирование культуры межнационального общения в полиэтническом регионе : коллективная монография / Л. Н. Авдеева, О. Ю. Колпачева, Т. В. Портнова [и др.]. — Ставрополь : Ставролит, 2018. — 168 с. — ISBN 978-5-907161-00-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/117425/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Межкультурное взаимодействие в современном мире. Сборник статей	https://elibrary.ru/item.asp?id=74879771
2	Есаков В.А. проблемы межкультурного взаимодействия в современном мире	https://elibrary.ru/item.asp?id=59765724
3	Даник О.Л., Садчикова И.А. Межкультурные связи в современном мире: коммуникация как ключевой фактор взаимодействия между культурами	https://elibrary.ru/item.asp?id=64252047

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Реферат	13-11 – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению; 10-8– основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы; 7-5 – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении. 4 - тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы;
2	Тестовые задания	12-11 – верные ответы составляют более 90% от общего количества; 10-7 – верные ответы составляют 80-50% от общего количества; 6-0 – менее 50% правильных ответов

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые темы рефератов

1. "Культура": многообразие философских и научных подходов и его причины.

2. Понятия "культуры" и "цивилизации" в истории философского анализа культуры.

3. "Науки о культуре". Культура как предмет междисциплинарного анализа.

4. Эволюционизм как парадигма изучения культуры.

5. Теория модернизации о социокультурной динамике.

6. Структурный функционализм в социологии и культурологии.

7. Структурализм: от лингвистики к культурологии.

8. Принципы семиотического анализа культуры.

9. Культурная антропология Э.Б. Тайлора.

10. Идея "прогресса" и ее значение для философии культуры и науки о культуре.

11. Просветительская концепция культуры и цивилизации.

12. "Идеи к философии истории человечества" И.-Г. Гердера в истории философии культуры.

13. Культура в классической немецкой философии.

14. Марксистская концепция культуры.

15. Становление и развитие философской герменевтики.

16. Специфика метода "наук о культуре" в неокантианстве (Г. Риккерт, В. Виндельбанд).

17. "Понимающая социология" М. Вебера как пример культурно-аналитического подхода в социологии.

18. Концептуализация культурного многообразия и проблема типологии культур.

19. "Культурная морфология" О. Шпенглера.

20. Теория "культурно-исторических типов" Н.Я. Данилевского.

21. Этнология Л.Н. Гумилева и культурология.

22. Динамика культуры у А.Д. Тойнби.

23. Социодинамика культуры П. Сорокина.

24. Культурно-антропологический синтез в исторической науке (Школа "Анналов").

25. Культура как проблема психоанализа (З. Фрейд).

26. Фрейдомарксизм и "Франкфуртская школа" о человеке и цивилизации.

27. "Архетипы коллективного бессознательного" К.-Г. Юнга.

28. Экзистенциалистская концепция культуры.

29. Диалогическая концепция культуры (М.М. Бахтин и "постбахтинцы").

30. Постмодернизм в культурологии.

31. "Запад" и "Восток" как проблема европейской мысли.

32. Особенности мифологического сознания. От мифа к логосу.

33. Восточная деспотия как проблема социокультурного анализа.

34. Мифология и религия Древнего Египта.

35. Историко-культурный путь буддизма.

36. Специфика индийской культуры.

37. Конфуцианство и его роль в традиционной культуре Китая.

38. Буддизм и индуизм в Индии: особенности взаимоотношений.

39. Ислам: вероучение и основные направления.

40. "Классика" как принцип и проблема античного типа культуры.

41. Мифология и религия античности.

42. Эллинистическая культура.

43. Византия: специфика типа культуры.

44. Христианство в культуре Средневековья.

45. Реформация: становление нового образа мира.

46. Социокультурный контекст развития западного искусства Нового времени (Возрождение, барокко, классицизм,
романтизм, реализм).

47. Проблемы самосознания европейской культуры (прогресс, европоцентризм, колониализм, модернизация).

48. Сциентизм в культуре Нового времени.

49. Тоталитаризм в культуре XX в.

50. Постмодернизм в культуре XX в.

51. Россия: проблема цивилизационной идентичности ("западники", "славянофилы", "евразийцы").

52. Крещение Руси - момент исторического выбора.

53. Язычество Древней Руси и его роль в русской культуре.

54. "Умозрение в красках".

55. Социокультурные особенности восточной ветви христианства.

56. Святые Древней Руси: социокультурная специфика.

57. Историософская доктрина "Москва - Третий Рим" - "Москва - Новый Иерусалим" в отечественной политической
культуре.

58. Самодержавие - феномен русской культуры. Царь и Бог.

59. Древняя Русь и Великая Степь: борьба и взаимодействие.

60. "Раскол" в истории России (к проблеме "генотипа" отечественной культуры).

61. Метаморфозы "русской идеи".

62. Раскол русской церкви: значение и смысл.

63. Петровская реформа: "псевдомодернизация" или модернизация "догоняющая"?

64. Русская интеллигенция как феномен отечественной культуры: между народом и властью.

65. "Серебряный век". Кризис "классической модели" культуры.

66. Идея "всеединства" в русской культуре XIX-XX вв.

67. Революция как социокультурный феномен.

68. Культура Русского Зарубежья.

69. Советская культура: специфика и основные этапы развития.

70. Современное российское социокультурное развитие: модернизация в период постмодерна.

<u>Типовые задания для проведения теста</u>

1. Представление о культуре как мере восхождения к

нравственному идеалу разрабатывалась в рамках…

а. аксиологического подхода

б. семиотического подхода

в. деятельностного подхода

г. гуманистического подхода

2. Представление о культуре как игре было разработано

а. Ю. Лотманом

б. К. Юнгом

в. Й. Хейзингой

г. Л. Уайтом

3. Как называются в аналитической психологии К. Юнга врожденные психические структуры, которые являются результатом исторического развития человечества?

а. архаизмы

б. архетипы

в. ареалы

г. артефакты

4. Классическая концепция культуры представлена в трудах двух немецких философов (2 варианта ответа):

а. Г. Гегеля

б. Г. Риккерта

в. Ф. Ницше

г. И. Канта

д. З. Фрейда

5. Философ, который различал мир природы и мир свободы, определяя последний как подлинно человеческий, как мир культуры, – …

а. Ж. Кондорсе

б. И. Кант

в. Г. Гегель

г. В. Гумбольдт

6. Суть неклассической концепции культуры заключается в утверждении, что культура…

а. есть развитие человека как разумного существа

б. выступает как специфический способ человеческой жизнедеятельности

в. находится в состоянии глубокого кризиса, вызванного многовековым господством христианства и рационалистической философии

г. является средством возвышения человека, совершенствования его духовной жизни

7. Иррационалистическую трактовку человека и культуры развивал в своем творчестве…

а. Г. Гегель

б. И.Г.Гердер

в. Ф. Ницше

г. И. Кант

8. В культурной антропологии ключевой является тема…

а. технологий жизнеобеспечения

б. разнообразия символических систем

в. социальной организации

г. многообразия культурных форм

9. Э. Кассирер определял культуру как …

а. сферу разума

б. символическую вселенную

в. кристализированную пассионарность

г. совокупность ценностей

10. Специфическим свойством религии как явления культуры является…

а. обращение к эмоциям человека

б. использование символики, образов

в. вера в сверхъестественное

г. особое мироощущение

11. Пройдя традиционную стадию своего развития, человечество вступило на следующую:

а. аграрную

б. постиндустриальную

в. информационную

г. индустриальную

12. Назовите две черты, НЕ характерные для западного типа культуры.

а. антропоцентризм

б. теоцентризм

в. коллективизм

13. Под философией культуры понимают…

а. изложение культурных событий в хронологическом порядке

б. сравнение культуры разных обществ и разных эпох

в. описание трансформации, изменения культуры

г. изучение сущности, целей и ценностей культуры, ее условий и форм проявления

14. Что предполагает креационистский подход к проблеме происхождения человека и культуры?

а. человек и культура — свободное творение Бога

б. перенос зародышей жизни на Землю из космического пространства

в. естественное усовершенствование человека и его культуры

15: Установите соответствие между мыслителями Просвещения и их взглядами на культуру:

а. Вольтер

б. Ж.Ж. Руссо

в. И.Г. Гердер

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Краткая характеристика оценочного средства	Критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов «Зачтено» – 90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Дайте определение понятию «коллективизм»
2. Какой процесс является противоположным по смыслу глобализации культуры?
3. Когда произошло формирование глобальной культуры
4. Дайте определение культурной самоидентификации
5. Перечислите, что составляет фундамент культурной компетентности личности
6. Обозначьте характерный признак современной культуры
7. Какова важнейшая личностная особенность, определяющая успешность межкультурной коммуникации
8. Определите важнейшую особенность традиционной культуры
9. Перечислите, что относится к сфере религиозной культуры
10. Дайте определение культурной идентификации
11. Дайте определение понятию «инновации»
12. Перечислите идеи, на которых было основано западничество как направление русской общественной мысли XIX века
13. Перечислите виды исторического типа культуры
14. Выделите феномены массовой культуры
15. Перечислите идеи, на которых было основано западничество как направление русской общественной мысли XIX века
16. Перечислите виды исторического типа культуры
17. Выделите феномены массовой культуры
18. Перечислите религиозные направления, которые относятся к христианству
19. Какие черты можно отнести к восточному типу культуры?
20. Назовите две черты, характерные для западного типа культуры
21. На основе общности чего формируется этническая культура
22. Укажите две черты, которые отличают восточный тип культур
23. С какими барьерами чаще всего может сталкиваться межкультурная коммуникация в некоторых случаях
24. Укажите две добровольные формы взаимодействие культур
25. Расположите известные артефакты культуры в обратнохронологическом порядке – от современных к древним.
26. Расположите в правильной последовательности уровни культурного взаимодействия от нисходящего к восходящему
27. Укажите правильную хронологическую последовательность развития культуры в истории человечества
28. Укажите, в каком порядке возникли а) буддизм, б) ислам, в) христианство, г) иудаизм
29. Распределите уровни культуры от самой простой к более сложной
30. Укажите хронологическую последовательность возникновения

цивилизаций
31. Дайте определение процессу глобализации
32. Дайте определение искусству
33. Укажите, на основе чего формируется этническая культура
34. Приведите определение понятия «толерантность»
35. Дайте определение понятию «антропоцентризм»
36. Дайте определение культуры
37. Приведите основные характеристики религиозного направления Ислам
38. Дайте определение понятию «карма»
39. Дайте определение понятия «социализация»
40. Приведите определение понятия «этнос»
41. Дайте определение этнического конфликта
42. Дайте определение понятия «миф»
43. Дайте определение понятия «архетип»
44. Дайте определение понятия «идеал»
45. Дайте определение понятия «повседневность»
46. Дайте определение понятия «субкультура»
47. Дайте определение понятия «традиционализм»
48. Дайте определение религиозным барьерам
49. Дайте определение понятия «Cancel culture»
50. Приведите определение понятия европеизация

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Методы и средства защиты информации в системах электронного документооборота»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 6

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 8

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 12

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Методы и средства защиты информации в системах электронного документооборота» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе в 2 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты информации в системах электронного документооборота.

Задачи изучения дисциплины:

– изучение основных понятий и принципов в области организации электронного документооборота;

– изучение требований стандартов организации делопроизводства и электронного документооборота;

– изучение теоретических и организационных основ создания систем электронного документооборота;

– приобретение умений анализировать угрозы безопасности систем электронного документооборота;

– приобретение умений в применении средств защиты информации в системах электронного документооборота;

– выработка навыков в организации в эксплуатации защищенных систем электронного документооборота.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП	Код компетен	Код и наименование	Перечень планируемых результатов обучения по дисциплине	Формы образовательной

(содержание компетенций)	ции	индикатора достижения компетенций	выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	деятельности
Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	**ОПК-1**	ОПК-1.1. Знать: принципы функционирования автоматизированных систем, в том числе поддержки документооборота, и обеспечения их безопасности; методы и средства управления информационной безопасностью; содержание нормативных документов, регламентирующих требования к системе обеспечения информационной безопасности	принципы функционирования автоматизированных систем, в том числе поддержки документооборота, и обеспечения их безопасности; методы и средства управления информационной безопасностью; содержание нормативных документов, регламентирующих требования к системе обеспечения информационной безопасности			Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа
		ОПК-1.2. Уметь: проводить оценку соответствия объекта требованиям нормативных документов и стандартам по информационной безопасности; оформления проекта технического задания на создание системы защиты информации объектов или защищенных систем, в том числе поддержки документооборота.		проводить оценку соответствия объекта требованиям нормативных документов и стандартам по информационной безопасности; оформления проекта технического задания на создание системы защиты информации объектов или защищенных систем, в том числе поддержки документооборота.		

		ОПК-1.3. Владеть: навыками анализа и подготовки содержания нормативно-распорядительных и иных документов для обоснования и поддержки безопасного функционирования объектов; разработки требований информационной безопасности к объектам информатизации.			анализа и подготовки содержания нормативно-распорядительных и иных документов для обоснования и поддержки безопасного функционирования объектов; разработки требований информационной безопасности к объектам информатизации	

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по [illegible]	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Основные понятия и принципы электронного документооборота. Теоретические и организационные основы создания систем электронного документооборота организации	4	6				6				7	Реферат/20
Тема 2. Классификация систем электронного документооборота.	4	6				6				7	Реферат/20
Тема 3. Особенности защиты систем электронного документооборота. Концептуальная модель аппаратной защиты технологии электронного обмена информацией.	5	5				7				7	Реферат/20
Тема 4. Реализация аппаратных средств защиты информации в системах электронного документооборота.	5	5				7				7	Реферат/20
Тема 5. Организация защищенной системы электронной почты	5	5				7				8	Реферат/10
Тема 6. Особенности эксплуатации защищенных систем электронного документооборота	5	5				7				8	Реферат/10
Всего:	**28**	**32**				**40**				**44**	**100**
Контроль, час	**36**										**100 Экзамен**
Объем дисциплины (в академических часах)	**180**										
Объем дисциплины (в зачетных единицах)	**5**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Основные понятия и принципы электронного документооборота. Теоретические и организационные основы создания систем электронного документооборота организации

Этапы документооборота. Представление о системе электронного документооборота. Требования к системам электронного документооборота. История автоматизации документооборота. Отечественные и международные стандарты организации делопроизводства и электронного документооборота. Задачи, функции и структура информационной системы электронного документооборота. Электронный регламент управления организацией. Проблема стандартизации метаданных и форматов в контексте реализации проекта "Электронного правительства". Юридическая сила электронного документа. Проблема защиты информации и информационной безопасности в системах электронного документооборота. Защита персональных данных в информационных системах. Реализованные проекты внедрения систем электронного документооборота в ведомствах и негосударственных структурах РФ. Общегосударственные информационные системы. Федеральные целевые программы в области внедрения электронного документооборота.

Тема 2. Классификация систем электронного документооборота

Признаки классификации систем электронного документооборота. Степень интегрированности программного обеспечения в рамках организации, многофункциональность, масштабирование, мультиформатность, открытость формата, отношение к поддержке безбумажного документооборота, отечественным стандартам делопроизводства. Различие технологий workflow и docflow. Корпоративные информационные системы (КИС) и их роль в контексте внедрения международных стандартов управления качеством.

Тема 3. Особенности защиты систем электронного документооборота. Концептуальная модель аппаратной защиты технологии электронного обмена информацией

Особенности конфиденциального электронного документооборота. Основные виды защищаемой информации в системе электронного документооборота, виды документов ограниченного доступа. Уровни конфиденциальности. Угрозы безопасности информации в системах электронного документооборота. Основные требования и меры по защите информации. Защита от вредоносных программ. Особенности аппаратной защиты электронного обмена информацией. Особенности резидентного компонента безопасности. Принципы аппаратной реализации механизмов аутентификации в электронной среде.

Тема 4. Реализация аппаратных средств защиты информации в системах электронного документооборота

Интерфейсные средства электронного обмена информацией.

Техническая реализация аппаратных средств защиты информации. Архитектура семейства технических устройств аппаратной защиты информации. Использование аппаратных средств защиты. Система контроля целостности и подтверждения достоверности электронных документов. Применение кодов аутентификации в подсистемах технологической защиты информации. Эффективность аппаратных средств защиты.

Тема 5. Организация защищенной системы электронной почты

Организация электронного почтового взаимодействия. Роль и функции электронной почты. Основные принципы организации электронной почты. Угрозы безопасности информации, связанные с использованием электронной почты. Почтовые протоколы взаимодействия. Основные методы и средства защиты электронной почты. Общая схема криптостеганографической системы скрытой передачи ЭД на стороне отправителя. Общая схема криптостеганографической системы скрытой передачи ЭД на стороне адресата.

Тема 6. Особенности эксплуатации защищенных систем электронного документооборота

Особенности эксплуатации систем защищенного электронного документооборота. Обеспечение контроля защиты систем электронного документооборота. Аттестация автоматизированных систем электронного документооборота. Оценка эффективности защиты информации в системах электронного документооборота. Методы и средства защиты информации в системах электронного документооборота

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Степанова, Е. Н. Система электронного документооборота (облачное решение) : учебное пособие / Е. Н. Степанова. — 2-е изд.. — Москва : Ай Пи Ар Медиа, 2025. — 182 с. — ISBN 978-5-4497-3822-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/144371/details

2. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 3-е изд.. — Саратов : Профобразование, 2024. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/145909/details

Дополнительная литература:

1. Минин, О. В. Защита конфиденциальной информации при электронном документообороте : учебное пособие / О. В. Минин, И. В. Минин. — Новосибирск : Новосибирский государственный технический

университет, 2011. — 20 c. — ISBN 978-5-7782-1829-1. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/44918/details

2. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, А. Г. Фабричнов, Т. В. Кондрашева ; под редакцией Н. Н. Куняев. — Москва : Логос, 2013. — 452 c. — ISBN 978-5-98704-711-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/9083/details

3. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 21 c. — ISBN 978-5-906953-22-3. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/98199/details

4. Кузнецова, И. В. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебное пособие / И. В. Кузнецова, Г. А. Хачатрян. — 2-е изд.. — Москва : Ай Пи Ар Медиа, 2025. — 192 c. — ISBN 978-5-4497-3878-3. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/145149/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Ассоциация по вопросам защиты информации	http://bis-expert.ru/
2	Официальный сайт компании Infowatch	http://www.infowatch.ru/
3	Официальный сайт Лаборатории Касперского	http://www.kaspersky.ru/
4	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информационных технологий для проведения лабораторных занятий, предусмотренных программой, в том числе

групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; набор демонстрационного оборудования (проектор, экран).

Аудитория (защищаемое помещение)

Предназначена для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Реферат	10-8/20-16 – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению; 7-5/15-10 – основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы; 4-3/9-6 – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении. 2/5 - тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы;

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые темы для рефератов

1. Защита персональных данных в информационных системах электронного документооборота.
2. Коммерческая тайна и порядок ее защиты.
3. Методы и средства защиты электронного документооборота для ВУЗов.
4. Методы и средства защиты электронного документооборота для банков.
5. Программные закладки. Программы – шпионы.

6. Парольная защита.

7. Сетевые атаки. Системы обнаружения атак

8. Защита программ от несанкционированного копирования

9. Технологии шифрования данных. Шифрование файлов, каталогов, дисков. Шифрованные файловые системы

10. Программные продукты для криптографической защиты данных

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	Критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **-90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо) –** ответ в целом правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно) –** ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично. **-Менее 50 (неудовлетворительно)** – ответы на теоретическую часть неправильные или неполные. Задания не решены

Задания для проведения промежуточной аттестации обучающихся

1. Реализованные проекты внедрения систем электронного документооборота в ведомствах и негосударственных структурах РФ.
2. Федеральные целевые программы в области внедрения электронного документооборота.
3. Защита персональных данных в информационных системах электронного документооборота.
4. Общегосударственные информационные системы электронного документооборота.
5. Критерии выбора программного обеспечения для системы электронного документооборота и фирмы-разработчика.
6. Интегрированность программного обеспечения системы электронного документооборота в рамках организации (многофункциональность, масштабирование, мультиформатность, открытость формата).
7. Соответствие безбумажного документооборота, отечественным стандартам делопроизводства.
8. Корпоративные информационные системы (КИС) и их роль в контексте внедрения международных стандартов управления качеством.
9. Защита от вредоносных программ систем электронного документооборота.
10. Основные требования и меры по защите информации в системах электронного документооборота.
11. Методы и средства защиты информации в информационных системах.
12. Архитектура семейства технических устройств аппаратной защиты информации.
13. Использование аппаратных средств защиты.
14. Особенности почтовых протоколов взаимодействия.
15. Характеристики применяемых СУБД.
16. Аттестация автоматизированных систем электронного документооборота.
17. Оценка эффективности защиты информации в системах электронного документооборота

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Социально-психологические проблемы развития личности»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 6

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ..... **ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 7

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 10

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Социально-психологические проблемы развития личности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе во 2 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование социально ответственной личности, способной к самоорганизации и развитию, умеющей выстраивать и реализовывать свою жизненную стратегию, способной управлять своим временем в новых социальных реалиях, в условиях непрерывного образования, умеющей осуществлять социальное взаимодействие и реализовывать свою роль в команде.

Задачи изучения дисциплины: сформировать у студентов знания и навыки, необходимые для собственного личностного и профессионального становления в процесс обучения и профессиональной деятельности

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	**УК-3**	УК-3.1. Знает методики формирования команд; методы эффективного руководства коллективами. УК-3.2. Уметь разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту. УК-3.3. Владеть методами организации и управления коллективом, планированием его действий.	методы организации команды и приемы руководства работой команды, методики выработки командной стратегии для достижения поставленной цели	разрабатывать командную стратегию; применять эффективные стили руководства командой для достижения поставленной цели	умением анализировать, проектировать и организовывать межличностные, групповые и организационные коммуникации в команде для достижения поставленной цели	Контактная работа: Лекции Практическое занятие Самостоятельная работа

Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	**УК-6**	УК-6.1. Знает основные принципы профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда; способы совершенствования своей деятельности на основе самооценки. УК-6.2. Уметь решать задачи собственного профессионального и личностного развития, включая задачи изменения карьерной траектории; расставлять приоритеты. УК-6.3. Владеть способами управления своей познавательной деятельностью и ее совершенствования на основе самооценки и принципов образования в течение всей жизни.	основные способы определения и реализации приоритетов собственной деятельности и способы ее совершенствования на основе самооценки	выбирать цели и технологии определения и реализации приоритетов собственной деятельности и способов ее совершенствования на основе самооценки	методами и навыками реализации приоритетов собственной деятельности и способами ее совершенствования на основе самооценки, методами планирования траектории своего профессионального развития и способами её реализации	Контактная работа: Лекции Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Социально-психологические основы, принципы и технологии определения и реализации приоритетов собственной деятельности и способов ее совершенствования на основе самооценки	10	10								17	Реферат/30
Тема 2. Психология личности в контексте развития управленческой деятельности и ее совершенствования на основе самооценки	9	9								17	Реферат/30
Тема 3. Социально -психологические проблем организации командной работы	9	9								18	Реферат/40
Всего:	**28**	**28**								**52**	**100**
Контроль, час											**100 Зачет**
Объем дисциплины (в академических часах)	**108**										
Объем дисциплины (в зачетных единицах)	**3**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Социально-психологические основы, принципы и технологии определения и реализации приоритетов собственной деятельности и способов ее совершенствования на основе самооценки

Психологические основы управленческой деятельности. Психология реализации управленческих функций: планирование, мотивация, организация, контроль мотивация.

Тема 2. Психология личности в контексте развития управленческой деятельности и ее совершенствования на основе самооценки

Личность как субъект управленской деятельности. Индивидуально-психологические особенности личности.

Тема 3. Социально-психологические проблемы организации командной работы

Стили управленческой деятельности и проблемы организации командной работы. Социально-психологические проблемы организации командной работы

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Абдурахманов, Р. А. Социальная психология личности, общения, группы и межгрупповых отношений : учебник / Р. А. Абдурахманов. — Саратов : Ай Пи Эр Медиа, 2018. — 368 с. — ISBN 978-5-4486-0173-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/72456/details

2. Алмаев, Н. А. Применение контент-анализа в исследованиях личности : методические вопросы / Н. А. Алмаев. — 2-е изд.. — Москва : Издательство «Институт психологии РАН», 2019. — 166 с. — ISBN 978-5-9270-0242-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/88364/details

Дополнительная литература:

1. Коломинский, Я. Л. Социальная психология развития личности / Я. Л. Коломинский, С. Н. Жеребцов. — Минск : Вышэйшая школа, 2009. — 336 с. — ISBN 978-985-06-1635-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/20142/details

2. Харламенкова, Н. Е. Психология личности: от методологии к научному факту / Н. Е. Харламенкова. — Москва : Издательство «Институт психологии РАН», 2023. — 403 с. — ISBN 978-5-9270-0461-4.

— Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/155062/details

3. Методология, теория, история психологии личности / А. А. Адамян, Т. Н. Адеева, А. А. Алдашева [и др.] ; под редакцией А. Л. Журавлева, Е. А. Никитиной, Н. Е. Харламенковой. — Москва : Издательство «Институт психологии РАН», 2019. — 734 с. — ISBN 978-5-9270-0397-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/155035/details

4. Психологические исследования личности: история, современное состояние, перспективы / М. И. Воловикова, Н. Е. Харламенкова, В. А. Кольцова [и др.] ; под редакцией М. И. Воловиковой, А. Л. Журавлева, Н. Е. Харламенковой. — Москва : Издательство «Институт психологии РАН», 2016. — 448 с. — ISBN 978-5-9270-0317-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/88133/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Колтунова О.А. Взаимосвязь профессиональной самооценки руководителя и стратегии принятия им управленческих решений	https://elibrary.ru/item.asp?id=80268462
2	Петрунева Р.М., Васильева В.Д. Социально-психологические основы командной работы и саморазвития	https://elibrary.ru/item.asp?id=50431907
3	Бегалинова К.К., Ашилова М.С., Бегалинов А.С. Проблемы социально-психологического развития личности в условиях цифровизации	https://elibrary.ru/item.asp?id=42844178

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование: оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Реферат	30-25/40-33 – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению; 24-19/32-25 – основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы; 18-13/24-17 – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении. 12/16 - тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы;

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые темы рефератов

1. Специфика создания команды в подразделениях
2. Специфика труда специалиста на ледостойкой стационарной платформы (ЛСП) и платформы жилого модуля
3. (ПЖМ)
4. Социально-психологическая компетентность лидера
5. Коммуникативная компетентность лидера.
6. Эмоциональная компетентность лидера.
7. Готовность к изменениям как компетенция лидера в нефтегазовой

отрасли.

8. Ассертивность как лидерское качество.

9. Стрессоустойчивость как личностное качество лидера.

10. Роли в проектной команде.

11. Темы для подготовки рефератов (УК-6):

12. Стратегия «управление временем» как управление собственной деятельностью, рациональная организация

13. выполнения задач и распределения собственных ресурсов.

14. Первый шаг на пути к овладению искусством управления временем – изменение его восприятия.

15. Основные причины нерационально потраченного времени.

16. Основные способы организации жизни. Управление стрессами.

17. Само-менеджмент – умение управлять собой. Управление временем, управляя знаниями.

18. Функции и цели самоменеджмента. Основной принцип самоменеджмента – принцип роста и изменений.

19. Целеполагание как процесс сознательного осуществления своих действий в соответствии с генеральной

20. линией или ориентиром: принципы, технология, основные правила, анализ «цель-средство».

21. Определение жизненных приоритетов и постановка задач.

22. Оптимальная система планирования в самоменеджменте.

23. Технология принятия решения в разрешении и конфликта между долгосрочными и краткосрочными

24. целями.

25. Техники самоменеджмента в управлении временем. Правила повышения эффективности персонального

26. менеджмента.

27. Оптимальная система планирования времени. Методы и принципы повышения собственной эффективности

28. А.А. Любищева.

29. Искусство делегирования полномочий.

30. Основные требования к составлению плана дел: список каждодневных дел, составление расписания.

31. Технология планирования по методу «Альпы», «Парето», Эйзенхауэра. Система управления временем Б.

32. Франклина. Прямое планирование с помощью картотек и дневников учета времени.

33. Выбор инструмента для эффективного планирования времени.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Краткая характеристика оценочного средства	Критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов «Зачтено» – 90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Опишите сильные стороны интроверта
2. Опишите слабые стороны интроверта
3. Опишите сильные стороны экстраверта
4. Опишите слабые стороны экстраверта
5. Сформулируйте два принципа эффективного управленческого общения, если Ваш подчиненный – меланхолик.
6. Сформулируйте два принципа эффективного управленческого общения, если Ваш подчиненный – флегматик
7. Сформулируйте два принципа эффективного управленческого общения, если Ваш подчиненный – сангвиник
8. Сформулируйте два принципа эффективного управленческого общения, если Ваш подчиненный – холерик
9. Сформулируйте два принципа эффективного управленческого общения, если Ваш подчиненный – экстраверт
10. Сформулируйте два принципа эффективного управленческого общения, если Ваш подчиненный – интроверт
11. Что такое стресс?
12. В чем состоит отличие потребности и мотива профессиональной деятельности человека?
13. Раскройте значение теории потребностей А. Маслоу (пирамида потребностей)
14. Охарактеризуйте основные виды потребностей человека. Каковы типичные потребности, удовлетворяемые в труде?
15. Для каких ситуаций управленческого общения наиболее эффективен директивный стиль управления?
16. Для каких ситуаций управленческого общения наиболее эффективен демократический стиль управления?
17. Для каких ситуаций управленческого общения наиболее эффективен либеральный стиль управления?
18. Для каких ситуаций управленческого общения наиболее эффективен такой стиль решения конфликтной ситуации, как компромисс
19. Для каких ситуаций управленческого общения наиболее эффективен такой стиль решения конфликтной ситуации, как конкуренция
20. В чем сложность реализации такой управленческой функции, как планирование
21. В чем сложность реализации такой управленческой функции, как контроль
22. Сравните понятия (назовите сходство и отличие) «команда» и «рабочая группа»

1.Расскажите, под влиянием каких факторов складывается образ «Я» личности. Какова его роль в осуществлении регуляции поведения?

23. В чем заключаются причины низкой самооценки? Каковы последствия высокой и низкой самооценки?

24. Как соотносятся самопознание и саморазвитие?

25. Как соотносятся понятия «задатки» и «способности»?

26. Сформулируйте задачу подчиненному («начать работу в новом проекте») таким образом, чтобы максимально мотивировать, если вы знаете, что для него важны следующие мотиваторы – «деньги», «отношения в коллективе», «справедливость»

27. Что такое темперамент? Какие бывают типы темперамента?

28. Дайте психологическую характеристику меланхолическому темпераменту

29. Дайте психологическую характеристику флегматическому темпераменту

30. Дайте психологическую характеристику сангвинику.

31. Дайте психологическую характеристику холерическому темпераменту

32. Подумайте, какие типы темперамента психологически совместимы и почему?

33. Какие приемы способствуют формированию волевых качеств личности?

34. Что такое «способности», и как они связаны с деятельностью человека?

35. Какие существуют точки зрения на происхождение способностей?

36. Какая существует зависимость между способностями, умениями и знаниями

37. Проведите сравнение понятий «Индивид» и «Личность».

38. Проведите сравнение понятий «Темперамент» и «Характер».

39. Дайте определение понятию потребность

40. Дайте определение понятию тайм-менеджмент

41. Почему проблема овладения человеком навыками саморегуляции является одной из ключевых для изучения развития и становления личности?

42. Что такое самовоспитание и самопрограммирование?

43. Раскройте значение понятия «индивидуальный стиль профессиональной деятельности»

44. Назовите 5 качеств личности, которые можно включить в перечень ПВК (профессионально важных качеств) для профессии руководителя.

45. Сравните понятия «потребность» и «мотив»

46. Назовите 3 профессии, которые относятся к группе профессий «Человек-Человек» (по классификации Е.А. Климова)

47. Назовите 3 профессии, которые относятся к группе профессий

«Человек-Природа» (по классификации Е.А. Климова)

48. Назовите 3 профессии, которые относятся к группе профессий «Человек-Техника» (по классификации Е.А. Климова)

49. Назовите 3 профессии, которые относятся к группе профессий «Человек-художественный образ» (по классификации Е.А. Климова)

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Проектирование организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 8

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Проектирование организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе в 2 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование компетенций обучающегося в области использования нормативно-правовых актов по информационной безопасности и организации технологического процесса защиты информации ограниченного доступа в соответствии с требованиями регуляторов по информационной безопасности.

Задачи изучения дисциплины:

– рассмотреть особенности организации режима секретности на объектах и системах различного профиля и организационной структуры;

– раскрыть принципы обеспечения защиты информации, составляющей государственную тайну и конфиденциальную информацию;

– ознакомиться с принципами организации конфиденциального документооборота в организации;

– рассмотреть особенности работы с документами, отмеченными пометкой «Для служебного пользования»;

– показать особенности правового регулирования отношений в области компьютерных преступлений.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП	Код компетен	Код и наименование	Перечень планируемых результатов обучения по дисциплине	Формы образовательной

(содержание компетенций)	ции	индикатора достижения компетенций	выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	деятельности
Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	**ОПК-3**	ОПК-3.1.Знать: основы законодательных и иных нормативно-правовых актов в сфере обеспечения информационной безопасности. ОПК-3.2. Уметь: свободно ориентироваться в структуре необходимых нормативно-правовых актов и информационно-правовых норм действующего законодательства по обеспечению информационной безопасности, в том числе с помощью систем правовой информации. ОПК-3.3. Владеть: навыками разработки проектов нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.	основные нормативно-правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации	применять нормативные правовые акты и эксплуатационно-технические документы в области обеспечения информационной безопасности; разрабатывать организационно-распорядительные и эксплуатационно-технические документы системах обеспечения информационной безопасности	разработки организационно-распорядительных и эксплуатационно-технических документов по защите информации в автоматизированных системах	Контактная работа: Лабораторный практикум Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Законодательство РФ в области информационной безопасности			4			5				9	Тест/10
Тема 2. Обзор руководящих документов, касающихся организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности			4			5				9	Тест/10
Тема 3. Политика безопасности организации		4				5				9	Реферат/10
Тема 4. Организационно-распорядительные документы при обеспечении безопасности ИСПДн.			4			5				9	Тест/20
Тема 5. Организационно-распорядительные документы при обеспечении безопасности ГИС			4			5				9	Тест/20
Тема 6. Организационно-распорядительные документы при обеспечении безопасности объектов КИИ			4			5				9	Тест/10
Тема 7. Организационно-			4			5				9	Тест/10

распорядительные документы при обеспечении коммерческой тайны											
Тема 8. Организация пропускного и внутри объектового режима		4				5				9	Реферат/10
Всего:		**8**	**24**			**40**				**72**	**100**
Контроль, час											**100 Зачет**
Объем дисциплины (в академических часах)	**144**										
Объем дисциплины (в зачетных единицах)	**4**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Законодательство РФ в области информационной безопасности

Основы законодательства. Стратегические документы. Системообразующие документы. Государственные регуляторы. Техническое регулирование. Сертификация средств защиты информации. Аттестация объектов информатизации. Информационная безопасность и персонал

Тема 2. Обзор руководящих документов, касающихся организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности

Закрепление права предприятия на защиту информации в нормативных документах. Перечень информационных систем и информации ограниченного доступа. Перечень лиц, допущенных к обработке информации. Модель угроз и нарушителя. Лицензирование деятельности и сертификация средств в области защиты конфиденциальной информации.

Тема 3. Политика безопасности организации

Стандарты. Приказ ответственного за защиту информации. Правила обращения с носителями информации. Инструкции по парольной защите, антивирусной защите, инструкции пользователей и администраторов и т.д. Правовые нормы защиты информации в автоматизированных системах

Тема 4. Организационно-распорядительные документы при обеспечении безопасности ИСПДн

Правовые нормы защиты информации в автоматизированных системах. Порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных

Тема 5. Организационно-распорядительные документы при обеспечении безопасности ГИС

Организационно-распорядительные документы для ГИС.

Тема 6. Организационно-распорядительные документы при обеспечении безопасности объектов КИИ

Разработка организационно-распорядительных документов. Что определяют организационно-распорядительные документы. Что включают организационно-распорядительные документы. Правила безопасной работы работников.

Тема 7. Организационно-распорядительные документы при обеспечении коммерческой тайны

Создание системы информационной безопасности предприятия. Разработка и утверждение Положения о коммерческой тайне. Издание приказов о коммерческой тайне. Оформление трудовых соглашений с сотрудниками. Создание специализированного делопроизводства

Тема 8. Организация пропускного и внутри объектового режима

Определение внутриобъектового режима. Цели и задачи внутриобъектового режима. Пропускной режим. Основные элементы системы организации пропускного режима. Установление пропускного и внутриобъектового режимов

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Степанова, Е. Н. Система электронного документооборота (облачное решение) : учебное пособие / Е. Н. Степанова. — 2-е изд.. — Москва : Ай Пи Ар Медиа, 2025. — 182 с. — ISBN 978-5-4497-3822-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/144371/details

2. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 3-е изд.. — Саратов : Профобразование, 2024. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/145909/details

Дополнительная литература:

1. Минин, О. В. Защита конфиденциальной информации при электронном документообороте : учебное пособие / О. В. Минин, И. В. Минин. — Новосибирск : Новосибирский государственный технический университет, 2011. — 20 с. — ISBN 978-5-7782-1829-1. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/44918/details

2. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, А. Г. Фабричнов, Т. В. Кондрашева ; под редакцией Н. Н. Куняев. — Москва : Логос, 2013. — 452 с. — ISBN 978-5-98704-711-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/9083/details

3. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 21 с. — ISBN 978-5-906953-22-3. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/98199/details

4. Кузнецова, И. В. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебное пособие / И. В. Кузнецова, Г. А. Хачатрян. — 2-е изд.. — Москва : Ай Пи Ар Медиа, 2025. — 192 с. — ISBN 978-5-4497-3878-3. — Текст : электронный //

Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/145149/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Ассоциация по вопросам защиты информации	http://bis-expert.ru/
2	Официальный сайт компании Infowatch	http://www.infowatch.ru/
3	Официальный сайт Лаборатории Касперского	http://www.kaspersky.ru/
4	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информационных технологий для проведения лабораторных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; набор демонстрационного оборудования (проектор, экран).

Аудитория (защищаемое помещение)

Предназначена для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Реферат	10-8 – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению; 7-5 – основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы; 4-3 – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении. 2 - тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы;
2	Тест	20-18 – верные ответы составляют более 90% от общего количества; 17-10 – верные ответы составляют 80-50% от общего количества; 9-0 – менее 50% правильных ответов

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые темы для рефератов

1. Принципы и средства построения систем информационной безопасности
2. Этапы создания систем защиты информации
3. Моделирование системы защиты информации
4. Системный подход к защите информации и показатели

безопасности

5. информации

6. Требования к структуре системы защиты информации

7. Мероприятия, способы и средства по обеспечению защиты информации на

8. объекте

9. Комплекс мероприятий по обеспечению информационной безопасности

10. Технические средства защиты информации

11. Категории средств защиты информационно-программного обеспечения

Типовые тестовые задания

1. Подготовка организационно-распорядительной документации предполагает выполнение следующих видов работ (установите соответствие):

a. разработка организационно-распорядительной документации анализ полученных сведений по результатам обследования

b. формирование плана работ и перечня документов

c. обследование объекта информатизации

d. внедрение организационно-распорядительной документации

2. Установите правильную последовательность действий при разработке модели угроз безопасности информации:

a. Идентификация уязвимостей информационной системы.

b. Анализ возможных угроз безопасности информации.

c. Оценка вероятности реализации угроз.

d. Определение перечня защищаемых ресурсов информационной системы.

3. Установите правильную последовательность этапов внедрения системы защиты информации (СЗИ):

a. Ввод СЗИ в эксплуатацию.

b. Разработка проекта системы защиты информации.

c. Выбор средств защиты информации.

d. Настройка и тестирование СЗИ.

e. Установка средств защиты информации.

4. Установите правильную последовательность действий при разработке инструкции пользователя информационной системы:

a. Утверждение инструкции пользователя.

b. Разработка проекта инструкции пользователя.

c. Определение перечня действий пользователя, которые должны быть описаны в инструкции.

d. Тестирование инструкции пользователями.

5. Установите правильную последовательность действий при разработке руководства по эксплуатации средства защиты информации (СЗИ):

a. Утверждение руководства по эксплуатации СЗИ.

b. Определение структуры и содержания руководства по эксплуатации СЗИ.
c. Разработка проекта руководства по эксплуатации СЗИ.
d. Определение целевой аудитории руководства.

6. Какой документ является основополагающим при разработке системы защиты информации?
a. Должностные инструкции
b. Политика информационной безопасности
c. Приказ о назначении ответственных лиц
d. Регламент работы с документами

7. Кто утверждает организационно-распорядительные документы по информационной безопасности?
a. Начальник службы безопасности
b. Системный администратор
c. Руководитель организации
d. Начальник IT-отдела

8. Какой документ определяет порядок действий при возникновении инцидентов информационной безопасности?
a. Политика безопасности
b. Инструкция по реагированию на инциденты
c. Должностная инструкция
d. План проверок

9. В каком документе описываются требования к паролям пользователей?
a. Трудовой договор
b. Положение о конфиденциальности
c. Регламент управления доступом
d. Приказ о назначении ответственных

10. Как часто должны пересматриваться эксплуатационно-технические документы?
a. Раз в 5 лет
b. При существенных изменениях в системе защиты
c. Только при смене руководства
d. Раз в 10 лет

11. Что должен включать акт классификации информационной системы?
a. Список сотрудников
b. План помещений
c. Перечень обрабатываемых данных и их уровень защиты
d. Финансовые показатели

12. Какой документ регламентирует порядок резервного копирования информации?
a. Политика безопасности
b. Приказ руководителя
c. Регламент резервного копирования

d. Должностная инструкция

13. В каком документе определяется ответственность за нарушение требований информационной безопасности?

a. Технический регламент

b. Положение о дисциплинарной ответственности

c. Инструкция пользователя

d. План мероприятий

14. Кто должен быть ознакомлен с инструкцией по защите информации?

a. Только руководители подразделений

b. Только системные администраторы

c. Все сотрудники, работающие с защищаемой информацией

d. Только служба безопасности

15.Какой документ определяет порядок проведения внутреннего аудита информационной безопасности?

a. Политика безопасности

b. План работы службы безопасности

c. Регламент проведения внутреннего аудита

d. Должностная инструкция

16.Какой документ определяет порядок эксплуатации системы информационной безопасности?

a. Политика информационной безопасности

b. Регламент эксплуатации системы информационной безопасности

c. План реагирования на инциденты безопасности

d. Отчет о состоянии информационной безопасности

17.Какой документ содержит информацию о мерах безопасности, реализованных в системе информационной безопасности?

a. Политика информационной безопасности

b. План реагирования на инциденты безопасности

c. Отчет о состоянии информационной безопасности

d. Документация на систему информационной безопасности

18.Какова основная цель разработки плана реагирования на инциденты безопасности?

a. Предотвращение инцидентов безопасности

b. Реагирование на инциденты безопасности и минимизация их последствий

c. Расследование инцидентов безопасности

d. Устранение последствий инцидентов безопасности

19.Какой документ определяет порядок проведения аудита информационной безопасности?

a. Политика информационной безопасности

b. Регламент эксплуатации системы информационной безопасности

c. План аудита информационной безопасности

d. Отчет о состоянии информационной безопасности

20.Какой документ содержит информацию о требованиях к защите

информации в системе информационной безопасности?
a. Политика информационной безопасности
b. Регламент эксплуатации системы информационной безопасности
c. План реагирования на инциденты безопасности
d. Документация на систему информационной безопасности

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Краткая характеристика оценочного средства	Критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **«Зачтено»** – **90-100** – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – **70 -89** – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – **50 - 69** – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. **«Не зачтено»** – **менее 50** – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Структура политики информационной безопасности и процесс ее разработки
2. Характеристика различных уровней политики ИБ
3. Формирование политики управления инцидентами ИБ. Основное содержание политики управления инцидентами ИБ
4. Создание группы реагирования на инциденты ИБ. Цель создания.

Роли группы реагирования на инциденты ИБ

5. Подготовка к обработке инцидентов ИБ. Классификация инцидентов ИБ по значимости

6. Обеспечение осведомленности и обучение управлению инцидентами. Цель осведомления об управлении инцидентами ИБ. Цель обучения управлению инцидентами ИБ

7. Тестирование системы управления инцидентами ИБ

8. Первичная оценка событий ИБ. Цель проведения первичной оценки. Последовательность действий при проведении первичной оценки

9. Вторичная оценка инцидента ИБ. Цель проведения вторичной оценки. Последовательность действий при проведении вторичной оценки

10. Сдерживание, устранение инцидента ИБ и восстановление после него

11. Формирование и хранение свидетельств инцидентов ИБ

12. Определение инцидента неавторизованного доступа. Цели инцидента неавторизованного доступа

13. Определение инцидента отказа в обслуживании. Цели инцидента отказа в обслуживании. Примеры инцидентов отказа в обслуживании

14. Определение инцидента сбора информации. Цели инцидента сбора информации

15. Определение инцидента внедрения вредоносного кода. Средства реализации инцидента внедрения вредоносного кода. Цели инцидента

16. Определение инцидента несоответствующего использования. Примеры инцидентов несоответствующего использования

17. Стратегии управления непрерывностью функционирования АС для помещений и технологий

18. Стратегии управления непрерывностью функционирования АС для данных. Стратегии управления непрерывностью функционирования АС для поставщиков

19. Стратегии управления непрерывностью функционирования АС для компьютеров

20. Стратегии управления непрерывностью функционирования АС для серверов

21. Стратегии управления непрерывностью функционирования АС для локальной сети

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Теоретические основы управления»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 6

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 9

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Теоретические основы управления» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе во 2 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование теоретических знаний и практических умений по управлению информационной безопасностью сложных социально-технических и производственных систем, использующих современные знания теории управления и информационные технологии.

Задачи изучения дисциплины:

– изучение специфических особенностей управленческой деятельности в системах информационной безопасности, основываясь на организационных формах и структурах управления предприятиями и организациями;

– изучение новейших тенденций управления информационными системами с учетом передового отечественного и зарубежного опыта;

– овладение навыками управленческой работы, использование которых позволит повысить эффективность деятельности предприятий и организаций.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	**ОПК-5**	ОПК-5.1. Знать: логические методы и приемы научного исследования; о видах экспериментов и методах обработки данных; методы анализа, синтеза, способы математического моделирования в области исследований и разработок, в том числе, организации современных систем управления.	основные методы и принципы разработки процессов управления информационной безопасностью	разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность	владеть терминологией и процессным подходом построения СУИБ	Контактная работа: Лекции Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Основы теории и практики управления.	10	10								17	Реферат/30
Тема 2. Передовые концепции менеджмента, особенности управления организациями и современные модели управления.	9	9								17	Реферат/30
Тема 3. Методы принятия управленческих решений	9	9								18	Реферат/40
Всего:	**28**	**28**								**52**	**100**
Контроль, час											**Зачет**
Объем дисциплины (в академических часах)	**108**										
Объем дисциплины (в зачетных единицах)	**3**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Основы теории и практики управления

Методология теории управления. Цели и функции теории управления. История развития теории и практики управления социальными, техническими и производственными системами. Важнейшие элементы управленческого процесса. Вклад советских ученых в теорию научного управления. Административная теория. Функции и принципы управления А. Файоля. Бюрократическая теория. Э. Мэйо и его Хоуторнские эксперименты. Школа поведенческих наук.

Тема 2. Передовые концепции менеджмента, особенности управления организациями и современные модели управления

Ознакомление с передовыми концепциями менеджмента, особенностями управления организациями и современные модели управления. Стили управления. Теория научного управления. Ф. Тейлор – основоположник научного менеджмента. Исследования Г. Ганта, Ф. и Л. Гилбреттов. Поточная организация труда по концепции Г. Форда. Система целесообразностей Г. Эмерсона. Сущность и формы управленческой деятельности. Функции управления. Принципы управления. Методы социального управления. Стили руководства. Делегирование полномочий. Организация и методы принятия управленческих решений. Принципы управления. Цели управления. Основные законы управления. Кибернетические подходы к управлению.

Тема 3. Методы принятия управленческих решений

Классификация методов обоснования управленческих решений. Формирование способности выполнять моделирование и анализ процессов управления сложных социально-технических и производственных систем. Математические методы, используемые для принятия решений.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Глебова, О. В. Методы принятия управленческих решений : учебное пособие / О. В. Глебова. — Саратов : Вузовское образование, 2017. — 274 c. — ISBN 978-5-906172-20-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/62071/details

2. Чернякова, М. М. Современные методы принятия управленческих решений : учебное пособие / М. М. Чернякова, И. А. Чернякова. — Новосибирск : Новосибирский государственный технический университет, 2023. — 126 c. — ISBN 978-5-7782-5079-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/155758/details

Дополнительная литература:

1. Денисова, Л. А. Разработка, исследование и оптимизация автоматизированных систем управления в среде MATLAB : учебное пособие / Л. А. Денисова. — Омск : Омский государственный технический университет, 2023. — 120 c. — ISBN 978-5-8149-3631-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/140860/details

2. Камышанская, Н. Н. Теоретические основы управления организацией : учебное пособие / Н. Н. Камышанская, Е. А. Репина. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2025. — 118 c. — ISBN 978-5-9275-5010-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/157829/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Наугольнова И.А. Менеджмент 4.0: эволюция и инновации в управлении организацией в цифровую эпоху	https://elibrary.ru/item.asp?id=54131117
2	Илаева З.М., Садуева М.А. Эльгайтарова Н.Т. Управление персоналом и человеческими ресурсами в условиях современного менеджмента.	https://elibrary.ru/item.asp?id=54766818
3	Малюгина Я.А. Эффективность методов принятия управленческих решений в организации	https://elibrary.ru/item.asp?id=80468766

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и

индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Реферат	30-25/40-33 – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению; 24-19/32-25 – основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы; 18-13/24-17 – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении. 12/16 - тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы;

Типовые контрольные задания или иные материалы в рамках

текущего контроля успеваемости

<u>Типовые темы рефератов</u>

1. Образовательная организация как открытая система и объект управления.
2. Научные основы управления образовательной организацией: структура, принципы, подходы, методы.
3. Развитие управленческой мысли. Основные научные теории управления.
4. Основные функции управления.
5. Планирование работы образовательной организации.
6. Организация как функция управления.
7. Контроль как функция управления.
8. Связующие процессы в управлении: мотивация, коммуникация.
9. Основы выработки и реализации управленческих решений.
10. Руководитель образовательной организации как субъект управления.
11. Имидж современного руководителя.
12. Стиль управления как условие формирования социально-педагогического климата образовательной организации.
13. Организационная культура как показатель качества деятельности образовательной организации.
14. Управление коллективом.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Краткая характеристика оценочного средства	**Критерии оценки, балл**
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов «Зачтено» – 90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом

Краткая характеристика оценочного средства	Критерии оценки, балл
	правильно интерпретирует полученный результат. – 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Понятие автоматизированной системы управления предприятием (АСУП). Концепции MRP, MRP II, ERP, APS.
2. Назначение и основные функциональные блоки ERP-систем.
3. Отличия MRP- и ERP-систем.
4. Типовые модули современной ERP-системы.
5. Основные проблемы при внедрении и использовании ERP-систем.
6. Выбор ERP-системы и ключевые вопросы выбора.
7. Информационные технологии управления корпорацией.
8. Концепции, методологии и стандарты корпоративного управления
9. Концепция CSRP. Подсистемы управления документооборотом (Docflow) и бизнес- процессами (BPM).
10. Отличия MES системы от ERP-систем.
11. Оперативная коррекция производственных планов в MES-системе.
12. Оптимизация производства в MES-системе.
13. Связь в реальном времени производственных процессов с бизнес процессами
14. Формирование данные о текущих производственных показателях в MES-системе.
15. Подсистемы АСУ предприятий.
16. Состав АСУП; функциональное подразделение предприятия.
17. SCADA-системы. Технические характеристики SCADA-систем.
18. Математическое обеспечение АСУ.
19. Модели и алгоритмы логико-программного управления
20. Модели и алгоритмы диспетчирования.
21. Состав и назначение программного обеспечения АСУП.
22. Системное программное обеспечение АСУ П.
23. Прикладное программное обеспечение АСУ П.
24. Инструментальные средства разработки корпоративных

информационных систем. CASE-системы. Назначение и виды CASE-систем.

25. Проектирование информационных систем по технологии RUP
26. Применение модельно-ориентированной архитектуры.
27. Выбор готовых решений на рынке КИС.
28. Внедрение системы. Эксплуатация КИС. Развитие КИС.
29. Процессный подход к построению СУИБ и циклическая модель PDCA.
30. Цели и задачи, решаемые СУИБ.
31. Стандартизация в области построения СУИБ: сходства и различия стандартов.
32. Стратегии выбора области деятельности СУИБ.
33. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
34. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
35. Политика ИБ и политика СУИБ: сходства и различия.
36. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
37. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
38. Анализ рисков ИБ: основные подходы, основные этапы процесса.
39. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
40. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
41. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
42. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
43. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ
44. Внедрение процессов управления ИБ: этапы и последовательность.
45. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины
«Проектирование технических средств и систем в защищенном исполнении»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 6

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 10

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Проектирование технических средств и систем в защищенном исполнении» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе в 3 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование у учащихся знания о базовых принципах и подходах к проектированию технических средств и систем в защищенном исполнении, а также обеспечение развития практических навыков и способностей к решению прикладных задач проектирования.

Задачи изучения дисциплины:

- ознакомление с методологическими основами организации защиты информации при проектировании технических средств и систем, с характеристиками и способами применения мер и средств защиты информации;
- формирование представлений о системах защиты информации;
- приобретение навыков обоснования требований к системам защиты информации.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	**ОПК-2**	ОПК-2.1. Знать: основные понятия, используемые при проектировании, создании, модернизации системы защиты информации объектов информатизации; требования к разработке компьютерной системы в защищенном исполнении. ОПК-2.2. Уметь: определять основные мероприятия по организации разработки системы защиты информации на объектах информатизации; разрабатывать технические проекты, документы, регламентирующие обеспечение информационной безопасности объектов информатизации (подсистемы либо компонента системы). ОПК-2.3. Владеть: навыками работы с нормативно-правовыми документами и стандартами в области информационной безопасности; разработки (формирования) требований информационной безопасности к объектам и субъектам деятельности по проектированию, созданию (модернизации) объектов информатизации на базе компьютерных систем в защищенном исполнении.	основные понятия, используемые при проектировании, создании, модернизации системы защиты информации объектов информатизации; требования к разработке компьютерной системы в защищенном исполнении.	определять основные мероприятия по организации разработки системы защиты информации на объектах информатизации; разрабатывать технические проекты, документы, регламентирующие обеспечение информационной безопасности объектов информатизации	работы с нормативно-правовыми документами и стандартами в области информационной безопасности; разработки (формирования) требований информационной безопасности к объектам и субъектам деятельности по проектированию, созданию (модернизации) объектов информатизации на базе компьютерных систем в защищенном исполнении	Контактная работа: Лабораторный практикум Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Изучение принципов построения технических средств и систем в защищенном исполнении		6	6			18				18	Тест/40
Тема 2. Изучение методов утечки информации от технических средств и систем, и факторов, воздействующих на объекты информатизации		6	6			18				18	Тест/40
Тема 3. Изучение стандартов по разработке технических средств и систем		6	6			20				16	Реферат/20
Всего:		**18**	**18**			**56**				**52**	**100**
Контроль, час	**36**										**100 Экзамен**
Объем дисциплины (в академических часах)	**180**										
Объем дисциплины (в зачетных единицах)	**5**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Изучение принципов построения технических средств и систем в защищенном исполнении

Основные понятия и определения, понятие автоматизированной системы. Особенности автоматизированных систем в защищённом исполнении. Основные виды АС в защищённом исполнении. Общий порядок проектирования систем в защищённом исполнении, стандарты, регламентирующие этот процесс. Руководящие документы Гостехкомиссии России (ФСТЭК России). Понятие модели угроз, документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Понятие модели нарушителя, документы ФСТЭК России, регламентирующие порядок разработки моделей нарушителя в автоматизированных системах. Подходы к оценке эффективности комплексной системы информационной защиты

Тема 2. Изучение методов утечки информации от технических средств и систем, и факторов, воздействующих на объекты информатизации

Понятие и структура технического канала утечки информации. Классификация технических каналов утечки информации. Факторы, воздействующие на объекты информатизации. Основные меры защиты информации от утечки по техническим каналам.

Тема 3. Изучение стандартов по разработке технических средств и систем

Понятие стандартизации. Изучение стандартов по разработке технических средств и систем. Виды стандартов. Разработка технического задания. Правила оформления технических условий.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Помазанов, А. В. Защита информации от утечки по техническим каналам : учебное пособие / А. В. Помазанов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2024. — 132 с. — ISBN 978-5-9275-4851-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/152195/details

Дополнительная литература:

1. Ксендзов, А. В. Защищенные системы передачи информации. Ч.1 : учебное пособие / А. В. Ксендзов. — Рязань : Рязанский государственный радиотехнический университет, 2021. — 96 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/137320/details

2. Прокопенко, Е. В. Техническая защита информации : учебное пособие / Е. В. Прокопенко, В. О. Коротин. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2024. — 131 с. — ISBN 978-5-00137-494-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/148668/details

3. Васильева, М. А. Фильтрация набора данных. Рекомендации по выполнению работы и перечень типовых заданий : учебно-методическое пособие / М. А. Васильева, К. М. Филипченко, В. А. Пугачёв. — 3-е изд.. — Москва : Российский университет транспорта (МИИТ), 2024. — 137 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/147367/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Агапов Е.В. Классификация технических каналов утечки информации в современных ИТ-инфраструктурах: эволюция и актуальные угрозы	https://elibrary.ru/item.asp?id=91522620
2	Денисов Я.Ю. Методы защиты персональных данных в корпоративных информационных системах от современных киберугроз	https://elibrary.ru/item.asp?id=90539572
3	Официальный сайт Лаборатории Касперского	http://www.kaspersky.ru/
4	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информационных технологий обеспечения информационной безопасности и защищенных информационных систем для проведения лабораторных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения,

с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; набор демонстрационного оборудования (проектор, экран), средства вычислительной техники, сетевое оборудование, технические, программными и программно-аппаратные средства защиты информации и средства контроля защищенности информации.

Помещение для самостоятельной работы обучающихся

Основное оборудование: оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Реферат	20-16 – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению; 15-10 – основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы; 9-6 – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении. 5 - тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы;
2	Тест	40-29 – верные ответы составляют более 90% от общего количества; 30-21 – верные ответы составляют 80-50% от общего количества; 20-0 – менее 50% правильных ответов

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые темы для рефератов

1. Графические средства представления проектных решений;
2. Методы и инструментальные средства организации проектной деятельности;
3. Автоматизация создания модели угроз безопасности объектов;
4. Применение нелинейного локатора для обнаружение

полупроводниковых элементов;

5. Уязвимости в программном обеспечении на примере «» и возможные меры по их устранению;

6. Модель угроз безопасности информации автоматизированной системы управления на базе станка с числовым программным

7. управлением;

8. Модель угроз безопасности информации Web-сайта;

9. Типовые настройки средства защиты информации в зависимости от класса защищенности автоматизированной системы;

10. Комплексное моделирование системы активной защиты информации

Типовые тестовые задания

1. Выберите сертифицированные средства ФСТЭК и ФСБ антивирусной защиты из предложенных:

а) Kaspersky Internet Security,
б) Kaspersky Total Security,
в) ESET NOD32,
г) Kaspersky Anti-Virus,
д) Dr.Web,
е) Kaspersky Endpoint Security

2. Для какого(-их) уровня(-ей) защищенности персональных данных разрешено неиспользование средства обнаружения вторжений?

а) для 2го уровня защищенности
б) для 3го и 4го уровней
в) для всех уровней необходимо обеспечить данную меру защиты информации

3. Выберите вариант, который относится ко 2 категории ИСПДн:

а) расовая, национальная принадлежность
б) общедоступные данные
в) состояние здоровья
г) идентификация субъекта и доп. информация

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	Критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов

Краткая характеристика оценочного средства	Критерии оценки, балл
	-90 и более (отлично) – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо) –** ответ в целом правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно) –** ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично. **-Менее 50 (неудовлетворительно)** – ответы на теоретическую часть неправильные или неполные. Задания не решены

Задания для проведения промежуточной аттестации обучающихся

1. Меры обеспечения безопасности АС. Раскройте понятие идентификация.
2. Меры обеспечения безопасности АС. Раскройте понятие аутентификация. Виды.
3. Меры обеспечения безопасности АС. Какие основные методы разграничения доступа Вам известны?.
4. Общая классификация мер обеспечения безопасности АС.
5. Для чего нужны общие критерии оценки безопасности ИТ?
6. Раскройте понятие объект оценки общих критериев оценки безопасности ИТ
7. По каким критериям относить автоматизированную систему к ГИС?
8. Раскройте понятие «аудит информационной безопасности».
9. Раскройте термин «событие информационной безопасности».
10. Основные угрозы безопасности информации АС и их классификация.
11. Примеры уязвимостей информационно-технологических ресурсов АС.
12. Классификация каналов проникновения в систему и утечки информации.
13. Кратко опишите спиральную модель (эволюционную) модель

жизненного цикла разработки АС.

14. Кратко опишите процессную модель жизненного цикла разработки АС.

15. Какие методы проектирования АС Вам известны?

16. Что является целью защиты информации (ЗИ) в автоматизированной системе в защищенном исполнении?

17. Какие стороны принимают участие в работах по созданию (модернизации) АСЗИ и ее системы ЗИ?

18. Основные этапы развития ИС и АС.

19. Администрирование АС. Каковы функции и службы администрирования?

20. Администрирование АС. Назовите категории административного персонала.

21. Меры обеспечения безопасности АС. Что такое криптографическое преобразование информации в АС?

22. Меры обеспечения безопасности АС. Что такое межсетевое экранирование?

23. Раскройте понятия функциональные требования и требования доверия общих критериев оценки безопасности ИТ.

24. Раскройте понятие профиль защиты общих критериев оценки безопасности ИТ.

25. Чем опытная эксплуатация АС отличается от промышленной?

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Теоретические основы компьютерной безопасности»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 6

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 9

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Теоретические основы компьютерной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе в 3 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – обучение студентов теоретическим основам компьютерной безопасности, общим принципам построения моделей безопасности и политик безопасности, основным методам исследования корректности систем защиты, методологии обследования и проектирования систем защиты; раскрыть практическое применение теоретических моделей защиты информации в современных операционных системах, основы технических средств, используемых в компьютерной индустрии для защиты информации.

Задачи изучения дисциплины: изложить теоретические основы компьютерной безопасности; обучить составлению политики безопасности, применению моделей безопасности и технических средств защиты на практике; познакомить с методологией обследования и проектирования систем защиты; дать навыки настройки основных компонентов систем защиты и применения технологий защиты в современных операционных системах.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой	**ПК-2**	ПК-2.1. Знать: источники и классификацию угроз безопасности информации, обрабатываемой автоматизированной системой и содержащейся в ее базах данных; положения типовых методик оценки рисков нарушения информационной безопасности. ПК-2.2. Уметь: формировать модель угроз, анализировать и оценивать угрозы информационной безопасности объекта; создавать диаграммы, моделирующие систему в специализированных графических редакторах на базе известных нотаций и стандартов. ПК-2.3. Владеть: методами и средствами выявления угроз безопасности в базах данных, автоматизированных системах; навыками применения средств анализа безопасности информационных систем.	источники и классификацию угроз информационной безопасности; методы анализа компьютерных систем; требования к разработке защищенных автоматизированных систем	проводить оценку соответствия объекта требованиям нормативных документов и стандартам по информационной безопасности	анализа и подготовки содержания нормативно-распорядительных и иных документов для поддержки безопасного функционирования объектов, в том числе в автоматизированных системах.	Контактная работа: Лекции Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Основные определения компьютерной безопасности.	12	12								12	Реферат/30
Тема 2. Задачи обеспечения компьютерной безопасности.	12	12								12	Реферат/30
Тема 3. Сервисы безопасности на основе модели OSI (по ISO 7498-2)	12	12								12	Реферат/40
Всего:	**36**	**36**								**36**	**100**
Контроль, час	**36**										**100 Экзамен**
Объем дисциплины (в академических часах)	**144**										
Объем дисциплины (в зачетных единицах)	**4**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Основные определения компьютерной безопасности

Объектно-ориентированный подход компьютерной безопасности. Суть объектно-ориентированного подхода. Комплексность решения. Создание рубежей защиты. Угрозы компьютерной безопасности конфиденциальности. Наиболее распространенные угрозы конфиденциальности, целостности, доступности. Модель нарушителя.

Тема 2. Задачи обеспечения компьютерной безопасности

Управление доступом. Основы дискреционного управления доступом. Мандатное управление доступом. Методы аутентификации в компьютерных системах. Одно- и многофакторная аутентификация. Технологии решения. Методы обеспечения конфиденциальности. Модели шифрования. Основные типы криптоанализа.

Тема 3. Сервисы безопасности на основе модели OSI (по ISO 7498-2)

Протоколы, обеспечивающие решение задач информационной безопасности. Программно-аппаратные решения, обеспечивающие решение задач информационной безопасности. Системы обнаружения вторжений.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Басыня, Е. А. Сетевая информационная безопасность : учебник / Е. А. Басыня. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/132693/details

2. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 3-е изд.. — Саратов : Профобразование, 2024. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/145909/details

Дополнительная литература:

1. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 5-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2026. — 605 с. — ISBN 978-5-4497-3470-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/162528/details

2. Основы защиты информации в современных информационных системах : учебное пособие / Н. Ю. Бабанов, А. А. Евстифеев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр –

ВНИИЭФ, 2022. — 175 с. — ISBN 978-5-9515-0491-3. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/132622/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Ассоциация по вопросам защиты информации	http://bis-expert.ru/
2	Официальный сайт компании Infowatch	http://www.infowatch.ru/
3	Официальный сайт Лаборатории Касперского	http://www.kaspersky.ru/
4	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование: оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Реферат	30-25/40-33 – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению; 24-19/32-25 – основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы; 18-13/24-17 – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении. 12/16 - тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы;

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые темы рефератов

1. Автоматизированная система обработки информации. Представление информации в АС Классификация возможных угроз информационной безопасности АС. Важные свойства информации и систем ее обработки.

2. Уровни доступа к информации. Анализ угроз информационной безопасности. Базовая эталонная модель взаимодействия открытых систем

3. Протокол. Сеть как набор протоколов

4. Стек протоколов TCP/IP. Соответствие уровней стека TCP/IP уровням модели OSI. IP адресация. Классы IP сетей. Характеристики классов IPадресов. Выделенные IP-адреса.

5. Шлюзы и мосты. Маска подсети. Подсети - первый бастион защиты.

6. Интернет протоколы: Протокол пересылки файлов FTP; Протокол Telnet; Протокол SNMP; Протокол SMTP; Сетевая файловая система NFS; Протокол передачи гипертекста(HTTP); Сервис DNS.

7. Схема инкапсуляции данных в стеке протоколов TCP/IP. ARP-таблица.

8. Проблемы безопасности IP-сетей. Угрозы безопасности IP-сетей. Анализ угроз сетевой безопасности.

9. Схемы сетевой защиты на базе МЭ.

10. Формирование политики межсетевого взаимодействия. Основные схемы подключения МЭ.

11. Персональные и распределенные сетевые экраны.

12. Виртуальные защищенные сети (VPN).

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	**Критерии оценки, балл**
Экзамен представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **-90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо) –** ответ в целом правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно) –** ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично. **-Менее 50 (неудовлетворительно)** – ответы на теоретическую часть неправильные или неполные. Задания не решены

Задания для проведения промежуточной аттестации обучающихся

1. Гарантируют ли очень сложные пароли 100% защиту
2. Как называется преднамеренно внесенный в программное обеспечение объект, приводящий к действиям программного обеспечения не предусмотренным производителем, приводящим к нарушению конфиденциальности и целостности информации?
3. Для чего необходим Firewall?
4. Свойство информации при котором невозможно ее искажение…
5. Обеспечивает ли антивирус 100 % защиту компьютера от вирусов и атак при работе в сети.
6. Укажите количество типов безопасности применительно к одному субъекту в модели Белла-Лападула
7. Совокупность данных, определяющих конкретное преобразование из множества преобразований шифра
8. Сколько групп классов защиты безопасности выделены в Оранжевой книге?
9. Действие take в модели Take-Grand означает:
10. Укажите количество типов преобразований в модели Take-Grand для построения канала утечки информации наоснове tg-цепочки
11. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название…:
12. Самый лучший способ хранения паролей в информационной системе?
13. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа
14. Если компьютер работает в нормальном режиме, означает ли это что он не заражен?
15. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это
16. Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.
17. Можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru:
18. Пластиковая карточка, содержащая чип для криптографических вычислений и встроенную защищенную память для хранения информации:
19. Какая из изученных моделей управления доступом опирается на аппарат теории вероятностей.

20. Часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба

21. Какое количество политик безопасности может быть в одной системе обработки данных

22. Как называется запись определенных событий в журнал безопасности сервера

23. Какая категория субъектов является наиболее рискованной с точки зрения обеспечения информационной безопасности.

24. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

25. Какое ведомство России ведет основные работы по контролю и оценке защищенности систем обработки данных

26. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?

27. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?

28. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?

29. Укажите модель управления доступом, к которой относится основная теорема безопасности сервера

30. Какая категория субъектов является наиболее рискованной с точки зрения обеспечения информационной безопасности.

31. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

32. Какое ведомство России ведет основные работы по контролю и оценке защищенности систем обработки данных

33. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?

34. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?

35. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?

36. Укажите модель управления доступом, к которой относится основная теорема безопасности.

37. Что такое информация в контексте компьютерной безопасности? Какие существуют виды информации с точки зрения ее

конфиденциальности, целостности и доступности?

38. Какие основные угрозы информационной безопасности вы знаете? Приведите примеры.

39. Опишите структуру теории безопасности компьютерных систем. Какие основные компоненты она включает?

40. Что такое модель управления доступом? Какие типы моделей управления доступом существуют?

41. Что такое политика безопасности? Какие виды политик безопасности вы знаете? Приведите примеры.

42. Как вы понимаете термин "уязвимость"? Приведите примеры уязвимостей в компьютерных системах.

43. Какие существуют методы выявления наиболее вероятных маршрутов злоумышленного проникновения на объект защиты?

44. Что такое DDoS-атака? Как она осуществляется и какие существуют методы защиты от нее?

45. Какие существуют угрозы нарушения целостности информации? Приведите примеры.

46. Как злоумышленник может нарушить конфиденциальность информации? Какие существуют методы защиты от таких атак?

47. Какие основные принципы построения систем защиты информации вы знаете?

48. Опишите методы защиты от угроз нарушения целостности информации.

49. Какие существуют средства противодействия в системах с накапливающимся ущербом? Как выбрать оптимальное количество таких средств?

50. Какие существуют методы оценки параметров систем безопасности с отказами?

51. Как можно оптимизировать распределение ресурсов для обеспечения информационной безопасности?

52. Какие существуют программные и аппаратные средства защиты информации? Приведите примеры.

53. Как проводится аудит информационной безопасности?

54. Какие существуют стандарты и нормативные документы в области информационной безопасности?

55. Какова роль человеческого фактора в обеспечении информационной безопасности?

56. Какие этические вопросы возникают в связи с использованием компьютерных систем и информационных технологий?

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Основы системного анализа»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 7

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Основы системного анализа» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе в 1 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – дать студентам знания и навыки, позволяющие им в сложных ситуациях, связанных с процессом принятия решений видеть все составляющие этого процесса, что позволяет при всесторонней компьютерной поддержке исключить случаи, когда принимаются решения явно ошибочные в данных условиях или выбирается альтернатива, далекая от оптимальной.

Задачи изучения дисциплины:

- постижение мировоззренческого и культурного значения теории систем как необходимого результата развития науки с учётом потребностей исследования всё более сложных объектов познания;
- создание базовой теоретической основы и элементарных навыков, необходимых для становления системного мировоззрения и овладения системным подходом;
- овладение понятийным аппаратом теории систем как частью профессионального языка современного менеджера;
-изучение общих законов управления сложными системами;
-овладение начальными навыками прикладного системного анализа в целях их дальнейшего развития в дисциплинах управленческого цикла.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП	Код компетен	Код и наименование	Перечень планируемых результатов обучения по дисциплине	Формы образовательной

(содержание компетенций)	ции	индикатора достижения компетенций	выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	деятельности
Способен проводить анализ безопасности компьютерных систем	**ПК-4**	ПК-4.1 Знать: источники и классификацию угроз информационной безопасности; методы анализа и тестирования компьютерных систем; требования к разработке автоматизированных систем в защищенном исполнении. ПК-4.2 Уметь: разрабатывать модели нарушителя и угроз для компьютерных систем, выделять подсистемы и модули, содержащие критическую информацию. ПК-4.3 Владеть: методами и средствами для проверки выполнения требований информационной безопасности компьютерных систем.	- принципы и подходы целевого планирования и управления; -основные подходы к решению задач планирования и прогнозирования развития экономических систем; - подходы к оценке эффективности стратегических решений в социально-экономических системах; - проблемы развития социально-экономических систем различного уровня экономической иерархии; - система целей социально-экономического развития -целевой подход к анализу стратегии развития социально-экономических систем; - методологии разработки стратегий развития социально-экономических систем	анализировать проблемы развития реальных социально-экономических объектов регионального или корпоративного уровня	анализ состояния и перспектив развития социально-экономических систем; –анализ основных целевых показателей функционирования социально-экономических систем	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									я работа	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Теоретические основы системных исследований	8					10				17	Лабораторный практикум/30
Тема 2. Основные положения и подходы теории управления организацией	8					11				17	Лабораторный практикум/30
Тема 3. Методы и средства моделирования систем	8					11				18	Лабораторный практикум/40
Всего:	**24**					**32**				**52**	**100**
Контроль, час											**Зачет**
Объем дисциплины (в академических часах)	**108**										
Объем дисциплины (в зачетных единицах)	**3**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Теоретические основы системных исследований

Развитие научных знаний и эволюция представлений о действительности. Определенность и неопределенность в теоретических исследованиях и практических приложениях. Аналитическое мышление в науке и практике. Системное мышление как альтернатива аналитическому мышлению. Системность в практической деятельности человека. Сущность диалектического способа мышления. Системность познавательных процессов. Системный анализ как методология изучения объектов (процессов) и исследований, связанных с объектом проблемной ситуации, т. е. с постановкой задачи. Составные части системного анализа как междисциплинарной дисциплины - кибернетика, теория информации, теория принятия решений и т. д. Внедрение системного мировоззрения и системной методологии в науку, технику и практическую деятельность как главный вклад современных системных исследований. Теория циклов. Синергетика как теория самоорганизации систем. Теория катастроф нелинейного развития систем. Сложные системы. Слияние / поглощение как процессы образования новых систем. Классификация и закономерности функционирования систем. Анализ и синтез в системных исследованиях Декомпозиция и агрегирование. Система как целое, обладающее свойствами, отсутствующими у ее составных частей. Система как совокупность элементов, находящихся в определенных отношениях друг с другом и со средой. Иерархичность как свойство систем. Наличие цели, характеристики или критерия качества. Границы системы. Понятия входа и выхода системы и их роль в процессе обмена организации со средой ресурсами и результатами своей деятельности. Система как потенциальный источник данных. Понятие внутренних факторов (переменных). Множественность описаний как следствие относительности любого описания системы Внутреннее и внешнее описание изменения систем во времени. Целостность в системных исследованиях как методологическая установка определения программы исследований. Влияние внутренних и внешних связей на целостность объекта

Тема 2. Основные положения и подходы теории управления организацией

Основные механизмы системной организации. Особенности экономических систем. Вариативные продукты и ресурсы экономических систем. Классическая и неоклассическая теории организации. Подходы к управлению компаний. Предпосылки системного кризиса. Экономика как большая и сложная система. Основные законы управления в кризисных явлениях. Ограниченность системного анализа в исследовании социальных систем. Сложность формализации социальных процессов. Анализ политических процессов

как многокритериальных анализ систем. Описание проблем с целью выявления элементов и критериев решения задачи. Дедукция в анализе проблем управления. Итеративный подход к уточнению проблемы. Индукция в системном анализе. Комбинированный подход в решении проблем системного анализа (формулирование и уточнение целей при анализе каждого фактора. Структурирование и формализация в системном анализе. Организационные ресурсы как средство достижения целей. Типы ресурсов. Входные ресурсы (материалы, энергия, услуги, кадры, финансы, информация. Конечность и ограниченность ресурсов при планировании. Распределение ресурсов для выполнения задач проектов. Методы управления ресурсами. Линейное программирование как метод распределения ресурсов. Принцип обратной связи как фундаментальное общенаучное понятие в сфере управления. Информация как ресурс. Виды современных ИС. Преимущества технологий цифровой экономики.

Тема 3. Методы и средства моделирования систем

Моделирование как этап целенаправленной деятельности. Цель как модель. Эмпирические и логические методы познания. Классификация моделей. Познавательные и прагматические модели. Соответствие модели действительности. Имитационные модели. Информационные системы, современные компьютерные технологии в моделировании. Этапы разработки моделей. Моделирование от простого к сложному. Усложнение и упрощение модели. Построение моделей «сверху вниз» и «снизу –вверх». Языки моделирования. Абстрагирование как процесс выделения наиболее существенных элементов проблемы (объекта). Проверка адекватности модели. Критерии выбора модели. Интерпретация данных, полученных в процессе моделирования. Структурно-функциональное моделирование. Стандарт IDEF0. Основные компоненты диаграмм IDEF0 моделей бизнес-процессов предметной области. Правила декомпозиции. Нотация DFD. Формирование ER-модели. Разработка BPMN-моделей. Объектно-ориентированное моделирование. Диаграммы вариантов использования, деятельности, последовательности. Реализация методов статистического анализа в современных программных средствах.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Макрусев, В. В. Основы системного анализа : учебник / В. В. Макрусев. — 2-е изд.. — Санкт-Петербург : Троицкий мост, 2022. — 250 с. — ISBN 978-5-4377-0138-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/111173/details

2. Лукьянова, Л. М. Основы теории систем и системного анализа: в

2 книгах. Кн.1: основы теории систем : учебное пособие / Л. М. Лукьянова. — Калининград : Балтийский федеральный университет им. Иммануила Канта, 2024. — 216 с. — ISBN 978-5-9971-0846-5. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/155210/details

Дополнительная литература:

1. Глушань, В. М. Основы системного анализа. В 2 частях. Ч.1 : учебное пособие / В. М. Глушань. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2022. — 89 с. — ISBN 978-5-9275-4112-6 (ч.1), 978-5-9275-4111-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/125707/details

2. Глушань, В. М. Основы системного анализа. В 2 частях. Ч.2 : учебное пособие / В. М. Глушань, О. Р. Норкин, С. С. Парфенова. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2023. — 128 с. — ISBN 978-5-9275-4111-9, 978-5-9275-4428-8 (ч.2). — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/135658/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Интернет-проект «Корпоративный менеджмент»	http://www.cfin.ru /
2	Портал iTeam- Технологии корпоративного управления	https://iteam.ru/blog/
3	Системный анализ – ключевой элемент системного и критического подход	https://1economic.ru/lib/114184?ysclid=ms78qgg8de276232463

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информатики, технологий и методов программирования

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; оснащена рабочими местами на базе вычислительной техники, подключенными к локальной вычислительной сети и сети "Интернет", сетевым программным обеспечением, обучающим программным обеспечением

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Контрольная работа	12–11/13-11 – верные ответы составляют более 90% от общего количества; 10–7 – верные ответы составляют 80–50% от общего количества; 6–0 – менее 50% правильных ответов.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые задания для лабораторных практикумов

1. Моделирование бизнес-процессов управления

1. Разработать диаграммы IDE0 трёх уровней на заданную тему (по вариантам).
2. Разработать диаграмму DFD.
3. Указать в готовой диаграмме IDEF0 ошибки.
4. Использовать программное средство RAMUS для разработки структурно-функциональной модели предметной области.

2. Разработка объектно-ориентированных моделей описания предметной области

1. Разработать диаграммы UML (вариантов использования), описывающие предметную область на индивидуальные темы.
2. Разработать диаграммы деятельности, описывающие процессы предметной области.
3. Продемонстрировать использование ArgoUML для описания предметной области.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	Критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной

Краткая характеристика оценочного средства	Критерии оценки, балл
	шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов «Зачтено» – 90-100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Системный анализ как методология постановки, исследования и решения сложных и взаимосвязанных проблем.
2. Системный подход к решению сложных проблем.
3. Специфика применения системного анализа в задачах управления и решения проблем.
4. Развитие организации как задача управления эффективностью.
5. Информационные технологии в системном анализе.
6. Целевой подход к процессу решения проблем: содержание, основные понятия (ценности, цели, политика, решения) и особенности применения.
7. Проблема совершенствования управления: рациональность и эффективность управления.
8. Структурирование и формализация в системном анализе
9. Сложность формализации социально-экономических процессов
10. Кибернетика как наука об управлении на основе информации и общих законах управления.
11. Принцип обратной связи как фундаментальное общенаучное понятие в сфере управления.
12. Рациональность и эффективность решений в управлении

организацией.

13. Организационные ресурсы как средство достижения целей.

14. Управление как инструмент эффективного расходования ресурсов

15. Индукция, дедукция и комбинированный подход в решении проблем системного анализа.

16. Методы управления ресурсами.

17. Информация как ресурс. Преимущества технологий цифровой экономики.

18. Моделирование как этап целенаправленной деятельности.

19. Классификация моделей.

20. Этапы разработки моделей.

21. Языки моделирования.

22. Структурно-функциональное моделирование. Стандарт IDEF0. Основные компоненты диаграмм IDEF0 моделей бизнес-процессов предметной области.

23. Правила декомпозиции в структурно-функциональном моделировании. Нотация DFD. Формирование ER-модели.

24. Объектно-ориентированное моделирование с использованием UML. Диаграммы вариантов использования

25. Объектно-ориентированное моделирование. Диаграммы деятельности.

26. Программные средства статистического анализа.

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Технология обеспечения информационной безопасности»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 6

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 7

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 11

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Технологии обеспечения информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 1 курсе в 2 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование у обучающихся знаний в области технологий обеспечения информационной безопасности; изучение и освоение основных технологий, используемых при формировании системы защиты информации предприятия.

Задачи изучения дисциплины: анализ основных видов технологий обеспечения безопасности; изучение и освоение состава подсистем системы защиты информации, особенностей их создания и внедрения.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**УК-1**	УК-1.1. Знает процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения	типовую структуру системы защиты информации; методики анализа результатов исследования	разрабатывать стратегию проведения исследований; анализировать структуру систем защиты информации	организации процесса принятия решения	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа
		УК-1.2. Уметь принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий	методики разработки стратегий действий при проблемных ситуациях	принимать конкретные решения для повышения эффективности процедур анализа проблем	применения полученных знаний в научно-исследовательской и практической работе	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа
		УК-1.3. Владеть методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий и действий при проблемных ситуациях	методики постановки цели и определения способов ее достижения	пользоваться методами установления причинно-следственных связей и определения наиболее значимых среди них	постановки цели и определения способов ее достижения	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа

Способен обосновывать необходимость защиты информации в автоматизированной системе	**ПК-1**	ПК-1.1. Знать: основные положения отечественных и зарубежных стандартов по оценке информационной безопасности автоматизированных систем; понятие и виды защищаемой информации, требования к эффективному использованию системы мониторинга и аудита процессов обеспечения информационной безопасности.	основные национальные и зарубежные стандарты в области обеспечения информационной безопасности	работать со стандартами и нормативными документами в своей профессиональной деятельности	Использования международных и национальных стандартов в области информационной безопасности	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа
		ПК-1.2. Уметь: проводить оценку соответствия объекта требованиям нормативных документов и стандартам по информационной безопасности.	основные этапы проектирования систем защиты информации	проектировать системы защиты информации с использованием различных технологий обеспечения информационной безопасности	проектирования системы защиты информации	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа
		ПК-1.3. Владеть: навыками анализа и подготовки содержания нормативно-распорядительных и иных документов для поддержки безопасного функционирования объектов, в том числе в автоматизированных системах.	основные разделы технического задания на проектирование системы защиты информации	пользоваться приобретёнными знаниями для формирования проекта технического задания на создание системы защиты информации	участия в разработке системы защиты информации объекта	Контактная работа: Лекции Лабораторный практикум Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Требования к технологии управления информационной безопасностью. Основные принципы реализации технологий обеспечения безопасности	6	7				8				6	Контрольная работа/25
Тема 2. Основные виды технологий обеспечения информационной безопасности	6	7				8				6	Контрольная работа/25
Тема 3. Структура и состав подсистем системы защиты информации	6	7				8				6	Контрольная работа/25
Тема 4. Проектирование и внедрение системы защиты информации	6	7				8				6	Контрольная работа/25
Всего:	**24**	**28**				**32**				**24**	**100**
Контроль, час	**36**										**Экзамен**
Объем дисциплины (в академических часах)	**144**										
Объем дисциплины (в зачетных единицах)	**4**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Требования к технологии управления информационной безопасностью. Основные принципы реализации технологий обеспечения безопасности

Предмет и содержание дисциплины, основные понятия, методы изучения, основная литература, контроль освоения дисциплины. Основные стадии развития средств и методов защиты информации. Типовая структура системы защиты информации. Базовые требования к технологии управления информационной безопасностью. Основные принципы реализации технологий обеспечения безопасности.

Тема 2. Основные виды технологий обеспечения информационной безопасности

Особенности IPS-систем по выявлению и предотвращению вторжений. Роль межсетевого экранирования и основные классы межсетевых экранов. Защита от компьютерных вирусов. Идентификация и аутентификация пользователей и основные используемые при этом технологии. Основные методы реализации доступа к информации. Особенности криптографической защиты информации. Назначение DLP-систем.

Тема 3. Структура и состав подсистем системы защиты информации

Основные функциональные и обеспечивающие подсистемы системы защиты информации. Назначение функциональных и обеспечивающих подсистем. Классификация автоматизированных систем с учётом обеспечения информационной безопасности и требования по защите информации. Основные функциональные подсистемы и требования по уровню защищённости, предъявляемые к ним.

Тема 4. Проектирование и внедрение системы защиты информации

Основные этапы разработки системы защиты информации. Назначение и структура технического задания на систему. Состав технического и рабочего проектов. Особенности внедрения системы защиты информации.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 4-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 424 с. — ISBN 978-5-4497-2415-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].

— URL: https://www.iprbookshop.ru/books/133955/details

2. Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства : практикум / Д. В. Фомин. — Саратов : Вузовское образование, 2021. — 218 c. — ISBN 978-5-4487-0795-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/110329/details

Дополнительная литература:

1. Аль-Ханани, М. А. А. Защита информации. Dallas Lock : практикум / М. А. А. Аль-Ханани. — Москва : Ай Пи Ар Медиа, 2024. — 73 c. — ISBN 978-5-4497-2809-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/138377/details

2. Александрова, Е. Б. Криптографические методы защиты информации. Элементы алгебраической геометрии : учебное пособие / Е. Б. Александрова, А. В. Ярмак. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2023. — 106 c. — ISBN 978-5-7422-8017-0. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/143094/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Официальный сайт компании Infowatch	https://www.infowatch.ru/analytics
2	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/
3	СКЗИ: что это, и для чего используются криптографические средства защиты информации	https://selectel.ru/blog/cryptographic-protecting-information/?ysclid=ms79u5w0si883656710

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информатики, технологий и методов

программирования

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; оснащена рабочими местами на базе вычислительной техники, подключенными к локальной вычислительной сети и сети "Интернет", сетевым программным обеспечением, обучающим программным обеспечением

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Контрольная работа	25–20 – верные ответы составляют более 90% от общего количества; 19–13 – верные ответы составляют 80-50% от общего количества; 12–0 – менее 50% правильных ответов.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые задания для контрольных работ

1. Какой ГОСТ Р содержит свод норм и правил применения мер обеспечения информационной безопасности?

2. Определите соответствие между понятиями:

3. Идентификация – процедура, в результате выполнения которой для субъекта выявляется его уникальный признак, однозначно определяющий его в информационной системе.

4. Аутентификация – процедура проверки подлинности, например, проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

5. Авторизация – предоставление определенному лицу прав на выполнение определенных действий

6. Что такое эффективность защиты информации?

7. Кто устанавливает политику информационной безопасности компании?

8. В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам – это…

9. Определите соответствие между определением стратегии защиты информации и содержанием:

оборонительная — защита от уже известных угроз, осуществляемая автономно, т. е. без оказания существенного влияния на информационно-управляющую систему;

наступательная — защита от всего множества потенциально возможных угроз, при осуществлении которой в архитектуре информационно-управляющей системы и технологии ее функционирования должны учитываться условия, продиктованные потребностями защиты;

упреждающая — создание информационной среды, в которой угрозы информации не имели бы условий для проявления

10. Как определяется в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" конфиденциальность информации?

11. Как определяется в соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" распространение информации?

12. Может ли быть ограничен доступ к нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления?

13. Какой орган исполнительной власти 12наделен полномочием выдавать лицензии на деятельность по созданию средств защиты информации, предназначенные для защиты (сохранения) государственной тайны?

14. В соответствии с комплексным (системным) подходом приступать к созданию системы защиты информации можно, когда определены следующие ее компоненты:

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	Критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **-90 и более (отлично)** – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. **-70 и более (хорошо) –** ответ в целом

Краткая характеристика оценочного средства	Критерии оценки, балл
	правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **-50 и более (удовлетворительно) –** ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично. **-Менее 50 (неудовлетворительно)** – ответы на теоретическую часть неправильные или неполные. Задания не решены

Задания для проведения промежуточной аттестации обучающихся

1. Основные этапы развития методов и средств защиты информации в процессе эволюции человечества.
2. Базовые элементы типовой системы защиты информации (СЗИ).
3. Основные принципы реализации технологий обеспечения безопасности.
4. Характеристика DLP-систем, представленных на российском рынке.
5. Основные методы реализации доступа к информации.
6. Базовые задачи, решаемые межсетевыми экранами.
7. Особенности биометрической системы защиты информации.
8. Основные алгоритмы криптографической защиты информации.
9. Функциональные подсистемы системы защиты информации.
10. Основные требования к криптографической подсистеме СЗИ.
11. Основные требования к подсистеме обеспечения целостности СЗИ.
12. Характеристика современных IPS-систем по обнаружению и предотвращению вторжений.
13. Характеристика антивирусных программных комплексов на российском рынке.
14. Основные стадии проектирования системы защиты информации.
15. Базовые разделы технического задания на СЗИ.
16. Особенности внедрения СЗИ.

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины
«Разработка и реализация проектов в сфере информационной безопасности»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 6

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 8

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ..... **ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 9

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 12

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Разработка и реализация проектов в сфере информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе в 3 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – формирование теоретических знаний и практических умений по разработке и реализации проектов в сфере информационной безопасности.

Задачи изучения дисциплины:

- изучение этапов жизненного цикла проекта, разработки и реализации проекта;
- овладение методиками разработки проекта с учетом анализа альтернативных вариантов его реализации, определения целевых этапов, основных направлений работы, навыками управления проектом на всех этапах его жизненного цикла.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен управлять проектом на всех этапах его жизненного цикла	**УК-2**	УК-2.1. Знает методы управления проектами; этапы жизненного цикла проекта. УК-2.2. Уметь разрабатывать и анализировать альтернативные варианты проектов для достижения намеченных результатов; разрабатывать проекты, определять целевые этапы и основные направления работ. УК-2.3. Владеть навыками разработки проектов в избранной профессиональной сфере; методами оценки эффективности проекта, а также потребности в ресурсах	этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами	разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять целевые этапы, основные направления работ; объяснить цели и сформулировать задачи, связанные с подготовкой и реализацией проекта; управлять проектом на всех этапах его жизненного цикла	владеть методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта	Контактная работа: Практическое занятие Самостоятельная работа

Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**ПК-3**	ПК-3.1 Знать: основные понятия, используемые при проектировании, создании, модернизации системы защиты информации объектов информатизации, в том числе автоматизированных систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. ПК-3.2 Уметь: проводить рациональный выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; организацию защиты информации от утечки по техническим каналам на объектах информатизации. ПК-3.3 Владеть: навыками разработки требований информационной безопасности к объектам; формирования проектных решений по защите информации в автоматизированных системах.	основные понятия, используемые при проектировании, создании, модернизации системы защиты информации объектов информатизации, в том числе автоматизированных систем.	ь проводить рациональный выбор программно-аппаратных средств обеспечения информационной безопасности объекта информатизации	владеть навыками разработки требований информационной безопасности к объектам; формирования проектных решений по защите информации	Контактная работа: Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Описание объекта информатизации				8						7	Тест/10
Тема 2. Сбор и систематизация сведений об объекте информатизации. Подбор необходимых нормативно-распорядительных документов				8						7	Тест/10
Тема 3. Формирование требований защищенности объекта информатизации				7						7	Тест/10
Тема 4. Категорирование информации и других ресурсов. Анализ руководящих документов				7						7	Тест/10
Тема 5. Анализ угроз и уязвимостей объекта информатизации				7						7	Тест/10
Тема 6. Подбор и применение методики для формирования модели угроз				7						7	Тест/10
Тема 7. Анализ существующей системы информационной безопасности				7						7	Тест/10
Тема 8. Комплексный анализ модели угроз и уязвимостей и существующих мер защиты информации				7						7	Тест/10
Тема 9. Подбор необходимых мер и средств защиты на основе проведенного				7						8	Тест/10

анализа											
Тема 10. Формирование комплексного проекта мер обеспечения защищенности объекта информатизации				7						8	Тест/10
Всего:				**72**						**72**	**100**
Контроль, час											**Зачет**
Объем дисциплины (в академических часах)	**144**										
Объем дисциплины (в зачетных единицах)	**4**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Описание объекта информатизации

Общие сведения об объекте информатизации. Состав программного обеспечения. Класс защищённости автоматизированной системы. Основные объекты защиты информации и их классификация

Тема 2. Сбор и систематизация сведений об объекте информатизации. Подбор необходимых нормативно-распорядительных документов

Инвентаризация имеющихся информационных ресурсов и обеспечивающих их формирование, поддержание и использование информационных технологий. Организационные документы. Распорядительные документы.

Тема 3. Формирование требований защищенности объекта информатизации

Принятие решения о необходимости защиты обрабатываемой информации. Классификация объекта по требованиям защиты информации. Определение угроз безопасности информации. Определение требований к системе защиты информации. Основные документы, формируемые по результатам исполнения работ на этапе формирования требований к системе защиты информации.

Тема 4. Категорирование информации и других ресурсов. Анализ руководящих документов

Установление градации важности защищаемой информации (объекта защиты) с точки зрения нормативных правовых требований, ценности, критичности и чувствительности к неавторизованному раскрытию или модификации. Анализ руководящих документов. Требования ГОСТ Р ИСО/МЭК 27002-2021. Цель категорирования.

Тема 5. Анализ угроз и уязвимостей объекта информатизации

Определение угроз. Анализ уязвимостей. Экспертная оценка. Статистический анализ рисков. Факторный анализ.

Тема 6. Подбор и применение методики для формирования модели угроз

Определение негативных последствий. Инвентаризация информационных систем и сетей. Определение источников угроз и оценка возможностей нарушителей. Оценка способов реализации угроз. Определение актуальности угроз

Тема 7. Анализ существующей системы информационной безопасности

Управление доступом. Физическая безопасность. Сетевая безопасность. Безопасность приложений. Управление уязвимостями. Аудит безопасности.

Тема 8. Комплексный анализ модели угроз и уязвимостей и существующих мер защиты информации

Определение основных ресурсов информационной системы.

Идентификация имеющихся угроз и уязвимостей. Расчёт рисков, связанных с реализацией угроз безопасности. Анализ существующих мер защиты информации. Разработка рекомендаций по улучшению защиты информации.

Тема 9. Подбор необходимых мер и средств защиты на основе проведенного анализа

Определение возможных угроз. Оценка последствий проявлений угроз. Разработка методов и средств защиты. Оценка эффективности выбранных методов и средств защиты.

Тема 10. Формирование комплексного проекта мер обеспечения защищенности объекта информатизации

Анализ объекта информатизации. Разработка документации. Проектирование подсистем технической защиты информации. Анализ эффективности спроектированной системы.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Дронов, В. Ю. Бизнес-процесс «Обеспечение информационной безопасности организации» : учебное пособие / В. Ю. Дронов, Г. А. Дронова. — Новосибирск : Новосибирский государственный технический университет, 2021. — 76 с. — ISBN 978-5-7782-4537-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/126547/details

2. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 5-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2026. — 581 с. — ISBN 978-5-4497-1653-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/160032/details

Дополнительная литература:

1. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. — ISBN 978-5-9729-0864-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/124242/details

2. Ивановский, М. А. Управление ИТ-проектами : учебное пособие / М. А. Ивановский, И. А. Глазкова. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2025. — 129 с. — ISBN 978-5-8265-2876-1. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/154966/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/
2	Security by design на практике: проектирование безопасной инфраструктуры	https://habr.com/ru/companies/selectel/articles/963986/?ysclid=ms7adunhxw517364659
3	Судьба требований ГОСТ 34-й серии в проектах по информационной безопасности	https://www.anti-malware.ru/practice/methods/GOST-requirements-34th-series-in-information-security-projects?ysclid=ms7adrvxed474217131

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Контрольная работа	25–20 – верные ответы составляют более 90% от общего количества; 19–13 – верные ответы составляют 80-50% от общего количества; 12–0 – менее 50% правильных ответов.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые задания к контрольным работам

1. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию и на информацию ограниченного доступа, к которой можно отнести:
   а. государственная тайна;
   б. служебная тайна;
   в. конфиденциальная информация;
   г. персональные данные;
   д. все ответы верны.

2. Распределите следующие информационные ресурсы по видам: 1 - общедоступная информация и 2 -информация, которую можно отнести к коммерческой тайне:
   а. информация о ноу-хау;
   б. условия действующих контрактов;
   в. документы, дающие право на осуществление предпринимательской деятельности;
   г. планы, перспективы, предполагаемые шаги по развитию компании;
   д. учредительные документы юридического лица;
   е. о численности и оплате труда работников некоммерческих организаций.

1. Проектирование системы предполагает выполнение ряда стадий, в том числе (отметьте необходимые):
   а. формирование требований к системе,
   б. разработку концепции системы,
   в. разработку технического задания,

г. эскизное проектирование,
д. техническое проектирование
е. разработку рабочей документации,
ж. все перечисленные стадии необходимы

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию и на информацию ограниченного доступа, к которой можно отнести:

а. государственная тайна;
б. служебная тайна;
в. конфиденциальная информация;
г. персональные данные;
д. все ответы верны.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Краткая характеристика оценочного средства	Критерии оценки, балл
Экзамен представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0–30 баллов Задание 2: 0–30 баллов Задание 3: 0–40 баллов -90 и более (отлично) – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. -70 и более (хорошо) – ответ в целом правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. -50 и более (удовлетворительно) – ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично. -Менее 50 (неудовлетворительно) – ответы на теоретическую часть неправильные или неполные. Задания не решены

Задания для проведения промежуточной аттестации обучающихся

1. С какого этапа необходимо начинать разработку системы информационной безопасности? Какие мероприятия могут быть заложены на данном этапе?
2. Что включает в себя комплексная система информационной безопасности?
3. Перечислите план мероприятий (задач), которые необходимо реализовать для защиты коммерческой тайны согласно N98 ФЗ «О коммерческой тайне»?
4. Приведите примеры организационных мер защиты информации, принимаемых при разработке и реализации проектов в сфере информационной безопасности.
5. Расшифруйте аббревиатуру и дайте определение ГИС.
6. Расшифруйте аббревиатуру и дайте определение ИСПДн.
7. Расшифруйте аббревиатуру КИИ. Что относится к объектам КИИ?
8. Расшифруйте аббревиатуру и приведите примеры СЗИ.
9. Приведите примеры стадий проектирования системы информационной безопасности.
10. Как определить необходимый набор требования по защите информации для ИСПДн?
11. Дайте определение технического задания на создание системы.
12. Как определить наличие и актуальность сертификата ФСТЭК у средства защиты информации?
13. Что такое «объект информатизации»?
14. Что такое «обезличивание ПДн» и в каких целях оно производится?
15. Какой основной документ выдается по результатам проведения аттестационных испытаний объекта информатизации?
16. Опишите этапы жизненного цикла системы ИБ
17. Сформулируйте причину(ы) привлечения к процессу анализа информационных рисков при автоматизированной обработке информации специалистов из различных подразделений компании?
18. Что такое «пентестинг»?
19. Раскройте понятие «частные политики ИБ».
20. Какие категории сведений, обрабатываемых в АС, можно отнести к сведениям конфиденциального характера (защищаемой информации)?
21. Сформулируйте цель обеспечения безопасности автоматизированной системы
22. Приведите примеры преднамеренных угроз информационной безопасности АС.
23. Приведите примеры непреднамеренных угроз информационной безопасности АС.
24. Перечислите методы разграничения доступа в автоматизированных системах.

25. Что такое политика информационной безопасности автоматизированной системы?
26. Раскройте термин «событие информационной безопасности».
27. Что такое техническое задание на разработку системы защиты? Для чего этот документ нужен?
28. Что такое «Руководство пользователя по средствам безопасности»? Для чего этот документ нужен?
29. Что такое «Руководство администратора по средствам безопасности»? Для чего этот документ нужен?
30. Из каких этапов состоит процесс проектирования системы защиты информации?
31. Что такое уязвимость? И как она связана с атакой?
32. Что такое модель угроз безопасности информации?
33. Какими нормативными документами регламентируется построение модели угроз ИБ?
34. Что такое модель нарушителя?
35. Какими нормативными документами регламентируется построение модели нарушителя?
36. Что такое предпроектное обследование объекта?
37. Что такое уровень защищенности «ИСПДн»?
38. Какие есть уровни защищенности «ИСПДн»?
39. Какие регуляторы есть в сфере информационной безопасности?
40. Какие ГИС существуют? Опишите их.
41. Кто занимается проектированием системы ИБ? Зависит ли это от вида организации?
42. Опишите примерный состав эксплуатационной документации, разрабатываемой на этапе проектирования системы ИБ?
43. Что относится к организационным мерам защиты информации?
44. Опишите жизненный цикл системы защиты информации?
45. Что такое «Акт классификации по требованиям безопасности информации»?

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Организационно-правовые механизмы обеспечения информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе в 3 семестре.

Цели и задачи дисциплины

Цель изучения дисциплины – слушатель получает систематизированные теоретические знания в области законодательных основ обеспечения информационной безопасности и их практического применения на российских предприятиях различных форм собственности.

Задачи изучения дисциплины:

Эксплуатационная деятельность • установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований; • администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем. Проектно-технологическая деятельность • сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности; • проведение проектных расчетов элементов систем обеспечения информационной безопасности; • участие в разработке технологической и эксплуатационной документации; • проведение предварительного технико-экономического обоснования проектных расчетов. Экспериментально-исследовательская деятельность • сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования; • проведение экспериментов по заданной методике, обработка и анализ их результатов; • проведение вычислительных экспериментов с использованием стандартных программных средств. Организационно-управленческая деятельность • осуществление организационно-правового обеспечения информационной безопасности объекта защиты; • организация работы малых коллективов исполнителей; • участие в совершенствовании системы управления информационной

безопасностью; • изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа; • контроль эффективности реализации политики информационной безопасности объекта защиты.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	**ПК-5**	ПК-5.1 Знать: основы формирования политики информационной безопасности; основные принципы и методы комплексной защиты информации. ПК-5.2 Уметь: формировать политику информационной безопасности; подбирать меры и средства обеспечения информационной безопасности на объекте защиты. ПК-5.3 Владеть: навыками выявления угроз и технические каналы утечки информации ограниченного доступа; разработки требований информационной безопасности к объектам информатизации.	Сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности общества и государства	Применять основные методы обеспечения информационной безопасности	Базовой терминологией и гуманитарным и аспектами в области информационной безопасности личности, общества и государства	Контактная работа: Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Введение в организационное и правовое обеспечение информационной безопасности.	2	2				3				5	Отчета по лабораторному практикуму/10
Тема 2 Организационные основы защиты информации.	2	2				3				5	Отчета по лабораторному практикуму/10
Тема 3 Отнесение сведений к конфиденциальной информации.	2	2				3				5	Отчета по лабораторному практикуму/10
Тема 4 Организация допуска и доступа персонала к конфиденциальной информации.	2	2				3				5	Отчета по лабораторному практикуму/10
Тема 5 Организация внутриобъектового и пропускного режимов на предприятии.	2	2				3				5	Отчета по лабораторному практикуму/10
Тема 6 Организация защиты информации при проведении совещаний, в ходе издательской и рекламной деятельности.	2	2				3				3	Отчета по лабораторному практикуму/10
Тема 7 Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу.	2	2				2				2	Отчета по лабораторному практикуму/10
Тема 8 Допуск	1	1				2				3	Отчета по

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
предприятий к проведению работ с конфиденциальной информацией.											лабораторному практикуму/10
Тема 9 Правовая защита конфиденциальной информации.	1	1				2				2	Отчета по лабораторному практикуму/10 Реферат/10
Всего:	**16**	**16**				**24**				**52**	**100**
Контроль, час											**Зачет**
Объем дисциплины (в академических часах)	**108**										
Объем дисциплины (в зачетных единицах)	**3**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Введение в организационное и правовое обеспечение информационной безопасности.

История возникновения органов защиты информации. Концептуальные основы информационной безопасности.

Тема 2 Организационные основы защиты информации.

Основные принципы и условия организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Основные силы и средства, используемые для организации защиты информации. Организация охраны предприятий. Организация аналитической работы и контроля состояния защиты конфиденциальной информации.

Тема 3 Отнесение сведений к конфиденциальной информации.

Засекречивание и рассекречивание сведений. Отнесение сведений к различным видам конфиденциальной информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей. Отнесение сведений к коммерческой тайне.

Тема 4 Организация допуска и доступа персонала к конфиденциальной информации.

Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну. Порядок доступа к конфиденциальной информации командированных лиц. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей.

Тема 5 Организация внутриобъектового и пропускного режимов на предприятии.

Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима. Силы и средства, используемые при организации внутриобъектового режима. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

Тема 6 Организация защиты информации при проведении совещаний, в ходе издательской и рекламной деятельности.

Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации.

Тема 7 Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу.

Порядок передачи различных видов конфиденциальной информации иностранным государствам. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.

Тема 8 Допуск предприятий к проведению работ с конфиденциальной информацией.

Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий. Организация проведения государственной аттестации руководителей предприятий. Организация аналитической работы и контроля состояния защиты конфиденциальной информации. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.

Тема 9 Правовая защита конфиденциальной информации.

Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну. Уголовно-правовая защита в сфере компьютерной информации. Уголовно-правовая защита сведений, составляющих государственную тайну. Административно-правовая защита информации с ограниченным доступом. Гражданско-правовая защита служебной и коммерческой тайны. Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений. Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения данной дисциплины используются такие виды учебной работы, как лекция, лабораторный практикум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к зачету.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции, обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические указания для обучающихся по выполнению лабораторных практикумов

Лабораторные практикумы выполняются в соответствии с рабочим учебным планом при последовательном изучении тем дисциплины.

Порядок проведения практикума.

1. Получение задания и рекомендаций к выполнению практикума.
2. Настройка инструментальных средств, необходимых для выполнения практикума.
3. Выполнение заданий практикума.
4. Подготовка отчета в соответствии с требованиями.
5. Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций, рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии.

Требования к оформлению результатов практикумов (отчет)

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14, выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине определяется учебным планом.

При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя.

Работа с литературой (конспектирование)

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала,

формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине «Специальная математика и основы статистики» определяется учебным планом.

При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.

Реферат

Подготовка рефератов направлена на развитие и закрепление у обучающихся навыков самостоятельного глубокого, творческого и всестороннего анализа научной, методической и другой литературы по актуальным проблемам дисциплины; на выработку навыков и умений грамотно и убедительно излагать материал, четко формулировать теоретические обобщения, выводы и практические рекомендации.

Рефераты должны отвечать высоким квалификационным требованиям в отношении научности содержания и оформления.

Темы рефератов, как правило, посвящены рассмотрению одной проблемы. Объем реферата может быть от 12 до 15 страниц машинописного текста, отпечатанного через 1,5 интервала, а на компьютере через 1 интервал (список литературы и приложения в объем не входят).

Текстовая часть работы состоит из введения, основной части и заключения.

Во введении обучающийся кратко обосновывает актуальность избранной темы реферата, раскрывает конкретные цели и задачи, которые он собирается решить в ходе своего небольшого исследования.

В основной части подробно раскрывается содержание вопроса (вопросов) темы.

В заключении кратко должны быть сформулированы полученные

результаты исследования и даны выводы. Кроме того, заключение может включать предложения автора, в том числе и по дальнейшему изучению заинтересовавшей его проблемы.

В список литературы (источников и литературы) обучающийся включает только те документы, которые он использовал при написании реферата.

В приложении (приложения) к реферату могут выноситься таблицы, графики, схемы и другие вспомогательные материалы, на которые имеются ссылки в тексте реферата.

Навигация для обучающихся по самостоятельной работе в рамках изучения дисциплины

Наименование темы	**Вопросы, вынесенные на самостоятельное изучение**	**Формы самостоят. работы**	**Форма текущего контроля**
Тема 1. Введение в организационное и правовое обеспечение информационной безопасности.	Концептуальные основы информационной безопасности	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 2 Организационные основы защиты информации.	Организация аналитической работы и контроля состояния защиты конфиденциальной информации.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 3 Отнесение сведений к конфиденциальной информации.	Отнесение сведений к коммерческой тайне.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 4 Организация допуска и доступа персонала к конфиденциальной информации.	Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 5 Организация внутриобъектового и пропускного	Основные элементы системы организации пропускного режима, используемые силы и	Работа с литературой, включая ЭБС, источниками в сети Internet	Отчет по лабораторному практикуму

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоят. работы	Форма текущего контроля
режимов на предприятии.	средства.	Подготовка к лабораторному практикуму, подготовка отчета по практикуму	
Тема 6 Организация защиты информации при проведении совещаний, в ходе издательской и рекламной деятельности.	Основы организации защиты информации в ходе взаимодействия со средствами массовой информации.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 7 Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу.	Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 8 Допуск предприятий к проведению работ с конфиденциальной информацией.	Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 9 Правовая защита конфиденциальной информации.	Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму Реферат

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Овчинникова, Е. А. Организационно-правовые основы информационной безопасности. Ч.1 : учебное пособие / Е. А. Овчинникова, Г. В. Попков ; под редакцией С. Н. Новикова. —

Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2022. — 193 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/138773/details

2. Овчинникова, Е. А. Организационно-правовые основы информационной безопасности. Ч.2 : учебное пособие / Е. А. Овчинникова, Г. В. Попков ; под редакцией С. Н. Новикова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2022. — 168 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/138774/details

Дополнительная литература

1. Алексеева, М. В. Информационное право : учебное пособие / М. В. Алексеева, С. В. Рыбак, М. Б. Смоленский. — Ростов-на-Дону : Донской государственный технический университет, 2022. — 190 с. — ISBN 978-5-7890-2005-0. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/130406/details

2. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 197 с. — ISBN 978-5-4497-4146-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/148558/details

3. Полтавцева, М. А. Организационные и правовые аспекты информационной безопасности : учебное пособие / М. А. Полтавцева. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2023. — 145 с. — ISBN 978-5-7422-8431-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/147727/details

4. Серго, А. Г. Основы права интеллектуальной собственности для ИТ-специалистов : учебное пособие / А. Г. Серго, В. С. Пущин. — 4-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 292 с. — ISBN 978-5-4497-2422-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/133961/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№ п/п	Наименование ресурса	Ссылка
2.	Конституционный Суд Российской Федерации	http://www.ksrf.ru
3.	Президент Российской Федерации	http://www.kremlin.ru
4.	Правительство Российской Федерации	http://government.ru
5.	Официальная Россия. Сервер органов государственной власти Российской Федерации.	http://www.gov.ru

№ п/п	Наименование ресурса	Ссылка
6.	Государственная Дума Федерального Собрания Российской Федерации	http://www.duma.gov.ru
7.	Российская национальная библиотека.	http://www.nlr.ru

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информационных технологий для проведения лабораторных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; набор демонстрационного оборудования (проектор, экран).

Аудитория (защищаемое помещение)

Предназначена для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при

осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ

АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Виды контактной работы, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	10–8 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, использована требуемая информация, написан корректно работающий код, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все вопросы по работе программы; 7–5 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, написан корректно работающий код, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 4–3 – работа и отчет выполнены в срок, в основном самостоятельно, использованы соответствующие формулы; имеются недочеты в коде программы; необходимые выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 2–1 – обучающийся подготовил работу и отчет несамостоятельно или не завершил в срок, выводы и ответы на вопросы отсутствуют.
4.	Реферат	10 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 5 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 2 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

1 Лабораторная работа № 1. Закрепление права предприятия на защиту информации в нормативных документах

1.1 Цель работы

Освоение метода правовой защиты информации ограниченного доступа на предприятии.

1.2 Теоретическая часть

Организационно-правовое обеспечение информационной безопасности представляет совокупность законов и других нормативно-правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения *защиты информации*, так и организацию, и функционирование защиты конкретных объектов и систем.

Правовые аспекты организационно-правового обеспечения информационной безопасности направлены на достижение следующих целей:

− формирование правосознания граждан по обязательному соблюдению правил защиты конфиденциальной информации;

− определение мер ответственности за нарушение правил защиты информации;

− придание юридической силы технико-математическим решениям вопросов организационно-правового обеспечения защиты информации;

− придание юридической силы процессуальным процедурам разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

Информационные отношения достигли такой ступени развития, на которой оказалось возможным сформировать самостоятельную отрасль законодательства, регулирующую информационные отношения. В эту отрасль, которая целиком посвящена вопросам информационного законодательства, включаются:

− законодательство об интеллектуальной собственности;

− законодательство о средствах массовой информации;

− законодательство о формировании информационных ресурсов предоставлении информации из них;

− законодательство о реализации права на поиск, получение и использование информации;

− законодательство о создании и применении информационных технологий и средств их обеспечения.

В отрасли права, акты которых включают информационно-правовые нормы, входят конституционное право, административное право, гражданское право, уголовное право, предпринимательское право.

Формирование законодательства в области информационного права в Российской Федерации (РФ) началось, в основном, со времени появления «Концепции правовой информатизации России», утвержденной Указом Президента РФ от 28.06.93 г. № 966. В основе информационного законодательства находится свобода информации и запретительный принцип права (все, что не запрещено законом - разрешено).

Структура информационного законодательства строится исходя из принципа «верховенства закона»: нормы вышестоящего по иерархии акта обладают более высокой юридической силой и являются

определяющими для соответствующих норм всех нижестоящих актов.

Иерархия законодательных документов РФ представлена в таблице 1.1.

Таблица 1.1 – Иерархия законодательных документов РФ

<table>
<tr><td colspan="2">Конституция РФ</td></tr>
<tr><td colspan="2">Федеральные конституционные законы РФ</td></tr>
<tr><td colspan="2">Федеральные законы РФ</td></tr>
<tr><td colspan="2">Указы и распоряжения Президента РФ</td></tr>
<tr><td colspan="2">Законодательные акты субъектов РФ</td></tr>
<tr><td>Постановления и распоряжения Правительства РФ</td><td>Нормативные правовые акты высших органов исполнительной власти субъектов РФ</td></tr>
<tr><td>Нормативные правовые акты федеральных органов исполнительной власти</td><td>Нормативные правовые акты органов исполнительной власти субъектов РФ</td></tr>
<tr><td colspan="2">Правовые акты органов местного самоуправления</td></tr>
</table>

В статье 5, ФЗ «Об информации, информационных технологиях и защите информации» от 27.7.2006 г. № 149-ФЗ, сказано: "Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)".

Общедоступная информация - информация, которую нельзя скрывать от общества. Примером служит информация о состоянии окружающей среды, о деятельности органов государственной власти и органов местного самоуправления, документы, накапливаемые в открытых фондах библиотек и архивов. Так же в эту категорию можно отнести нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, правовое положение организаций и полномочия государственных органов, органов местного самоуправления.

Информацией ограниченного доступа является информация представляющая ценность для ее владельца, доступ к которой ограничивается на законном основании. В свою очередь информация ограниченного доступа подразделяется на информацию, составляющую государственную тайну (ГТ) и информацию, соблюдение конфиденциальности которой установлено федеральным законом (конфиденциальная информация (КИ)).

В соответствии с ФЗ РФ от 21.07.1993 N 5485-1 (ред. от 29.07.2018) «О государственной тайне» **государственная тайна** — «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и

оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

Сведения, которые могут быть отнесены к **государственной тайне**, определены в Указе Президента РФ от 30 ноября 1995 г. № 1203.

К ним относятся сведения:

− в военной области;

− о внешнеполитической и внешнеэкономической деятельности;

− в области экономики, науки и техники;

− в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Нельзя засекречивать информацию в качестве государственной тайны:

− если ее утечка (разглашение и т. п.) не влечет ущерба национальной безопасности страны;

− в нарушение действующих законов;

− если сокрытие информации будет нарушать конституционные законодательные права граждан;

− для сокрытия деятельности, наносящей ущерб окружающей природной среде, угрожающей жизни и здоровью граждан.

Подробный перечень содержится в ст. 5 Закона РФ «О государственной тайне».

Перечень сведений конфиденциального характера опубликован в Указе Президента РФ от 6.03.97 г. № 188 **«Об утверждении перечня сведений конфиденциального характера».**

Коммерческая тайна - сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;

Персональные данные - сведения о фактах, событиях и обстоятельствах частой жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленном федеральными законами случаях;

Служебная тайна - служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;

Профессиональная тайна - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т. д.);

Сведения о сущности изобретения - сведения о сущности изобретения, полезной модели или промышленного образца до

официальной публикации информации о них.

Тайна следствия и судопроизводства - сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. № 119-ФЗ и другими нормативными правовыми актами Российской Федерации;

Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 02.10.2007 № 229-ФЗ «Об исполнительном судопроизводстве». (Указом Президента от 13.07.2015г. № 357 Перечень дополнен 7 пунктом)

1.3 Порядок выполнения работы

1 Определить название организации в соответствии с вариантом, указанным в таблице 1.2.

Таблица 1.2 – Варианты заданий для выполнения лабораторной работы

Вариант	Наименование ОИ	Вариант	Наименование ОИ
1	Отделение ПАО Сбербанка России	11	ГБУЗ «МИАЦ»
2	Страховая компания «Согаз»	12	Газпромэнерго
3	Научно-исследовательский институт «Волга-Урал НИПИГаз»	13	Московский центр занятости населения
4	МФЦ г. Москва	14	ОГУ
5	Департамент информационных технологий Московской области	15	Пенсионный фонд Росси по г. Москва
6	МУ МВД «Москваское»	16	Московский областной Военный комиссариат
7	Московский областной арбитражный суд	17	Казначейство РФ по Московской области
8	Следственный комитет РФ по Московской области	18	Орский завод холодильного оборудования
9	ФНС РФ г. Москва Дзержинского района	19	Медногорский медно-серный комбинат
10	ПАО «Стрела»	20	ОАО РОСТЕЛЕКОМ г. Москва

2 Разработать организационную структуру предприятия / организации / учреждения в соответствии с заданным вариантом работы. Описать направления работы организации и основные функции его подразделений. Пример организационной структуры приведен на рисунке 1.1.

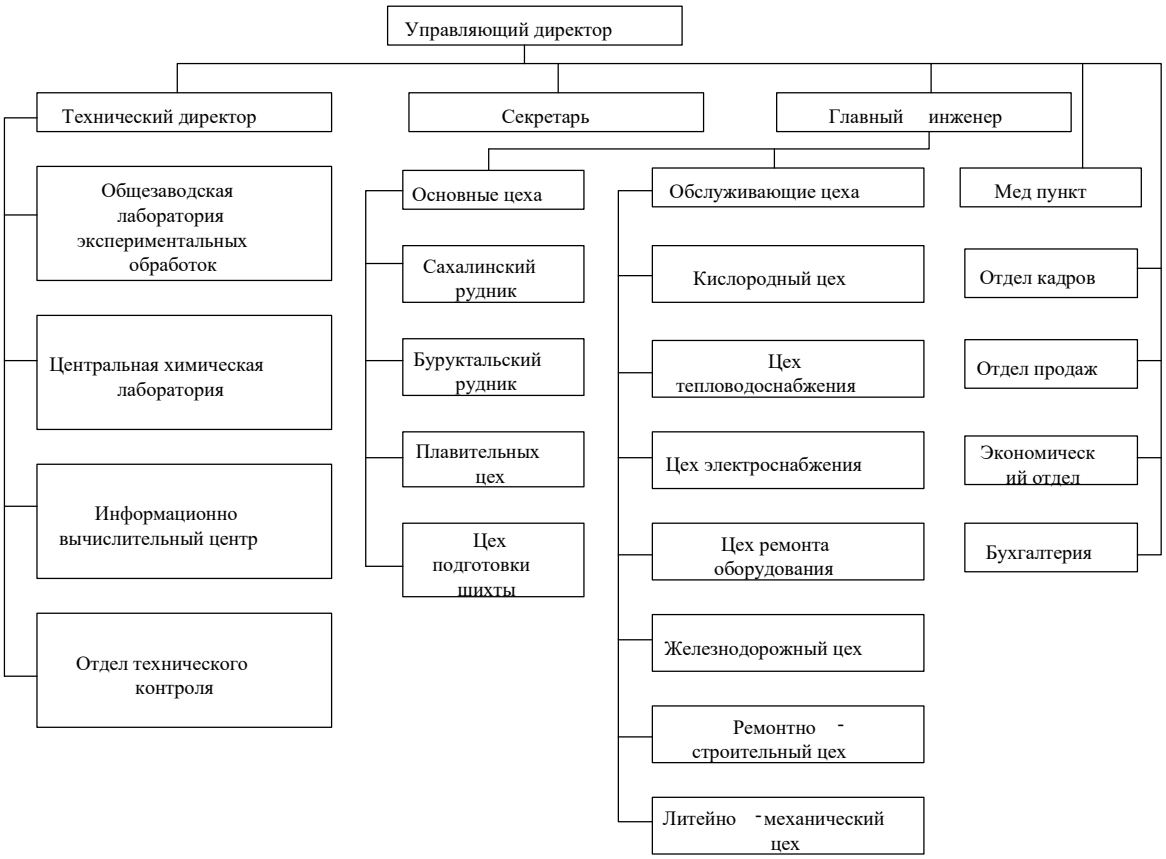


Рисунок 1.1 – Организационная структура ООО «Светлинский ферроникелевый завод»

3 Разработать схему информационных потоков предприятия / организации / учреждения. Пример схемы информационные потоков приведен на рисунке 1.2.

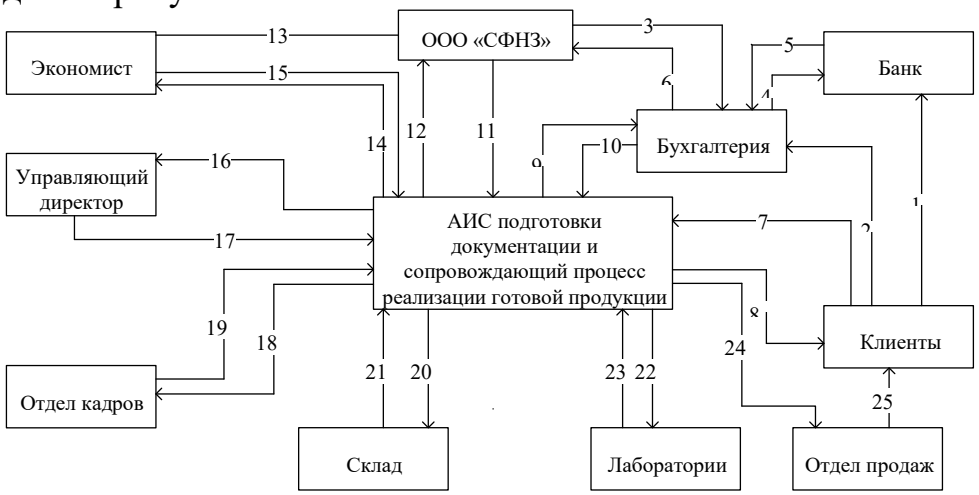


Рисунок 1.2 – Схема информационных потоков организации / предприятия

Схема информационных потоков, в обязательном порядке, сопровождается таблицей (таблица 1.3), в которой приводится их

описание и анализ.

Таблица 1.3 – Анализ информационных потоков организации/предприятия

Номер информационного потока	Наименование	Описание
1	Оплата услуг	Производится оплата услуг в Бухгалтерию ООО «СФНЗ» и в банк
2		
3	Запрос финансовой отчетности	Руководство ООО «СФНЗ» запрашивает финансовый отчет в Бухгалтерии
4	Запрос о состоянии счета	Бухгалтерия запрашивает отчет о состоянии счета
…	…	…
25	Продажа	Передача готовой продукции клиентам

4 Провести анализ защищаемых информационных ресурсов предприятия / организации / учреждения.

5 Опираясь на правовую базу в области защиты информации, обосновать право организации/предприятия на защиту информации ограниченного доступа.

2 Лабораторная работа №2. Правовые нормы защиты информации в автоматизированных системах

2.1 Цель работы

Освоить порядок классификации автоматизированных систем в защищенном исполнении и методы правовой защиты информации ограниченного доступа, обрабатываемой в них.

2.2 Теоретическая часть

Согласно ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на АС. АС. Термины и определения», под АС понимается система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. В зависимости от вида деятельности выделяют следующие виды АС:

− автоматизированные системы (АС);

− государственные автоматизированные системы (ГАС);

− автоматизированные системы управления (АСУ);

− автоматизированные системы управления технологическим процессом; − системы автоматизированного проектирования (САПР) и др.

При обработке или хранении в АС информации, не отнесенной к

категории секретной, в рамках системы защиты информации (СЗИ) от несанкционированного доступа (НСД) государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие ***организационные мероприятия***:

− выявление конфиденциальной информации и ее документально оформление в виде перечня сведений, подлежащих защите;

− определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

− установление и оформление правил разграничения доступа, т. совокупности правил, регламентирующих права доступа субъектов к объектам;

− ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной

информации;

− получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

− обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

− выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

− организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ от НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

− разработка СЗИ от НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

− осуществление приемки СЗИ от НСД в составе АС.

Согласно РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие ***конфиденциальную информацию***.

В целях разработки и применения обоснованных мер по

достижению требуемого уровня защиты информации АС делят на соответствующие классы по условиям их функционирования.

Дифференциация подхода к выбору методов и средств защиты определяется:

− важностью обрабатываемой информации,

− различием АС по своему составу, структуре, способам обработки информации,

− различием по количественному и качественному составу пользователей и обслуживающего персонала.

Основными этапами классификации АС являются:

− разработка и анализ исходных данных;

− выявление основных признаков АС, необходимых для классификации;

− сравнение выявленных признаков АС с классифицируемыми;

− присвоение АС соответствующего класса защиты информации от НСД.

Необходимыми исходными данными для проведения классификации конкретной АС являются:

− перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;

− перечень лиц, имеющих доступ к штатным средствам, АС, с указанием их уровня полномочий;

− матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС; − режим обработки данных в АС.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

− наличие в АС информации различного уровня конфиденциальности;

− уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

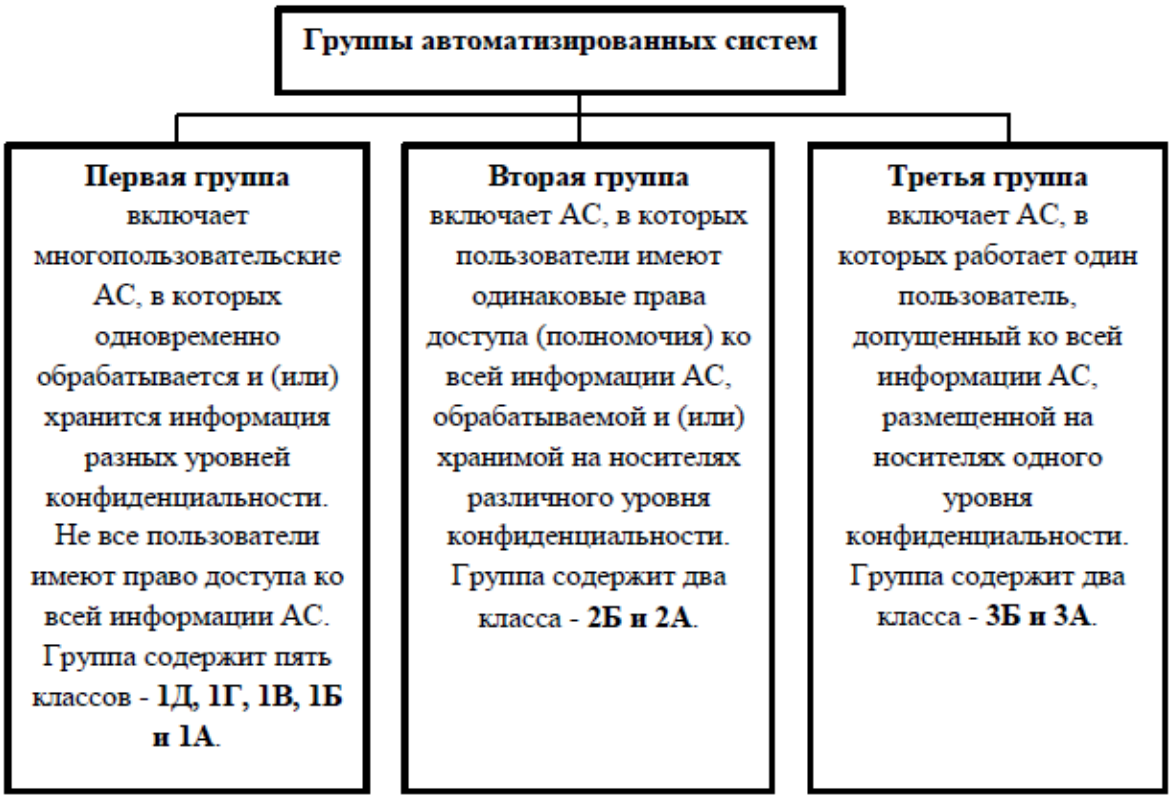
− режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. Деление АС по группам представлено на рисунке XX.



В соответствии с РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального/секретного характера:

− АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;

− АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д;

− АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам 3Б, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования);

− АС, обрабатывающие информацию, составляющую государственную тайну, в зависимости от режим обработки данных к классам 3А, 2А, 1В, 1Б, 1А.



Рисунок 2.2 – Классификация автоматизированных систем

Наибольшие требования по защиты информации, обрабатываемой в АС, предъявляются к АС класса 1А, наименьшие – к 3Б.

Наибольшие требования по защиты информации, обрабатываемой в АС, предъявляются к АС класса 1А, наименьшие – к 3Б.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации в АС от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), которая состоит из следующих четырех подсистем:

− управления доступом;
− регистрации и учета;
− криптографической;
− обеспечения целостности.

2.3 Задание на лабораторную работу

1 Разработать структурную схему АС для предприятия / организации / учреждения из лабораторной работы №1. Пример структурной схемы АС приведен на рисунке 2.3

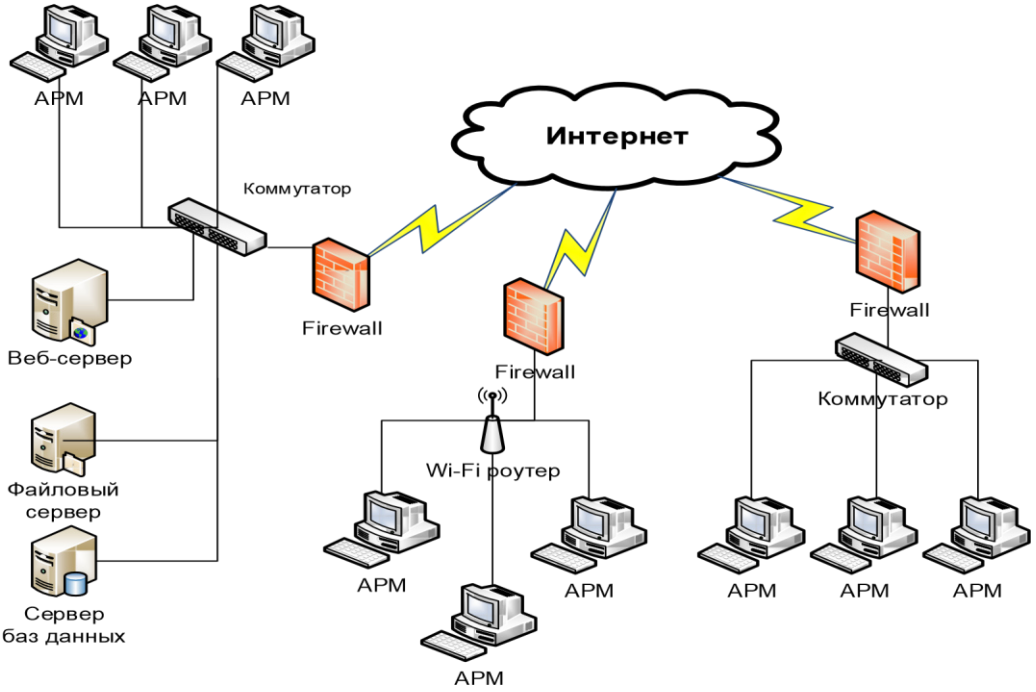


Рисунок 2.3 – Структурная схема АС предприятия / организации / учреждения

2 Проанализировать (составить таблицу) аппаратное обеспечение АС предприятия / организации / учреждения.

3 Проанализировать (составить таблицу) программное обеспечение предприятия / организации / учреждения.

4 Провести классификацию АС предприятия / организации / учреждения.

5 Определить недостатки АС предприятия / организации / учреждения, на основе требований предъявляемых в РД «Автоматизированные системы защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

3 Лабораторная работа №3. Лицензирование деятельности в области защиты информации

3.1 Цель работы

Освоить порядок получения лицензии в области защиты информации.

3.2 Теоретическая часть

Деятельность в области защиты информации ограниченного доступа подлежит обязательному лицензированию. Согласно закону от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», отдельным организациям требуется иметь лицензию ФСТЭК России на оказание услуг в области защиты конфиденциальной информации.

Лицензированием в области защиты информации называется деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации. Государственная

политика в области лицензирования отдельных видов деятельности и обеспечения защиты жизненно важных интересов личности, общества и государства определяется Постановление Правительства РФ от 21.11.2011 N 957 (ред. от 18.01.2018) «Об организации лицензирования отдельных видов деятельности»

Лицензией называется разрешение на право проведения работ в области защиты информации. Лицензия выдается на конкретные виды деятельности на три года, по истечении которых осуществляется ее перерегистрация в порядке, установленном для выдачи лицензии.

Лицензия выдается в том случае, если предприятие, подавшее заявку на получение лицензии, имеет условия для проведения лицензирования: производственную и испытательную базу, нормативную и методическую документацию, располагает научным и инженерно-техническим персоналом.

В ст.12 ФЗ перечислены виды деятельности, на которые требуется *лицензия*. В контексте информационной безопасности *лицензия* требуется на следующие виды деятельности:

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

2) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

3) деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

4) разработка и производство средств защиты конфиденциальной информации;

5) деятельность по технической защите конфиденциальной информации;

6) осуществление работ, связанных с использованием сведений, составляющих государственную тайну (только для юридических лиц);

7) деятельность, связанная с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну (только для юридических лиц);

8) осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (только для юридических лиц).

В таблице 3.1. показано, в какой лицензирующий орган, в зависимости от осуществляемого вида деятельности, необходимо подавать документы.

Таблица 3.1 – Лицензирующие органы в области защиты информации

Вид деятельности	Лицензирующие органы	
	ФСБ	ФСТЭК
1	+	
2	+	
3	+	
4	+	+
5		+
6	+	
7	+	
8	+	

В рамках рассматриваемых видов деятельности были выпущены отдельные постановления Правительства Российской Федерации, разъясняющие порядок лицензирования. Среди них:

− Постановление Правительства РФ от 21.11.2011 N 957 (ред. от 18.01.2018) «Об организации лицензирования отдельных видов деятельности»

− Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации»;

− Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 15.06.2016) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;

− Постановление Правительства РФ от 15.04.1995 № 333 (ред. от 23.08.2018 N 984) «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;

− Постановление Правительства РФ от 16.04.2012 № 313 «О лицензировании деятельности по разработке, производству,

распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»

Для получения лицензии соискатель должен направить в лицензирующий орган заполненное заявление, в котором указываются:

– для юридического лица: полное и сокращенное наименование и организационно-правовая форма, адреса, где планируется ведение лицензируемого вида деятельности, государственный регистрационный номер записи о создании юридического лица и данные документа, подтверждающего внесение в реестр юридических лиц РФ, номера телефонов и адрес электронной почты юр. лица.

– для индивидуального предпринимателя: полное ФИО, место жительства, адреса мест, где планируется ведение лицензируемой деятельности, данные документа, удостоверяющего личность (например, паспорта), государственный регистрационный номер записи о регистрации и данные документа, подтверждающего факт внесения сведений об индивидуальном предпринимателе в единый государственный реестр индивидуальных предпринимателей.

– ИНН и данные документа, подтверждающего постановку соискателя на учет в налоговом органе;

– лицензируемый вид деятельности;

– доказательства уплаты государственной пошлины за получение лицензии;

– реквизиты документов, перечень которых определяется положением о лицензировании конкретного вида деятельности и которые свидетельствуют о соответствии соискателя лицензии лицензионным требованиям.

К заявлению соискатель должен приложить копии документов в соответствии с положением о лицензировании конкретного вида деятельности и опись прилагаемых документов. Следует отметить, что в последних редакциях закона предусмотрена электронная *отправка* документов в лицензирующий орган с электронной подписью соискателя. В течение трех рабочих дней лицензирующий орган принимает решение о соответствии предоставленных документов. В случае принятия документов на рассмотрение в срок не позднее 45

рабочих дней принимается решение об отказе или предоставлении лицензии соискателю. Решение о предоставлении лицензии или об отказе в ее предоставлении оформляется приказом (распоряжением) лицензирующего органа.

Уведомление о принятии решения вручается или отправляется соискателю в письменной форме. Если решение отрицательное, должны указываться причины отказа и реквизиты акта проверки возможности выполнения соискателем лицензии лицензионных требований и условий, если причиной отказа является невозможность выполнения соискателем лицензии указанных требований и условий.

К соискателю лицензии предъявляются следующие требования:

– в штате **по основному месту работы** в соответствии со штатным расписанием руководителя и(или) уполномоченного руководить работами лица, имеющих высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности **не менее 3 лет**, или высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности **не менее 5 лет**, или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);

– не менее двух инженерно-технических работников имеющих высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности **не менее 3 лет** или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);

– наличие помещений, принадлежащих на праве собственности или ином законном основании, в которых созданы необходимые условия для осуществления лицензируемого вида деятельности;

– наличие необходимого оборудования, принадлежащего на праве собственности или ином законном основании, в соответствии с перечнем, определяемым ФСТЭК;

– использование принадлежащих лицензиату на праве собственности или ином законном основании автоматизированных систем, предназначенных для обработки конфиденциальной информации, а также средств защиты такой информации, прошедших

процедуру оценки соответствия, аттестованных и (или) сертифицированных по требованиям безопасности информации, в соответствии с законодательством Российской Федерации;

– наличие технической и технологической документации, национальных стандартов и методических документов в соответствии с определенным ФСТЭК перечнем.

Следует отметить, что если трактовать ФЗ «О лицензировании отдельных видов деятельности» буквально, то *лицензия* нужна всем организациям, которые пытаются защитить свою информацию. *По* этому поводу в 2012 г. было много дискуссий и вопросов к регулятору. Результатом стало *информационное сообщение* ФСТЭК от 30 мая 2012 г. N 240/22/2222:

«…получение юридическим лицом лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации является обязательным в случае, если эта деятельность направлена на получение прибыли от выполнения работ или оказания услуг по технической защите конфиденциальной информации и (или) она необходима для достижения целей деятельности, предусмотренных в учредительных документах юридического лица, а также, если это юридическое лицо (уполномоченное лицо) обеспечивает техническую защиту конфиденциальной информации при ее обработке в соответствии с Федеральным законом "Об информации, информационных технологиях и о защите информации" по поручению обладателя информации конфиденциального характера и (или) заказчика информационной системы».

3.3 Порядок выполнения работы

Выбрать абстрактную организацию и определить для нее вид деятельности в области информационной безопасности.

1 Разработать пакет документов для получения лицензии по выбранному, виду деятельности, который содержит:

− заявление в лицензирующий орган;

− таблицу, содержащую список сотрудников, их квалификацию, контактные данные;

− правоустанавливающие документы на помещения, предназначенные для осуществления лицензируемого вида деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним (в случае, если такие права зарегистрированы в указанном реестре, - сведения об этих помещениях);

− технические паспорта и аттестаты соответствия защищаемых помещений требованиям безопасности информации;

− технические паспорта автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации (с приложениями), актов классификации автоматизированных систем по требованиям безопасности информации,

планов размещения основных и вспомогательных технических средств и систем, аттестатов соответствия автоматизированных систем требованиям безопасности информации или сертификатов соответствия автоматизированных систем требованиям безопасности информации, а также перечень защищаемых в автоматизированных системах ресурсов, описание технологического процесса обработки информации в автоматизированных системах;

− документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;

− документы, содержащие сведения о наличии контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и маркировании контрольно-измерительного оборудования, а также документов, подтверждающих права соискателя лицензии на использование указанного оборудования, средств защиты информации и средств контроля защищенности информации;

− документы, содержащие сведения об имеющихся технической и технологической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, с приложением копий документов, подтверждающих, что документы, содержащие информацию ограниченного доступа, получены в установленном законодательством Российской

Федерации порядке;

− если лицензируемый вид деятельности – «услуги по мониторингу информационной безопасности средств и систем информатизации» - копии документов, подтверждающих наличие необходимой системы производственного контроля в соответствии с установленными стандартами.

4 Лабораторная работа №4. Создание организационной подсистемы информационной безопасности предприятия

4.1 Цель работы

Освоить методику оформления организационно-распорядительных документов, регламентирующих работу по защите информации в организации.

4.2 Теоретическая часть

Организационная защита информации является основой и важнейшим элементом в общей системе защиты информации предприятия, с высокой эффективностью обеспечивающим ее защиту при условии соблюдения должностными лицами предприятия норм и

правил защиты информации, определенных в соответствующих нормативно-методических документах.

Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и программно-аппаратные) реализовать на практике спланированные руководством предприятия меры по защите информации.

Цель принимаемых руководством предприятия и должностными лицами организационных мер — исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите.

Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

Используются два примерно равнозначных определения организационной зашиты информации.

Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

К основным организационным мероприятиям относят:

1 Организацию режима и охраны. Их цель - исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей.

2 Организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил ЗИ.

3 Организацию работы с документами и документированной

информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение.

4 Организацию использования ТС средств сбора, обработки, накопления и хранения конфиденциальной информации.

5 Организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты.

6 Организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Комплексная система защиты информации любой организации строится на базе организационно-распорядительных документов, которые в свою очередь являются элементом подсистемы организационной защиты информации.

Типовая структура организационно-нормативной документации включает в себя следующие документы:

− «Политика безопасности предприятия», предназначен для определения целей и принципов информационной безопасности. Он так же фиксирует перечень объектов информационной безопасности предприятия, а также список необходимых для ее обеспечения внутренних документов. Обычно оформляется в виде положения. Составляется подразделением, отвечающим за безопасность предприятия. Утверждается руководителем предприятия. Актуализируется не реже 1 раза в год или при изменении состава информационных средств.

− «Распределение ответственности за обеспечение безопасности», предназначен для определения ресурсов информационной безопасности и ответственности за доступ к ним. Оформляется в виде распоряжения. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после изменения политики безопасности или после изменения технологических участков и состава информационных ресурсов.

− «Процесс внедрения новой информационной системы», предназначен для описания процесса внедрения новой информационной системы в действующий бизнес-процесс. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после изменения политики безопасности предприятия.

− «Инвентаризация ресурсов», предназначен для определения категорий ресурсов, подлежащих инвентаризации. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется не реже 1 раза в год, перед проведением инвентаризации.

− «Классификация ресурсов», предназначен для классификации

ресурсов с точки зрения безопасности. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется не реже 1 раза в год.

− «Безопасность при выборе персонала и работе с ним», предназначен для определения мер по обеспечению безопасности при выборе персонала и работе с ним. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется по необходимости.

− Заключение соглашений о соблюдении режима информационной безопасности со всеми сотрудниками.

− «Реагирование на инциденты в области безопасности, а также на сбои и неисправности», предназначен для определения порядка реагирования на инциденты в области безопасности, на сбои и неисправности информационных систем. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется после возникновения инцидентов, сбоев, неисправностей, а также по необходимости.

− «Должностные инструкции по информационной безопасности», предназначен для установки прав и обязанностей, касающихся информационной безопасности, которые должны быть включены в должностные инструкции сотрудников. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия.

Актуализируется по необходимости.

− «Процедуры реагирования в случае инцидентов», предназначен для определения порядка реагирования персонала предприятия на возникающие в процессе работы инциденты. Оформляется в виде инструкции. Составляется подразделением безопасности предприятия. Утверждается руководителем предприятия. Актуализируется по необходимости.

− «Защита от вредоносного ПО (вирусов, троянских коней)», предназначен для определения правил и способов защиты информационных средств от вредоносного ПО. Оформляется в виде инструкции. Составляется подразделением безопасности и подразделением информатизации предприятия. Утверждается руководителем предприятия. Актуализируется при изменении состава информационных ресурсов.

− «Безопасность носителей данных», предназначен для определения правил работы с носителями информации. Оформляется в виде инструкции. Составляется подразделением безопасности. Утверждается руководителем предприятия. Актуализируется по необходимости.

Методические документы, на базе которых проводится разработка пакета организационно-нормативной документации:

– Российское законодательство;

– стандарты в области информационной безопасности РФ и рекомендации регулирующих органов;

– отраслевые стандарты;

– система технических регламентов;

– нормативные документы национальной системы стандартизации;

– ГОСТы по стандартизации;

– требования ФСБ России, ФСТЭК России, МВД и Минобороны;

– международные стандарты (такие как ISO 27001, ISO 27002 и др.).

4.3 Порядок выполнения работы

Для организации из лабораторной работы №1 разработать пакет организационно-распорядительных документов:

− Положение «Политика безопасности предприятия»;

− Распоряжение о распределении ответственности за обеспечени безопасности;

− Инструкцию по внедрении новой информационной системы;

− Инструкцию по инвентаризации ресурсов;

− Заключение соглашения о соблюдении режима информационно безопасности со всеми сотрудниками;

− Инструкция о порядке реагирования на инциденты в област информационной безопасности, а также на сбои и неисправности;

− Инструкцию по защите от вредоносного ПО (вирусов, троянских коней); − Инструкцию о безопасности носителей данных.

Состав организационно-распорядительных документов приводится в приложении.

<u>Темы рефератов</u>

1. Структура информационной сферы, характеристика ее элементов.
2. Информация как объект правоотношений, категории информации.
3. Система правовой защиты информации.
4. Понятие и виды защищаемой информации.
5. Особенности государственной тайны как защищаемой информации.
6. Система защиты государственной тайны.
7. Засекречивание информации, отнесенной к государственной тайне.
8. Защита сведений, отнесенных к государственной тайне.
9. Понятие информации конфиденциального характера.
10. Основные виды конфиденциальной информации, в соответствии с требованиями российской нормативно-правовой базы.
11. Правовой режим конфиденциальной информации.
12. Основные требования, предъявляемые к организации защиты

конфиденциальной информации.

13. Понятие и характеристика служебной тайны.

22

14. Нормативно - правовые основы защиты служебной тайны.

15. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения.

16. Правовые основы защиты коммерческой тайны.

17. Виды информации, составляющей коммерческую тайну.

18. Права и обязанности обладателя коммерческой тайны.

19. Основные угрозы коммерческой тайны.

20. Правовая защита коммерческой тайны.

21. Правовые основы защиты банковской тайны.

22. Раскрытие информации, относящейся к банковской тайне.

23. Нарушение банковской тайны и ответственность за подобные нарушения.

24. Нотариальная тайна и ее особенности. Тайна завещания.

25. Врачебная тайна и ее особенности.

26. Адвокатская тайна и ее особенности.

27. Тайна страхования и ее особенности.

28. Тайна связи и ее особенности. Тайна переписки, почтовых, телеграфных и иных сообщений.

29. Тайна усыновления (удочерения). Тайна исповеди.

30. Формирование российского законодательства в области защиты персональных данных.

31. Основные понятия и содержание закона РФ «О персональных данных».

32. Подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.

33. Государственный надзор и контроль обработки персональных данных, ответственность

за нарушения российского законодательства в данной области.

34. Правовые основы лицензирования в области защиты информации.

35. Правовые основы сертификации в области защиты информации.

36. Особенности правонарушений в информационной сфере.

37. Преступления в сфере компьютерной информации: виды, состав.

38. Основы расследования преступлений в сфере компьютерной информации.

39. Правовая защита информационных систем.

40. Правовая защита результатов интеллектуальной деятельности.

41. Соотношение организационных мер защиты информации с мерами правового и технического характера.

42. Основные термины, связанные с организацией защиты информации.

43. Организационные меры, направленные на защиту государственной тайны.

44. Режим секретности как основной порядок деятельности в сфере защиты государственной

тайны.

45. Особенности системы организационной защиты государственной тайны.

46. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны.

47. Организация деятельности режимно-секретных органов.

48. Установление и изменение степени секретности сведений, отнесенных к государственной тайне.

49. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.

50. Порядок допуска и доступа к государственной тайне. Основные принципы допускной

работы.

51. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок

ее составления и утверждения.

52. Документальное оформление для отправки на согласование.

53. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности.

54. Организация доступа к сведениям, составляющим государственную тайну.

23

55. Понятие «охрана». Цели и задачи охраны.

56. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы,

материальные и финансовые ценности. Особенности их охраны.

57. Виды, способы и особенности охраны различных объектов.

58. Понятие о рубежах охраны. Многорубежная система охраны.

59. Факторы выбора методов и средств охраны.

60. Организация охраны объектов защиты в процессе их транспортировки.

61. Понятие «режим», цели и задачи режимных мероприятий. Виды режима.

62. Организация пропускного режима. Основные положения инструкции об организации

пропускного режима и работе бюро пропусков.

63. Виды пропускных документов.

64. Порядок организации работы бюро пропусков.

65. Контрольно-пропускные пункты, их оборудование и

организация работы.

66. Понятие «внутриобъектовый режим» и его общие требования.

67. Противопожарный режим и его обеспечение.

68. Подбор и расстановка кадров.

69. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала.

70. Основные формы обучения и методы контроля знаний.

71. Мотивация персонала к выполнению требований по защите информации.

72. Основные формы воздействия на персонал как методы мотивации: вознаграждение,

управление карьерой, профессиональная этика.

73. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.

74. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.

75. Организационные меры по защите информации при увольнении сотрудника.

76. Основные требования, предъявляемые к подготовке и проведению конфиденциальных

переговоров.

77. Основные этапы проведения конфиденциальных переговоров.

78. Подготовка помещения для проведения конфиденциальных переговоров.

79. Подготовка программы проведения конфиденциальных переговоров.

80. Порядок проведения конфиденциальных переговоров.

81. Требования режима защиты информации при приеме в организации посетителей. Порядок доступа посетителей и командированных лиц к конфиденциальной информации. Порядок пребывания посетителей на территории и в помещениях организации.

82. Требования к программе приема иностранных представителей.

83. Требования к помещениям, в которых проводится прием иностранных представителей.

84. Обеспечение защиты информации при выезде за рубеж командируемых лиц.

85. Основные виды и формы рекламы. Общие требования режима защиты информации в

процессе рекламной деятельности.

86. Основные методы защиты информации в рекламной деятельности. Понятие «публикация

в открытой печати». Общие требования режима защиты конфиденциальной информации

при опубликовании материалов в открытой печати.

87. Особенности защиты информации при опубликовании

материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.

88. Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности.

89. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.

90. Основные документы службы информационной безопасности.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Процедура оценивания	Шкала и критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0–30 баллов Задание 2: 0–30 баллов Задание 3: 0–40 баллов «Зачтено» – 90–100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50–69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Типовые задания для проведения промежуточной аттестации по дисциплине

Задания 1 типа

1. История возникновения органов защиты информации.
2. Концептуальные основы информационной безопасности.
3. Основные принципы и условия организационной защиты информации.
4. Основные подходы и требования к организации системы защиты информации.
5. Основные силы и средства, используемые для организации защиты информации.

6. Организация охраны предприятий.
7. Организация аналитической работы и контроля состояния защиты конфиденциальной информации.
8. Засекречивание и рассекречивание сведений.
9. Отнесение сведений к различным видам конфиденциальной информации.
10. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.
11. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну.
12. Отнесение сведений к государственной тайне.
13. Засекречивание сведений и их носителей.
14. Основания и порядок рассекречивания сведений и их носителей.
15. Отнесение сведений к коммерческой тайне.
16. Основные положения допуска персонала предприятия к конфиденциальной информации.
17. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска.
18. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска.
19. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну.
20. Порядок доступа к конфиденциальной информации командированных лиц.
21. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.
22. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей.
23. Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии.
24. Основные цели, подходы и принципы организации внутриобъектового режима.
25. Силы и средства, используемые при организации внутриобъектового режима.

Задания 2-го типа

1. Сформулируйте цели и задачи пропускного режима.

2. Опишите основные элементы системы организации пропускного режима, используемые силы и средства.

3. Спланируйте мероприятия по защите информации при подготовке к проведению совещания.

4. Как происходит организация допуска участников совещания к обсуждаемым вопросам.

5. Опишите процедуру подготовки места проведения совещания.

6. Опишите порядок проведения совещания и использования его материалов.

7. Опишите процедуру организации защиты информации в ходе издательской и рекламной деятельности предприятия.

8. Опишите процедуру организации подготовки материалов к открытому опубликованию.

9. Опишите процедуру организации защиты информации в ходе взаимодействия со средствами массовой информации.

10. Опишите порядок передачи различных видов конфиденциальной информации иностранным государствам.

11. Опишите процедуру организации подготовки к передаче сведений, составляющих государственную тайну, другим государствам.

12. Какие существуют ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу.

13. Опишите ответственность должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.

14. Опишите основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну.

15. Опишите алгоритм работы лицензирующего органа по лицензированию деятельности предприятий.

16. Опишите процедуру организации проведения государственной аттестации руководителей предприятий.

17. Опишите процедуру организации аналитической работы и контроля состояния защиты конфиденциальной информации.

18. Опишите процедуру организации и проведения служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.

19. Опишите механизмы уголовно-правовой защиты сведений, составляющих коммерческую, налоговую или банковскую тайну.

20. Опишите механизмы уголовно-правовой защиты в сфере компьютерной информации.

21. Опишите механизмы уголовно-правовой защиты сведений, составляющих государственную тайну.

22. Опишите механизмы административно-правовой защиты информации с ограниченным доступом.

23. Опишите механизмы гражданско-правовой защиты служебной и коммерческой тайны.

24. Опишите элементы дисциплинарной ответственности за разглашение и (или) утрату конфиденциальных сведений.

25. Какие существуют грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну.

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Стандарты в сфере информационной безопасности»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Стандарты в сфере информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе в 3 семестре.

Цели и задачи дисциплины

Цель и задачи изучения дисциплины – слушатель получает систематизированные теоретические знания в области законодательных основ обеспечения информационной безопасности и их практического применения на российских предприятиях различных форм собственности.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен обосновывать необходимость защиты информации в автоматизированной системе	**ПК-1**	ПК-1.1. Знать: основные положения отечественных и зарубежных стандартов по оценке информационной безопасности автоматизированных систем; понятие и виды защищаемой информации, требования к эффективному использованию системы мониторинга и аудита процессов обеспечения информационной безопасности. ПК-1.2. Уметь: проводить оценку соответствия объекта требованиям нормативных документов и стандартам по информационной безопасности. ПК-1.3. Владеть: навыками анализа и подготовки содержания нормативно-распорядительных и иных документов для поддержки безопасного функционирования объектов, в том числе в автоматизированных системах.	Знать основные положения отечественных и зарубежных стандартов по оценке информационной безопасности автоматизированных систем; понятие и виды защищаемой информации	Уметь проводить оценку соответствия объекта требованиям нормативных документов и стандартам по информационной безопасности.	Владеть навыками анализа и подготовки содержания нормативно-распорядительных и иных документов для поддержки безопасного функционирования объектов, в том числе в автоматизированных системах.	Контактная работа: Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Обзор международных стандартов в сфере информационной безопасности.	4					8				18	Лабораторный практикум/20
Тема 2. Обзор стандартов РФ в сфере информационной безопасности	4		8			8				18	Тест/20 Лабораторный практикум/20
Тема 3. Стандартизация в области информационной безопасности	4		8			8				16	Тест/20 Лабораторный практикум/20
Всего:	**16**		**16**			**24**				**52**	**100**
Контроль, час	**0**										**Зачет**
Объем дисциплины (в академических часах)	**108**										
Объем дисциплины (в зачетных единицах)	**3**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Обзор международных стандартов в сфере информационной безопасности.

Рассматриваемые вопросы: Техническое регулирование; Требования технических регламентов; Стандартизация и ее принципы: системность, повторяемость, вариантность, взаимозаменяемость; Международный и национальный стандарты; Унификация, агрегатирование, симплификация, типизация; Нормативные документы по стандартизации; Виды национальных стандартов; Сертификация и ее основные этапы; Добровольная и обязательная сертификация; Функции органа по сертификации; Схемы декларирования соответствия; Обязанности органа по сертификации.; Система сертификации систем качества и производств (регистр систем качества).

Тема 2 Обзор стандартов РФ в сфере информационной безопасности

Федеральное агентство по техническому регулированию и его функции; Органы и службы стандартизации РФ; Центры стандартизации и метрологии (ЦСМ) и их функции; Виды и категории национальных стандартов РФ; Общероссийские классификаторы технико-экономической информации (ОКТЭИ); Комплексная и опережающая стандартизации; Межотраслевые системы стандартов; Параметрическая стандартизация.

Тема 3 Стандартизация в области информационной безопасности

Рассматриваемые вопросы: Проблема стандартизации в области информационной безопасности в международных и национальных стандартах; ГОСТы серии 27000; Стандартизация терминологии в ISO/IEC 27000; Стандартизация базовых требований в ISO/IEC 27001/27002; Стандартизация порядка внедрения СМИБ в ISO/IEC 27003.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения данной дисциплины используются такие виды учебной работы, как лекция, лабораторный практикум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к экзамену.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции, обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические указания для обучающихся по выполнению лабораторных практикумов

Лабораторные практикумы выполняются в соответствии с рабочим учебным планом при последовательном изучении тем дисциплины.

Порядок проведения практикума.

1. Получение задания и рекомендаций к выполнению практикума.
2. Настройка инструментальных средств, необходимых для выполнения практикума.
3. Выполнение заданий практикума.
4. Подготовка отчета в соответствии с требованиями.
5. Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций,

рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии.

Требования к оформлению результатов практикумов (отчет)

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14, выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине определяется учебным планом.

При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя.

Работа с литературой (конспектирование)

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине «Специальная математика и основы статистики» определяется учебным планом.

При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.

Реферат

Подготовка рефератов направлена на развитие и закрепление у обучающихся навыков самостоятельного глубокого, творческого и всестороннего анализа научной, методической и другой литературы по актуальным проблемам дисциплины; на выработку навыков и умений грамотно и убедительно излагать материал, четко формулировать теоретические обобщения, выводы и практические рекомендации.

Рефераты должны отвечать высоким квалификационным требованиям в отношении научности содержания и оформления.

Темы рефератов, как правило, посвящены рассмотрению одной проблемы. Объем реферата может быть от 12 до 15 страниц машинописного текста, отпечатанного через 1,5 интервала, а на компьютере через 1 интервал (список литературы и приложения в объем не входят).

Текстовая часть работы состоит из введения, основной части и заключения.

Во введении обучающийся кратко обосновывает актуальность избранной темы реферата, раскрывает конкретные цели и задачи, которые он собирается решить в ходе своего небольшого исследования.

В основной части подробно раскрывается содержание вопроса (вопросов) темы.

В заключении кратко должны быть сформулированы полученные результаты исследования и даны выводы. Кроме того, заключение может включать предложения автора, в том числе и по дальнейшему изучению заинтересовавшей его проблемы.

В список литературы (источников и литературы) обучающийся включает только те документы, которые он использовал при написании реферата.

В приложении (приложения) к реферату могут выноситься таблицы, графики, схемы и другие вспомогательные материалы, на которые имеются ссылки в тексте реферата.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Овчинникова, Е. А. Организационно-правовые основы информационной безопасности. Ч.1 : учебное пособие / Е. А. Овчинникова, Г. В. Попков ; под редакцией С. Н. Новикова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2022. — 193 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/138773/details

2. Овчинникова, Е. А. Организационно-правовые основы информационной безопасности. Ч.2 : учебное пособие / Е. А. Овчинникова, Г. В. Попков ; под редакцией С. Н. Новикова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2022. — 168 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/138774/details

Дополнительная литература

1. Алексеева, М. В. Информационное право : учебное пособие / М. В. Алексеева, С. В. Рыбак, М. Б. Смоленский. — Ростов-на-Дону : Донской государственный технический университет, 2022. — 190 с. — ISBN 978-5-7890-2005-0. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/130406/details

2. Информационное право : учебное пособие / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 197 с. — ISBN 978-5-4497-4146-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/148558/details

3. Полтавцева, М. А. Организационные и правовые аспекты информационной безопасности : учебное пособие / М. А. Полтавцева. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2023. — 145 с. — ISBN 978-5-7422-8431-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/147727/details

4. Серго, А. Г. Основы права интеллектуальной собственности для ИТ-специалистов : учебное пособие / А. Г. Серго, В. С. Пущин. — 4-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 292 с. — ISBN 978-5-4497-2422-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/133961/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№ п/п	Наименование ресурса	Ссылка

№ п/п	Наименование ресурса	Ссылка
2.	Конституционный Суд Российской Федерации	http://www.ksrf.ru
3.	Президент Российской Федерации	http://www.kremlin.ru
4.	Правительство Российской Федерации	http://government.ru
5.	Официальная Россия. Сервер органов государственной власти Российской Федерации.	http://www.gov.ru
6.	Государственная Дума Федерального Собрания Российской Федерации	http://www.duma.gov.ru
7.	Российская национальная библиотека.	http://www.nlr.ru

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информационных технологий для проведения лабораторных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; набор демонстрационного оборудования (проектор, экран).

Специальная библиотека

(библиотека литературы ограниченного доступа), предназначена для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа

Стеллажи, мебель

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Виды контактной работы, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	10–8 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, использована требуемая информация, написан корректно работающий код, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все вопросы по работе программы; 7–5 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, написан корректно работающий код, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 4–3 – работа и отчет выполнены в срок, в основном самостоятельно, использованы соответствующие формулы; имеются недочеты в коде программы; необходимые выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 2–1 – обучающийся подготовил работу и отчет несамостоятельно или не завершил в срок, выводы и ответы на вопросы отсутствуют.
4.	Тест	10 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 5 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 2 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Задания к лабораторному практикуму

Задание №1.

Сотрудник правоохранительного органа А. Иванов по роду своей служебной деятельности и должностным обязанностям был допущен к сведениям, составляющим государственную тайну, имел допуск по

второй форме.

А. Иванов утратил документ, содержащий секретные сведения. В ходе служебного расследования было установлено следующее: а) секретный документ был получен А. Ивановым под роспись; б) на персональном компьютере А. Иванова было обнаружено 10 файлов, содержащих сведения, составляющие государственную тайну; в) компьютер Иванова был подключен к Интернет через 4G модем. Однако Иванов свою вину отрицал, указывал, что доступ к компьютеру и секретному документу имели и иные сотрудники отдела.

Изучите положения Закона РФ о государственной тайне, нормы законодательства РФ, регламентирующего прохождение государственной службы в правоохранительных органах. Определите, к какому виду юридической ответственности может быть привлечен Иванов?

Допускается ли размещение носителей сведений, содержащих государственную тайну, в информационных системах?

Предложите комплекс организационно-технических и правовых мер, направленных на защиту информации, содержащей

государственную тайну на всех этапах ее обработки, хранения и передачи по каналам связи.

Задание №2.

Управление ФССП направило в адрес оператора сотовой связи запрос о предоставлении информации о регистрации абонентских номеров должников. Оператор сотовой связи отказал в предоставлении запрашиваемой информации. В отношении Оператора было возбуждено производство по делу об административном правонарушении и наложен административный штраф.

Определите перечень нормативно-правовых актов, подлежащих применению к возникшей ситуации.

К какой категории относится запрашиваемая информация?

В каком нормативно-правовом акте регламентирован порядок предоставления запрашиваемой информации? Оцените правомерность решения, принятого Оператором сотовой связи об отказе в предоставлении информации. Определите правомерность вынесенного постановления о назначении административного штрафа.

Задание № 3.

На основе анализа ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", определите комплекс мер по защите информации, сгруппируйте их по различным основаниям, приведите конкретные примеры. Разработайте систему мер по защите информации коммерческой организации от неправомерного доступа к ней и иных неправомерных действий.

Задание № 4.

Укажите основные угрозы информационной безопасности РФ в

общегосударственных информационных и телекоммуникационных системах и Основными направлениями обеспечения информационной безопасности (способы выявления каналов утечки информации на объектах защиты).

Задание № 5.

Раскройте следующие понятия в области интернет- мошенничества. **Фишинг и спуфинг**.

Задание № 6.

«О защите интеллектуальной собственности свободными лицензиями». Определить уязвимости для нарушения авторского права при распространении интеллектуальных продуктов в правовом поле свободных лицензий. Для определенности рассмотретьсемейства Common Public License, Cretive Commons Zero, Cretive Commons ttribution, GNU Generl Public License.

Задание № 7.

«О применении нейросетей для выявления террористических угроз». В США потратили миллиарды долларов на разработку искусственного интеллекта, способного заменить человеческие ресурсы (проект ELINT- electronic intelligence) в разведке путем прослушивания и анализа разговоров по телефонам и анализа контента информационных ресурсов, используемых потенциальными террористами. Когда проект ELINT был готов, президент Джимми Картер отозвал всех американских агентов с Ближнего Востока. С тех пор Соединенные Штаты не задержали ни одного крупного террориста. С помощью инверсионного анализа определите причину неудач.

Задание № 8.

«О проведении банковских транзакций». Платежи физических лиц в настоящее время все чаще производятся с помощью смартфонов через личный профиль интернет-банка. Подтверждение платежей физическим лицом происходит через одноразовые пароли, высылаемые на привязанный номер мобильного оператора смс-сообщением. Определить уязвимости данной системы, используя методы инверсионного анализа.

Задание № 9.

«Защиты персональных данных». С помощью инверсионного анализа определить уязвимости автоматизированной информационной системы (АИС) обработки персональных данных учреждения профессионального образования. Исходные данные АИС определить самостоятельно, используя сайт образовательного учреждения.

Тест

1 Соотнесите понятия и термины, закрепленные в ФЗ"О персональных данных" от N 152, с определениями:

1) автоматизированная обработка персональных данных –…

2)блокирование персональных данных -…

3) уничтожение персональных данных - …

4) обезличивание персональных данных - …

а) обработка персональных данных с помощью средств вычислительной техники;

б) временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для

уточнения персональных данных)

в) действия, в результате которых становится невозможным без использования дополнительной информации определить

принадлежность персональных данных конкретному субъекту персональных данных;

г) действия, в результате которых становится невозможным восстановить содержание персональных данных в

информационной системе персональных данных.

2 Какие из следующих информационных ресурсов относятся к общедоступной информации? Выберите все

возможные варианты ответа. а) информация о ноу-хау;

б)условия действующих контрактов;

в) документы, дающие право на осуществление предпринимательской деятельности;

г) планы, перспективы, предполагаемые шаги по развитию компании;

д) учредительные документы юридического лица;

е) о численности и оплате труда работников некоммерческих организаций.

3 Какие из следующих информационных ресурсов можно отнести к коммерческой тайне? Выберите все возможные

варианты ответа.

а) информация о ноу-хау;

б)условия действующих контрактов;

в) документы, дающие право на осуществление предпринимательской деятельности;

г) планы, перспективы, предполагаемые шаги по развитию компании;

д) учредительные документы юридического лица;

е) о численности и оплате труда работников некоммерческих организаций.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Процедура оценивания	Шкала и критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0–30 баллов Задание 2: 0–30 баллов Задание 3: 0–40 баллов «Зачтено» – 90–100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50–69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Типовые задания для проведения промежуточной аттестации по дисциплине

1. Что такое организационно-правовые методы защиты информации? Примеры.
2. Какие виды информации существуют в зависимости от категории доступа к ней?
3. Перечислите в общем виде содержание (основные разделы) Доктрина информационной безопасности РФ.
4. Опишите в общем виде структуру информационного законодательства РФ.
5. Приведите примеры сведений, не подлежащих засекречиванию.
6. Приведите примеры сведений, не подлежащих отнесению к конфиденциальным.
7. Какая организация выдает ЭЦП?
8. Какие виды ЭЦП Вы знаете?
9. По каким критериям можно отнести ИС к ГИС? Расшифруйте аббревиатуру ГИС.
10. Что такое профессиональная тайна? Примеры.
11. Приведите примеры объектов интеллектуальной собственности, защита которой предусмотрена законодательством РФ.
12. Что такое СТС (специальные технические средства) сбора и защиты информации? Примеры.
13. Что такое ноу-хау? Примеры.
14. Основной нормативно-правовым документом, защищающий права, свободы и безопасность человека в системе

информационных отношений?

15. Понятие и цель аттестации объекта информатизации?

16. Что такое политика информационной безопасности?

17. Какая информация может защищаться как тайна личной жизни?

18. В чем разница между профессиональной и служебной тайной?

19. Раскройте понятие «обезличивание ПДн». Приведите практический пример.

20. Приведите примеры должностей, для которые подразумевают получение допуска к государственной тайне

21. Что такое документированная информация (ФЗ «Об информации, информационных технологиях и о защите информации»)?

22. Что такое электронный документ (ФЗ «Об информации, информационных технологиях и о защите информации»)?

23. Для каких нужд применяются сети связи специального назначения?

24. Какие нормативно-правовые документы РФ являются базой лицензирования и сертификации в области защиты информации?

25. Как Вы понимаете термин служебная тайна?

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины
«Противодействие техническим разведкам»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Противодействие техническим разведкам» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе в 3 семестре.

Цели и задачи дисциплины

Цель и задачи изучения дисциплины – слушатель получает систематизированные теоретические знания в области законодательных основ обеспечения информационной безопасности и их практического применения на российских предприятиях различных форм собственности.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Индикаторы достижений	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**ПК-3**	ПК-3.1 Знать: основные понятия, используемые при проектировании, создании, модернизации системы защиты информации объектов информатизации, в том числе автоматизированных систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. ПК-3.2 Уметь: проводить рациональный выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; организацию защиты информации от утечки по техническим каналам на объектах информатизации. ПК-3.3 Владеть: навыками разработки требований информационной безопасности к объектам; формирования проектных решений по защите информации в автоматизированных системах.	угрозы информационной безопасности и разрабатывать подходы и методы	разрабатывать подходы и методы защиты информации, модели.	владеть навыками противодействия угрозам нарушения информационной	Контактная работа: Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Методы и средства защиты объектов и информации от технических разведок.	12		12			14				34	Лабораторный практикум/30 Тест/20
Тема 2. Демаскирующие признаки для технических разведок	12		12			14				34	Лабораторный практикум/30 Тест/20
Всего:	**24**		**24**			**28**				**68**	**100**
Контроль, час	**0**										**Зачет**
Объем дисциплины (в академических часах)	**144**										
Объем дисциплины (в зачетных единицах)	**4**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Методы и средства защиты объектов и информации от технических разведок.

Защита объектов от технической разведки. Защита объектов от оптической разведки. Защита объектов от оптикоэлектронных средств разведки. Защита радиоэлектронных средств и информации от радиотехнической разведки. Защита объектов от радиолокационных средств разведки. Мероприятия по защите лазерных систем от технических разведок. Защита от гидроакустических средств разведки. Защита от средств акустической разведки. Технический контроль эффективности принятых мер.

Тема 2 Демаскирующие признаки для технических разведок

Оптические характеристики объектов и их связь с демаскирующими признаками. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра. Демаскирующие признаки некоторых объектов в инфракрасном диапазоне электромагнитного спектра. Радиолокационные характеристики объектов разведки. Побочные электромагнитные излучения и наводки.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения данной дисциплины используются такие виды учебной работы, как лекция, лабораторный практикум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к экзамену.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в

ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции, обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические указания для обучающихся по выполнению лабораторных практикумов

Лабораторные практикумы выполняются в соответствии с рабочим учебным планом при последовательном изучении тем дисциплины.

Порядок проведения практикума.

1. Получение задания и рекомендаций к выполнению практикума.
2. Настройка инструментальных средств, необходимых для выполнения практикума.
3. Выполнение заданий практикума.
4. Подготовка отчета в соответствии с требованиями.
5. Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций, рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии.

Требования к оформлению результатов практикумов (отчет)

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14, выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого

обучающегося, ее объем по дисциплине определяется учебным планом.

При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя.

Работа с литературой (конспектирование)

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине «Специальная математика и основы статистики» определяется учебным планом.

При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.

Реферат

Подготовка рефератов направлена на развитие и закрепление у обучающихся навыков самостоятельного глубокого, творческого и всестороннего анализа научной, методической и другой литературы по актуальным проблемам дисциплины; на выработку навыков и умений грамотно и убедительно излагать материал, четко формулировать теоретические обобщения, выводы и практические рекомендации.

Рефераты должны отвечать высоким квалификационным требованиям в отношении научности содержания и оформления.

Темы рефератов, как правило, посвящены рассмотрению одной проблемы. Объем реферата может быть от 12 до 15 страниц

машинописного текста, отпечатанного через 1,5 интервала, а на компьютере через 1 интервал (список литературы и приложения в объем не входят).

Текстовая часть работы состоит из введения, основной части и заключения.

Во введении обучающийся кратко обосновывает актуальность избранной темы реферата, раскрывает конкретные цели и задачи, которые он собирается решить в ходе своего небольшого исследования.

В основной части подробно раскрывается содержание вопроса (вопросов) темы.

В заключении кратко должны быть сформулированы полученные результаты исследования и даны выводы. Кроме того, заключение может включать предложения автора, в том числе и по дальнейшему изучению заинтересовавшей его проблемы.

В список литературы (источников и литературы) обучающийся включает только те документы, которые он использовал при написании реферата.

В приложении (приложения) к реферату могут выноситься таблицы, графики, схемы и другие вспомогательные материалы, на которые имеются ссылки в тексте реферата.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Автоматизированные системы управления специального назначения : учебное пособие / В. Н. Козичев, А. А. Протасов, А. В. Ширманов, С. В. Крейдин. — Москва : Московский государственный технический университет имени Н.Э. Баумана, 2020. — 214 с. — ISBN 978-5-7038-5429-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/115300/details

Дополнительная литература

1. Федоров, А. В. Политологические основы информационной безопасности : учебное пособие / А. В. Федоров. — Москва : Московский государственный технический университет имени Н.Э. Баумана, 2020. — 124 с. — ISBN 978-5-7038-5279-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/115368/details

2. Эволюция подходов к построению модели угроз безопасности информации систем и сетей с учетом изменений законодательства Российской Федерации : учебное пособие / О. М. Голембиовская, М. Ю.

Рытов, Е. В. Кондрашова [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 252 с. — ISBN 978-5-4497-4487-6. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/152050/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№ п/п	Наименование ресурса	Ссылка
2.	Конституционный Суд Российской Федерации	http://www.ksrf.ru
3.	Президент Российской Федерации	http://www.kremlin.ru
4.	Правительство Российской Федерации	http://government.ru
5.	Официальная Россия. Сервер органов государственной власти Российской Федерации.	http://www.gov.ru
6.	Государственная Дума Федерального Собрания Российской Федерации	http://www.duma.gov.ru
7.	Российская национальная библиотека.	http://www.nlr.ru

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория информационных технологий для проведения лабораторных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; набор демонстрационного оборудования (проектор, экран).

Лаборатория Схемотехники

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; учебно-

лабораторные стенды и контрольно-измерительная аппаратура для измерения частотных свойств, форм и временных характеристик сигналов, средства для измерения параметров электрических цепей, средства генерирования сигналов, TBS1072C, Осциллограф цифровой, 2 канала х 70 МГц (Госреестр РФ)

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Лаборатория технической защиты информации

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; оснащена специализированным оборудованием по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам; системой виброакустической защиты "Гамма СВАЗ-01", ПЭВМ «Secret»

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Виды контактной работы, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	10–8 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, использована требуемая информация, написан корректно работающий код, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все вопросы по работе программы; 7–5 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, написан корректно работающий код, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы;

№ п/п	Виды контактной работы, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
		4–3 – работа и отчет выполнены в срок, в основном самостоятельно, использованы соответствующие формулы; имеются недочеты в коде программы; необходимые выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 2–1 – обучающийся подготовил работу и отчет несамостоятельно или не завершил в срок, выводы и ответы на вопросы отсутствуют.
4.	Тест	10 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 5 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 2 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Задания к лабораторному практикуму

Задача 1. Прибор СРМ-700. Провести оценку возможности утечки информации из помещения по радиоканалу

Задача 2 Прибор СРМ-700. Провести оценку возможности утечки информации из помещения по ИК-каналу

Задача 3 Прибор SP-81 Оракул. Провести оценку возможности утечки информации из помещения по ИК-каналу утечки информации

Задача 4 Прибор SP-81 Оракул. Провести оценку возможности утечки информации из помещения по НЧ-каналу утечки информации

Задача 5 Прибор Оракул. Провести анализ радиоэлектронных источников зафиксированных в памяти прибора. Дать им техническую характеристику

Задача 6 Прибор SP-81 Оракул. Произвести проверку звукоизоляции помещения

Задача 7 Прибор Катран. Определить наличие внедренной закладки в образцах материалов

Задача 8 Прибор Оракул. Провести поиск работающих радиоэлектронных устройств. Дать им техническую характеристику

Задача 9 Аппаратура АРК-Д6. Сформировать задание на оценку радиоэлектронной обстановки

Задача 10 Аппаратура АРК-Д6. Оценить радиоэлектронную

обстановку. Дать техническую характеристику источникам сигналов

Задача 11 Аппаратура АРК-Д6. Оценить радиоэлектронную обстановку. Дать характеристику спектрам обнаруженных сигналов

Задача 12 Аппаратура АРК-Д6. Провести поиск закладных устройств

Задача 13 Аппаратура АРК-Д6. Произвести поиск радиозакладки на естественном фоне

Задача 14 Аппаратура АРК-Д6. Определить характеристики тестового сигнала

Задача 15 Прибор AR-3000. Произвести установку исходных параметров и оценку радиоэлектронной обстановки в ручном режиме сигналов с am модуляцией

Задача 16 Прибор AR-3000. Произвести установку исходных параметров и оценку радиоэлектронной обстановки в ручном режиме сигналов с FM модуляцией

Задача 17 Прибор СРМ-700. Провести оценку возможности утечки информации из помещения по акустическому каналу

Задача 18 Прибор СРМ-700. Провести оценку возможности утечки информации из помещения по виброакустическому каналу

Тест

ВОПРОС №1. Стоимость защищаемых ресурсов определяется:

1.Затратами на ее создание.

2.Прибылью, которую может принести использование данного ресурса.

3.Наличием и условиями, предложенными владельцами конкурирующих ресурсов.

4.Подготовкой ИТ-специалистов.

ВОПРОС №2. Аспекты управления защитой:

1.Управление политикой защиты.

2.Управление архитектурой защиты.

3.Управление механизмами защиты.

4.Управление средствами защиты.

5.Управление персоналом.

6.Управление доступом.

7.Управление обучением.

ВОПРОС №3. Управление политикой защиты включает в себя процессы:

1.Управление персоналом.

2.Управление доступом.

3.Управление обучением.

4.Управление политикой защиты.

5.Управление архитектурой защиты.

6.Управление механизмами защиты.

ВОПРОС №4. Два фактора, определяющие уязвимость организации:

1. Последствия инцидента с безопасностью.

2. Учет политических или организационных последствий.

3. Наличие службы безопасности.

4. Наличие нормативно-методических документов по безопасности информации.

ВОПРОС №5. Каналы утечки информации и места подключений для хищения абонентского телетрафика:

1. Радиозакладка параллельного подключения.

2. Комбинированная телефонно-акустическая радиозакладка.

3. Радиозакладка последовательного включения.

4. Закладки типа «длинное ухо».

5. Низкоомный адаптер.

6. Высокоомный адаптер.

7. Бесконтактный адаптер

8. Наводки телефонного сигнала на другие цепи.

9. Акустоэлектрическое преобразование.

10. Акустооптическое преобразование.

ВОПРОС №6. Эффективность защиты информации:

1. Степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты информации.

2. Уровень соответствия достигнутых результатов действий по защите информации поставленной цели защиты информации.

3. Степень соответствия результатов действий по защите информации поставленной цели защиты информации.

4. Степень соответствия достигнутых результатов действий по защите информации.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Процедура оценивания	Шкала и критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0–30 баллов Задание 2: 0–30 баллов Задание 3: 0–40 баллов «Зачтено» – 90–100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50–69 – ответ в основном правильный, логически

Процедура оценивания	Шкала и критерии оценки, балл
	выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Типовые задания для проведения промежуточной аттестации по дисциплине

1. Что такое электронное закладное устройство
2. Основные элементы электронных закладных устройств, какие не обязательные
3. Способ реализации перехвата электромагнитного канала связи
4. Способ реализации перехвата электрического канала связи
5. Способ реализации перехвата индукционного канала связи
6. Способ реализации перехвата паразитных сигналов канала связи
7. Что такое прямые акустические каналы утечки информации
8. Принцип виброакустических каналов утечки информации
9. Как возникают лазерные каналы утечки информации
10. Как возникают акустоэлектрические каналы утечки информации
11. Как возникают акустоэлектромагнитные каналы утечки информации
12. Пассивные средства защиты по каналу ПЭМИН это
13. Активные средства защиты по каналу ПЭМИН это
14. Пассивные средства защиты по акустическому каналу утечки информации
15. Активные средства защиты по акустическому каналу утечки информации
16. Пассивные средства защиты по виброакустическому каналу утечки информации
17. Активные средства защиты по виброакустическому каналу утечки информации
18. Пассивные средства защиты по лазерному каналу утечки информации
19. Словесная разборчивость это?
20. Какие виды шумов применяются в активных средствах защиты информации
21. Основные этапы выявления закладных устройств
22. Организационные мероприятия для выявления закладных устройств
23. Какая техника применяется для выявления закладных устройств
24. Основные режимы ПЭМИН
25. Что такое ОТСС

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины
«Защита информации от утечки по техническим каналам»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ .....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Защита информации от утечки по техническим каналам» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в часть, формируемую участниками образовательных отношений, Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе в 3 семестре.

Цели и задачи дисциплины

Цель и задачи изучения дисциплины – слушатель получает систематизированные теоретические знания в области законодательных основ обеспечения информационной безопасности и их практического применения на российских предприятиях различных форм собственности.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
		выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**ПК-3**	-методы и алгоритмы проектирования распределенных информационных систем, их компоненты и протоколы взаимодействия; - методы и алгоритмы проектирования распределенных информационных систем, их компоненты и протоколы взаимодействия согласно критерия защиты информации сети.	-выбирать средства для проектирования систем, компоненты проектирования протоколы их связей; - выбирать средства для проектирования систем, компоненты проектирования протоколы защиты информации в сетях; - прогнозировать эффективность функционирования средств зашиты и механизмов защиты информации в сетях.	-навыками выбора инструментальных средств разработки и обеспечения защиты информации в сетях; - определения набора средств обеспечения безопасности сети; - пониманием принципа построения и зашиты базы; -организации процесса использования инфраструктуры; -мониторинга функционирования инфраструктуры; принятия управленческих решений, в том числе и по защите сети.	Контактная работа: Практическое занятие Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Тема 1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации	3	6				4				9	Лабораторный практикум/10 Доклад/5
Тема 2. Технические каналы утечки акустической (речевой) информации	3	6				4				9	Лабораторный практикум/10 Доклад/5
Тема 3. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	3					4				9	Лабораторный практикум/10
Тема 4. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	3	6				4				9	Лабораторный практикум/10 Доклад/5
Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам	3					3				8	Лабораторный практикум/10
Тема 6. Методы и средства контроля эффективности	3					3				8	Лабораторный практикум/10

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
защиты выделенных помещений от утечки речевой информации по техническим каналам											
Тема 7. Методы и средства выявления электронных устройств негласного получения информации	3					3				8	Лабораторный практикум/10 Доклад/5
Тема 8. Организация технической защиты информации	3	6				3				8	Лабораторный практикум/10
Всего:	**24**	**24**				**28**				**68**	**100**
Контроль, час	**0**										**Зачет**
Объем дисциплины (в академических часах)	**144**										
Объем дисциплины (в зачетных единицах)	**4**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации

Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации). Нормативные документы по технической защите информации. Термины и определения в области технической защиты информации: объект информатизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

Тема 2. Технические каналы утечки акустической (речевой) информации

Характеристики речевого сигнала. Общая характеристика и классификация технических каналов утечки акустической информации. Прямые акустические каналы утечки речевой информации. Акустовибрационные каналы утечки речевой информации. Акустооптический (оптикоэлектронный, лазерный) канал утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Акустоэлектромагнитные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики.

Тема 3. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.

Тема 4. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Классификация способов и средств защиты объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке). Защищённые средства вычислительной техники.

Тема 5. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке). Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

Тема 6. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки 6 возможностей средств акустической разведки по перехвату речевой информации. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Тема 7. Методы и средства выявления электронных устройств негласного получения информации

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и

выделенных помещений на наличие электронных устройств негласного получения информации.

Тема 8. Организация технической защиты информации

Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации. Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию. Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации. Порядок документального оформления результатов аттестационных испытаний и соответствия объекта информатизации требованиям по безопасности информации.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения данной дисциплины используются такие виды учебной работы, как лекция, лабораторный практикум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к экзамену.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции,

обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические указания для обучающихся по выполнению лабораторных практикумов

Лабораторные практикумы выполняются в соответствии с рабочим учебным планом при последовательном изучении тем дисциплины.

Порядок проведения практикума.

1. Получение задания и рекомендаций к выполнению практикума.
2. Настройка инструментальных средств, необходимых для выполнения практикума.
3. Выполнение заданий практикума.
4. Подготовка отчета в соответствии с требованиями.
5. Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций, рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии.

Требования к оформлению результатов практикумов (отчет)

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14, выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине определяется учебным планом.

При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя.

Работа с литературой (конспектирование)

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет

значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине «Специальная математика и основы статистики» определяется учебным планом.

При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Газизов, А. Р. Техническая защита информации : учебное пособие / А. Р. Газизов, Д. В. Фатхи. — Ростов-на-Дону : Донской государственный технический университет, 2022. — 108 с. — ISBN 978-5-7890-2053-1. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/130429/details

2. Мартынов, А. П. Информационная безопасность и защита информации : учебное пособие / А. П. Мартынов, И. А. Мартынова, А. А. Русаков. — 2-е изд.. — Москва : Ай Пи Ар Медиа, 2026. — 130 с. — ISBN 978-5-4497-2349-9. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/155918/details

Дополнительная литература

1. Киренберг, А. Г. Защита информации от утечки по техническим каналам : учебное пособие / А. Г. Киренберг, В. О. Коротин. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. — 221 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/135100/details

2. Солонская, О. И. Средства защиты информации : учебное пособие / О. И. Солонская. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. — 89 с. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/117115/details

3. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 4-е изд.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/146404/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№ п/п	Наименование ресурса	Ссылка
2.	Конституционный Суд Российской Федерации	http://www.ksrf.ru
3.	Президент Российской Федерации	http://www.kremlin.ru
4.	Правительство Российской Федерации	http://government.ru
5.	Официальная Россия. Сервер органов государственной власти Российской Федерации.	http://www.gov.ru
6.	Государственная Дума Федерального Собрания Российской Федерации	http://www.duma.gov.ru
7.	Российская национальная библиотека.	http://www.nlr.ru

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол

преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Лаборатория Схемотехники

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; учебно-лабораторные стенды и контрольно-измерительная аппаратура для измерения частотных свойств, форм и временных характеристик сигналов, средства для измерения параметров электрических цепей, средства генерирования сигналов, TBS1072C, Осциллограф цифровой, 2 канала х 70 МГц (Госреестр РФ)

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Лаборатория технической защиты информации

Основное оборудование:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональные компьютеры; оснащена специализированным оборудованием по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам; системой виброакустической защиты "Гамма СВАЗ-01", ПЭВМ «Secret»

Технические средства обучения:

персональный компьютер; набор демонстрационного оборудования (проектор, экран)

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Виды контактной работы, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	10–8 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, использована требуемая информация, написан корректно работающий код, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на

№ п/п	Виды контактной работы, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
		все вопросы по работе программы; 7–5 – работа и отчет выполнены в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, написан корректно работающий код, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 4–3 – работа и отчет выполнены в срок, в основном самостоятельно, использованы соответствующие формулы; имеются недочеты в коде программы; необходимые выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 2–1 – обучающийся подготовил работу и отчет несамостоятельно или не завершил в срок, выводы и ответы на вопросы отсутствуют.
4.	Доклад	5 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 4–3 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 2 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Задания к лабораторному практикуму

Задание 1

1. По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации детектора электромагнитного поля ST107 и меры безопасности при работе с ним. 2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку. 3. Обеспечить удаление из зоны действия прибора мощных помеховых объектов. 4. Провести обследование помещения лаборатории. Выявить и тщательно зафиксировать все источники ЭМС, и определить их характеристики, пользуясь всеми возможностями детектора электромагнитного поля ST107. 5. Провести обследование контрольных образцов имитаторов ЗУ и провести их идентификацию с использованием и без использования частотомера. 6. Составить отчет о проделанной работе, который должен включать: • описание индикатора, принципа его действия, характеристик

и основных приемы работы; • данные, полученные при исследовании ЭМО в лаборатории; • результаты идентификации контрольных образцов с подробным обоснованием принято решения. 7. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя.

Задание 2

1. По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации прибора ST031 «Пиранья» и меры безопасности при работе с ним. 2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку. 3. Обеспечить удаление из помещения, где проводятся занятия, мощных помеховых объектов, отключить сотовые телефоны. 4. С помощью контрольного устройства «Тест» провести проверку работоспособности прибора ST031 во всех основных режимах работу, или только в режимах указанных преподавателем. Зафиксировать характеристики тестовых сигналов, излучаемых КУ. 5. Провести обследование помещения в одном из режимов, указанном преподавателем, при обнаружении посторонних сигналов провести их идентификацию и определить характеристики. По возможности установить источник этих излучений и его примерное местоположение. 62 6. Составить отчет о проделанной работе, который должен включать: • краткое описание прибора «Пиранья», принципа его действия, характеристик и основных приемов работы; • данные, полученные при исследовании эталонных сигналов КУ «Тест»; • результаты идентификации тестовых сигналов с подробным обоснованием принято решения. 7. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя, проводящего занятие.

Задание 3

1. По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации нелинейного локатора «Катран» и меры безопасности при работе с ним. 2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку. 3. Обеспечить удаление из зоны действия локатора мощных помеховых объектов. 4. Провести обследование эталонных объектов: интегральной микросхемы, металлического предмета, МОМ структуры и элемента, содержащего одновременно полупроводник и МОМ структуру. Выявить и тщательно зафиксировать их отличительные признаки, пользуясь всеми возможностями нелинейного локатора. 5. Провести обследование контрольных образцов, скрытых в специальных коробочках и провести их идентификацию. 6. Составить отчет о проделанной работе, который должен включать: описание нелинейного локатора, принципа его

действия, характеристик и основных приемов работы; данные, полученные при исследовании эталонных образцов; результаты идентификации контрольных образцов с подробным обоснованием принятого решения. 7. Отчет составляется персонально каждым студентом, и полученные в нем результаты подлежат защите у преподавателя.

Темы для докладов

1. Современные цифровые диктофоны.
2. Типы микрофонных систем и их технические характеристики.
3. Область применения электронных стетоскопов (радиостетоскопов).
2. и их конструктивные особенности.
3. Лазерные акустические систем разведки.
4. Цифровые анализаторы спектра.
5. Векторные анализаторы сигналов.
6. Измерительные цифровые приемники.
7. Измерительные антенны, токосъемники, пробники для проведения специальных исследований средств вычислительной техники.
8. Программно-аппаратные комплексы для проведения специальных исследований СВТ на ПЭМИН.
9. Портативные шумомеры и виброметры.
10. Аудиоанализаторы и область применения.
11. Программно-аппаратные комплексы для проведения акустических и виброакустических измерений.
12. Программно-аппаратные комплексы для выявления акустоэлектромагнитных (акустопараметрических) каналов утечки информации.
13. Программно-аппаратные комплексы для оценки защищенности
14. вспомогательных технических средств и систем от акустоэлектрических преобразований.
15. Индикаторы электромагнитного поля.
16. Радиочастотомеры.
17. Сканирующие радиоприемники.
18. Специальные поисковые приемники ближней зоны и интерсепторы.
19. Программно-аппаратные комплексы радиомониторинга.
20. Анализаторы проводных линий.
21. Программно-аппаратные комплексы для исследования проводных линий.
22. Нелинейные радиолокаторы.
23. Рентгенотелевизионные комплексы.
24. Портативные металлоискатели.
25. Эндоскопы.
26. Нормативно-методические документы ФСТЭК в области

технической защиты информации.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Процедура оценивания	Шкала и критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0–30 баллов Задание 2: 0–30 баллов Задание 3: 0–40 баллов «Зачтено» – 90–100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50–69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Типовые задания для проведения промежуточной аттестации по дисциплине

1. Объект информатизации (определение). Основные технические средства и системы (ОТСС).

2. Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации

3. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).

4. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.

5. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.

6. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.

7. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации.

8. Средства акустической разведки: цифровые диктофоны, направленные микрофоны (классификация, характеристики, основные

возможности, схема канала перехвата). Дальность перехвата речевого сигнала средством акустической разведки направленными микрофонами.

9. Схемы перехвата речевой информации по акустовибрационному каналу утечки речевой информации.

10. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.

11. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.

12. Экранирующие материалы, их основные характеристики. Формула для расчета коэффициента экранирования для электрической и магнитной составляющей электромагнитного поля.

13. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).

14. Основные требования к заземлению технических средств. Схемы заземлителей. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.

15. Основные требования к системе пространственного электромагнитного зашумления. Схема установки системы пространственного зашумления на объекте информатизации.

16. Основные требования по установке системы пространственного зашумления на объекте информатизации. Основные характеристики генераторов шума.

17. Основные требования к системе электропитания технических средств.

Способы защиты цепей электропитания технических средств от утечки информации, возникающей за счет наводок побочных электромагнитных излучений.

18. Основные требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания технических средств. Основные характеристики фильтров нижних частот (ФНЧ). Схемы установки помехоподавляющих фильтров на объекте информатизации.

19. Характеристики речевого сигнала. Разборчивость речи.

20. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.

21. Средства звуко- и виброизоляции выделенных помещений.

Звукоизолирующие кабины. Специальные защищенные помещения.

22. Порядок проведения контроля эффективности защиты ВТСС. Состав и основные требования к аппаратуре контроля при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.

23. Схема измерительной установки при контроле ВТСС на подверженность акустоэлектрическим преобразованиям. Порядок проведения проверки ВТСС на подверженность акустоэлектрическим преобразованиям.

24. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН

25. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.

26. Сканирующие приемники (принцип работы, основные характеристики). Этапы выявления радиозакладок.

27. Методы обнаружения, идентификации радиозакладных устройств и определения их местоположения.

28. Порядок организации защиты информации на объектах информатизации.

29. Предварительное специальное обследование объекта информатизации.

30. Аналитическое обоснование необходимости создания СТЗИ объекта (содержание, порядок проведения).

31. Замысел создания СТЗИ. Техническое задание на разработку СТЗИ объекта информатизации.

32. Организация аттестации объекта информатизации по требованиям безопасности информации.

33. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.

34. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации.

35. Заключение по результатам аттестационной проверки объекта информатизации.

36. Аттестат соответствия объекта информатизации требованиям безопасности информации.

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Нейронные сети»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 4

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 8

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 13

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 15

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Нейронные сети» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Дисциплина «Нейронные сети» ориентирована на получение обучающимися знаний, умений и практического опыта разработки и реализации программных моделей нейрокомпьютерных систем.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в учебные планы по программам подготовки бакалавров по направлению 10.04.01 Информационная безопасность в факультативные.

Дисциплина изучается на 1 курсе в 2 семестре.

Цель и задачи дисциплины

Цель изучения дисциплины – формирование у обучающихся необходимых компетенций для успешного освоения образовательной программы, в частности знаний, умений и практического опыта разработки интеллектуальных информационных систем, использующих аппарат машинного обучения, которые позволяют решать практические задачи анализа данных в исследованиях и бизнес-приложениях.

Задачи изучения дисциплины:

- формирование знаний о современном состоянии исследований в области машинного обучения, принципов построения систем машинного обучения, моделях представления и описания технологий машинного обучения;
- формирование умений проводить анализ предметной области, определять назначение, выбирать методы и средства для построения систем машинного обучения, строить системы машинного обучения;
- развитие практического опыта использования аппарата простейшего анализа данных, применения методов классификации информации, реализации алгоритмов машинного обучения;
- формирование уровня знаний, умений, навыков, опыта деятельности в рамках программы подготовки кадров к Цифровой Экономике, построенных на основе Программы «Цифровая экономика России»;
- формирование умения создавать инфраструктуру практически всех видов телекоммуникационных сетей, в соответствии со знаниями, пониманием требований стандартов отрасли и конкретными навыками, которые лежат в основе лучшей практики в области профессионального исполнения, в соответствии с компетенциями блока Информационные и коммуникационные технологии формата WORLDSKILLS.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	**Код компетенции**	**Код и наименование индикатора достижения компетенций**	**Перечень планируемых результатов обучения по дисциплине**			**Формы образовательной деятельности**
			выпускник должен знать	**выпускник должен уметь**	**выпускник должен иметь практический опыт**	
Способен проводить анализ безопасности компьютерных систем	**ПК-4**	ПК-4.1 Знать: источники и классификацию угроз информационной безопасности; методы анализа и тестирования компьютерных систем; требования к разработке автоматизированных систем в защищенном исполнении.	архитектуру классических нейросетевых моделей; алгоритмы обучения нейронных сетей; способы применения нейронных сетей для решения различных прикладных задач	организовывать работу в построении нейронной сети	конструировать нейронные сети применять нейронные сети для решения прикладных задач	Контактная работа: Лекции Лабораторные работы Самостоятельная работа
		ПК-4.2 Уметь: разрабатывать модели нарушителя и угроз для компьютерных систем, выделять подсистемы и модули, содержащие критическую информацию.	методы обучения нейронных сетей	выбирать методы обучения нейронной сети в зависимости от поставленной задачи	обучать нейронные сети	
		ПК-4.3 Владеть: методами и средствами для проверки выполнения требований информационной безопасности компьютерных систем.	возможности и особенности построения нейрокомпьютерных алгоритмов, современных технологий разработки и адаптации прикладного программного обеспечения.	адаптировать отдельные компоненты прикладного программного обеспечения.	разработки прикладного программного обеспечения на современных языках программирования, программирование методами адаптации прикладного программного обеспечения в области нейрокомпьютерных систем.	

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Тема 1. Введение в машинное обучение	3					4				2	Отчет по лабораторному практикуму/10 Реферат/20
Тема 2. Статистические оценки и проверка гипотез										2	
Тема 3. Машинное обучение как математическое моделирование										2	Отчет по лабораторному практикуму/10
Тема 4. Введение в линейные модели и задача регрессии										2	Отчет по лабораторному практикуму/10
Тема 5. Линейные модели и задача классификации	3									2	
Тема 6. Выбор и оценка моделей, работа с признаками						4				2	Отчет по лабораторному практикуму/10
Тема 7. Деревья и ансамбли										2	Отчет по лабораторному практикуму/10
Тема 8. Бустинг										2	
Тема 9. Признаковые представления для дискретных входных данных										1	Отчет по лабораторному практикуму/10
Тема 10. Современные нейросетевые архитектуры										1	Отчет по лабораторному практикуму/10
Тема 11. Кластеризация										1	Отчет по лабораторному практикуму/10
Тема 12. Снижение размерности	2									1	
Всего:	**8**					**8**				**20**	**100**
Контроль, час	**0**										**Зачет**
Объем дисциплины (в академических	**36**										

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
часах)											
Объем дисциплины (в зачетных единицах)	1										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Введение в машинное обучение

Постановки основных классов задач в машинном обучении. Обучение с учителем: регрессия и классификация. Обучение без учителя: кластеризация, снижение размерности. Semi-supervised learning, рекомендательные системы, обработка текстов: тематическое моделирование, построение аннотаций, извлечение ответов на вопросы, машинный перевод. Обработка изображений: порождение, преобразование. Обучение представлений; обучение с подкреплением. Примеры задач. Виды данных: структурированные таблицы, тексты, изображения, звук, логи. Признаки.

Тема 2. Статистические оценки и проверка гипотез

Основные понятия математической статистики: статистические оценки (точечные и интервальные), их свойства, проверка гипотез.

Тема 3. Машинное обучение как математическое моделирование

Статистические модели. Теоретико-вероятностная постановка задачи обучения с учителем. Минимизация ожидаемой ошибки. No free lunch theorem. Пример: задача регрессии, минимизация квадрата отклонения. Регрессионная функция: условное матожидание. Линейная регрессия и метод k ближайших соседей. Переобучение и недообучение. Разложение ошибки на шум, смещение и разброс. Проклятие размерности. Методы оценивания обобщающей способности, кросс-валидация.

Тема 4. Введение в линейные модели и задача регрессии

Градиентный спуск, методы оценивания градиента. Функции потерь. Метрики качества регрессии. Линейная регрессия, метод наименьших квадратов и максимизация правдоподобия. Теорема Гаусса—Маркова. Явный вид решения в методе наименьших квадратов. Ковариационная матрица для коэффициентов. Практические соображения: что делать с категориальными данными? Вычислительные соображения: точное решение или градиентный спуск. Регуляризация.

Тема 5. Линейные модели и задача классификации

Задачи классификации. Общая постановка. 0-1 ошибка. Байесовский классификатор. Линейные методы для классификации. Логистическая регрессия, максимизация правдоподобия, кросс-энтропия.

Тема 6. Выбор и оценка моделей, работа с признаками

Тонкости кросс-валидации. Оценки ожидаемой ошибки для линейной регрессии: AIC и другие. L1 и L2 регуляризация. Метод главных компонент и singular spectrum analysis. Методы отбора признаков. Ядровые методы. Ядра и спрямляющие пространства, методы их построения.

Операции в спрямляющих пространствах.

Тема 7. Деревья и ансамбли

Ограничения линейных методов (пример: XOR). Решающие деревья. CART. Ансамбли. Бутстреп. Бэггинг. Случайный лес.

Тема 8. Бустинг

AdaBoost, градиентный бустинг. XGBoost.

Тема 9. Признаковые представления для дискретных входных данных

Практические соображения. Кодирование категориальных данных. Пропущенные значения. Обработка текстов: bag of words, tf-idf, векторные эмбеддинги.

Тема 10. Современные нейросетевые архитектуры

Нейронные сети в обработке изображений. Фильтры. Сверточные слои. Нейронные сети и обучение представлений. Обработка последовательностей. Рекуррентные нейронные сети.

Тема 11. Кластеризация

K-means. EM-алгоритм. Другие методы кластеризации: иерархическая кластеризация, DBSCAN, Affinity Propagation.

Тема 12. Снижение размерности

SVD-разложение. Метод главных компонент. t-SNE, UMAP.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения данной дисциплины используются такие виды учебной работы, как лекция, лабораторный практикум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к зачету с оценкой.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском

искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции, обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические указания для обучающихся по выполнению лабораторных практикумов

Лабораторные практикумы выполняются в соответствии с учебным планом при последовательном изучении тем дисциплины.

Порядок проведения практикума.

Получение задания и рекомендаций к выполнению практикума.

Настройка инструментальных средств, необходимых для выполнения практикума (при необходимости).

Выполнение заданий практикума.

Подготовка отчета о выполненных заданиях в соответствии с требованиями.

Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций, рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии (при необходимости).

Требования к оформлению результатов практикумов (отчет)

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14, выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине определяется учебным планом.

При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя.

Работа с литературой (конспектирование)

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Реферат

Подготовка рефератов направлена на развитие и закрепление у обучающихся навыков самостоятельного глубокого, творческого и всестороннего анализа научной, методической и другой литературы по актуальным проблемам дисциплины; на выработку навыков и умений грамотно и убедительно излагать материал, четко формулировать теоретические обобщения, выводы и практические рекомендации.

Рефераты должны отвечать высоким квалификационным требованиям в отношении научности содержания и оформления.

Темы рефератов, как правило, посвящены рассмотрению одной проблемы. Объем реферата может быть от 12 до 15 страниц машинописного текста, отпечатанного через 1,5 интервала, а на компьютере через 1 интервал (список литературы и приложения в объем не входят).

Текстовая часть работы состоит из введения, основной части и заключения.

Во введении обучающийся кратко обосновывает актуальность избранной темы реферата, раскрывает конкретные цели и задачи, которые он собирается решить в ходе своего небольшого исследования.

В основной части подробно раскрывается содержание вопроса (вопросов) темы.

В заключении кратко должны быть сформулированы полученные

результаты исследования и даны выводы. Кроме того, заключение может включать предложения автора, в том числе и по дальнейшему изучению заинтересовавшей его проблемы.

В список литературы (источников и литературы) обучающийся включает только те документы, которые он использовал при написании реферата.

В приложении (приложения) к реферату могут выноситься таблицы, графики, схемы и другие вспомогательные материалы, на которые имеются ссылки в тексте реферата.

Навигация для обучающихся по самостоятельной работе в рамках изучения дисциплины

Наименование темы	**Вопросы, вынесенные на самостоятельное изучение**	**Формы самостоят. работы**	**Форма текущего контроля**
Тема 1. Введение в машинное обучение	Виды данных: структурированные таблицы, тексты, изображения, звук, логи.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму Подготовка реферата	Отчет по лабораторному практикуму Реферат
Тема 2. Статистические оценки и проверка гипотез	Основные понятия математической статистики: статистические оценки (точечные и интервальные), их свойства, проверка гипотез.		
Тема 3. Машинное обучение как математическое моделирование	Методы оценивания обобщающей способности, кросс-валидация.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 4. Введение в линейные модели и задача регрессии	Регуляризация.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 5. Линейные модели и задача классификации	Логистическая регрессия, максимизация правдоподобия, кросс-энтропия.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к	Отчет по лабораторному практикуму

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоят. работы	Форма текущего контроля
		лабораторному практикуму, подготовка отчета по практикуму	
Тема 6. Выбор и оценка моделей, работа с признаками	Операции в спрямляющих пространствах.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 7. Деревья и ансамбли	Ограничения линейных методов (пример: XOR). Решающие деревья. CART. Ансамбли. Бутстреп. Бэггинг. Случайный лес.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 8. Бустинг	AdaBoost, градиентный бустинг. XGBoost.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 9. Признаковые представления для дискретных входных данных	Обработка текстов: bag of words, tf-idf, векторные эмбеддинги.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 10. Современные нейросетевые архитектуры	Проблемы: затухающие и взрывающиеся градиенты, не выпуклость функции потерь.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 11. Кластеризация	Рекуррентные нейронные сети.	Работа с литературой, включая ЭБС, источниками в сети	Отчет по лабораторному практикуму

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоят. работы	Форма текущего контроля
		Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	
Тема 12. Снижение размерности	Affinity Propagation.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Иванюк, В. А. Практикум по нейронным сетям : учебное пособие / В. А. Иванюк. — Москва : Прометей, 2024. — 230 с. — ISBN 978-5-00172-601-2. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/153439/details

2. Корячко, В. П. Интеллектуальные системы и нечеткая логика : учебник / В. П. Корячко, М. А. Бакулева, В. И. Орешков. — Москва : КУРС, 2024. — 352 с. — ISBN 978-5-906923-39-4. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/144784/details

Дополнительная литература:

1. Алетдинова, А. А. Системы искусственного интеллекта : учебное пособие / А. А. Алетдинова, М. Г. Гриф. — Новосибирск : Новосибирский государственный технический университет, 2023. — 76 с. — ISBN 978-5-7782-5124-3. — Текст : электронный // Цифровой образовательный ресурс IPR CMART : [сайт]. — URL: https://www.iprbookshop.ru/books/156060/details

2. Сазонов, С. Н. Системы искусственного интеллекта : учебное пособие / С. Н. Сазонов. — Ульяновск : Ульяновский государственный технический университет, 2023. — 84 с. — ISBN 978-5-9795-2352-1. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/149293/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№ п/п	Наименование ресурса	Ссылка
1.	Открытый образовательный видеопортал UniverTV.ru	http://univertv.ru
2.	Информационно-аналитический портал по компьютерной тематике	https://habr.com/ru/
3.	Нечёткая логика: предпосылки возникновения и основные принципы	https://cyberleninka.ru/article/n/nechyotkaya-logika-predposylki-vozniknoveniya-i-osnovnye-printsipy?ysclid=ms7er9qdob158160217

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран);

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется

доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

- Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;
- Office Professional Plus Education ALng LSA OLVS E 3Y;
- Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);
- Антивирусная программа Dr.Web (отечественное программное обеспечение);
- ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

- 7-ZIP – архиватор (https://www.7-zip.org/)
- OpenOffice (https://www.openoffice.org/ru/)
- PDF24 Toolbox (https://www.pdf24.org/ru/)
- GIMP (редактор растровой графики) (https://www.gimp.org/)
- Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)
- Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

- Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

- Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

- Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)
- Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего

контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	10–9 – работа и отчет выполнены в срок, самостоятельно, правильно выбрано и использовано инфокоммуникационное оборудование, серверы и программное обеспечение, необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы; 8–7 – работа и отчет выполнены в срок, самостоятельно, правильно выбрано и использовано инфокоммуникационное оборудование, серверы и программное обеспечение, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 6 – работа и отчет выполнены в срок, самостоятельно, правильно выбрано и использовано инфокоммуникационное оборудование, серверы и программное обеспечение, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 5 – обучающийся подготовил работу и отчет самостоятельно, но присутствуют неточности или неполнота в описании выбранных программно-аппаратных средств, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 4 – обучающийся подготовил работу и отчет несамостоятельно или не завершил в срок, описание спецификации содержит незначительные ошибки, выводы и ответы на вопросы отсутствуют.
2.	Реферат	20 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 10 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 5 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые задания к лабораторным практикумам

Лабораторный практикум. Вариант1.

Задания на лабораторную работу (по вариантам)

В каждом варианте должна быть реализована и обучена полносвязная нейронная сеть (НС) прямого распространения с несколькими входами и

одним выходным нейроном. Ниже представлены задания, для построения НС.

Вариант	Задания
1	Вычислить сумму двух произвольных действительных чисел
2	Вычислить среднее арифметическое двух произвольных действительных чисел
3	Вычислить разность двух произвольных действительных чисел
4	Выполнить следующее преобразование двух произвольных действительных чисел: 5 − (x 1+ x 2)
5	Вычислить значения линейной функции вида: 3x+ 5
6	Вычислить значения линейной функции вида: 0,5x - 3

Содержание отчета

1. Титульный лист с названием лабораторной работы, номером своего варианта, фамилией студента и группы.
2. Тексты программ.
3. Результаты работы программ.

Лабораторный практикум. Вариант 2.

Для БД MNIST – изображений рукописных цифр создать архитектуру НС с наименьшим числом нейронов, достаточных для правильной классификации изображений тестовой выборки на уровне не менее 97%. Обучить НС с контролем эффекта переобучения путем использования выборки валидации.

Содержание отчета

1. Титульный лист с названием лабораторной работы, номером своего варианта, фамилией студента и группы.
2. Тексты программ.
3. Результаты работы программ.

Лабораторный практикум. Вариант 3.

Для БД CIFAR-10 – полноцветных изображений реальных объектов создать архитектуру сверточной НС с наименьшим числом нейронов, достаточных для правильной классификации изображений тестовой выборки на уровне не менее 92%. Обучить НС с контролем эффекта переобучения путем использования выборки валидации.

Содержание отчета

1. Титульный лист с названием лабораторной работы, номером своего варианта, фамилией студента и группы.
2. Тексты программ.
3. Результаты работы программ.

Лабораторный практикум. Вариант 4.

1. Скачать файл http://tk.ulstu.ru/lib/info/usdrub.txt, в котором хранится история котировок курса рубля по отношению к доллару с 1 января 2015 года по 19 августа 2021 года с шагом в один час.

2. Прочитать этот файл и на его основе в программе на Python сформировать одномерный список из котировок (поле CLOSE).

3. Разбить этот список на наблюдения по N отсчетов со сдвигом на один элемент.

Содержание отчета

1. Титульный лист с названием лабораторной работы, номером своего варианта, фамилией студента и группы.

2. Тексты программ.

3. Результаты работы программ.

Лабораторный практикум. Вариант 5.

1. Изучить материал по теории стилизации изображений.

2. Подготовить свое собственное полноцветное изображение (там, где сам студент на фотографии) в формате RGB размером 224x224 пикселей.

3. Подготовить второе полноцветное изображение тех же размеров и в том же формате для стиля. (У каждого студента должно быть свое стилевое изображение).

4. Повторить программу по стилизации и сформировать свое стилизованное изображение.

Примерные темы рефератов:

1. Принцип частичной прецедентности.
2. Тупиковые тесты.
3. Поиск ассоциативных правил
4. Примеры прикладных задач: анализ рыночных корзин, выделение терминов и тематики текстов.
5. Недостатки и пути усовершенствования алгоритма APriori.
6. Два этапа поиска частых наборов в FP-growth: построение FP-дерева и рекурсивное порождение частых наборов.
7. Задачи с частичным обучением
8. Постановка задачи Semisupervised Learning, примеры приложений.
9. Простые эвристические методы: self-training, co-training, co-learning.
10. Адаптация алгоритмов кластеризации для решения задач с частичным обучением
11. Алгоритм Expectation-Regularization на основе многоклассовой регуляризированной логистической регрессии.
12. Коллаборативная фильтрация
13. Корреляционные методы user-based, item-based.
14. Алгоритм Брегмана.
15. Метод стохастического градиента.
16. Анализ распространения информации в социальных сетях

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме

зачета.

Процедура оценивания	Шкала и критерии оценки, балл
зачет представляет собой выполнение обучающимся заданий билета, включающего в себя: Задание №1 – теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень владения обучающимся принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними; Задание №2 – задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности; Задание №3 – задание на проверку умений и навыков, полученных в результате освоения дисциплины	Выполнение обучающимся заданий оценивается по следующей балльной шкале: Задание 1: 0–30 баллов Задание 2: 0–30 баллов Задание 3: 0–40 баллов **«Зачтено»** **- 90 и более** – ответ правильный, логически выстроен, использована профессиональная лексика. Задание выполнено правильно. Обучающийся правильно интерпретирует полученный результат. **- 70 и более баллов –** ответ в целом правильный, логически выстроен, использована профессиональная лексика. Ход решения задачи правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. **- 50 и более баллов–** ответ в основном правильный, логически выстроен, использована профессиональная лексика. Задание выполнено частично. «**Не зачтено»** **- Менее 50 баллов** – ответы на теоретическую часть неправильные или неполные. Задание не выполнено

Типовые задания для проведения промежуточной аттестации обучающихся

<u>Задания 1-го типа</u>

1. Обзор задач, решаемых алгоритмами машинного обучения
2. Классификация алгоритмов машинного обучения
3. Линейные модели регрессии
4. Базисные функции
5. Регуляризация
6. Целевая функция логистической регрессии
7. Регуляризация логистической регрессии
8. Структура нейрона
9. Структура нейронной сети
10. Перцептрон
11. Обучения нейронной сети с помощью алгоритма обратного распространения ошибки
12. Структура деревьев решений
13. Виды разделяющих функций
14. Обучения дерева решений
15. Алгоритм Random Forest
16. Алгоритм AdaBoost
17. Каскад классификаторов
18. Кластеризация
19. Обучение без учителя

20. Алгоритм k-means

21. Иерархическая кластеризация

22. Метод сравнения с подкреплением.

23. Уравнения Беллмана.

24. Метод итераций по ценностям и по стратегиям.

25. Методы временных разностей: TD, SARSA, Q-метод.

26. Линейные модели регрессии. Применение линейной регрессии к нелинейным отношениям между переменными.

27. Проблема мультиколлинеарности. Разновидности линейных моделей и применение регуляризаторов.

28. Гребневая регрессия (Ridge, L2-регуляризация). LASSO (L1-регуляризация).

29. Логистическая регрессия. Сигмоидная функция в задачах бинарной классификации.

Задания 2-го типа

1. Записать общую формулу байесовского классификатора (надо помнить формулу).

2. Какие вы знаете три подхода к восстановлению плотности распределения по выборке?

3. Что такое наивный байесовский классификатор?

4. Что такое оценка плотности Парзена-Розенблатта (надо помнить формулу). Выписать формулу алгоритма классификации в методе парзеновского окна.

5. Многомерное нормальное распределение (надо помнить формулу). Вывести формулу квадратичного дискриминанта. При каком условии он становится линейным?

6. На каких предположениях основан линейный дискриминант Фишера?

7. Что такое EM-алгоритм, какова его основная идея? Какая задача решается на E-шаге, на M-шаге? Каков вероятностный смысл скрытых переменных?

8. Последовательное добавление компонент в EM-алгоритме, основная идея алгоритма.

9. Что такое стохастический EM-алгоритм, какова основная идея? В чём его преимущество (какой недостаток стандартного EM-алгоритма он устраняет)?

10. Что такое обобщённый алгоритм классификации (надо помнить формулу)? Какие вы знаете частные случаи?

11. Как определяется понятие отступа в метрических алгоритмах классификации?

12. Что такое окно переменной ширины, в каких случаях его стоит использовать?

13. Что такое метод потенциальных функций? Идея алгоритма настройки. Сравните с методом радиальных базисных функций.

14. Зачем нужен отбор опорных объектов в метрических алгоритмах

классификации?

15. Что такое функция конкурентного сходства? Основная идея алгоритма FRiS-СТОЛП.

16. Приведите пример метрического алгоритма классификации, который одновременно является байесовским классификатором.

17. Приведите пример метрического алгоритма классификации, который одновременно является линейным классификатором.

18. Метод стохастического градиента. Расписать градиентный шаг для квадратичной функции потерь и сигмоидной функции активации.

19. Недостатки метода SG и как они устраняются?

20. Как выражается функция потерь в логистической регрессии (надо помнить формулу).

21. Две мотивации и постановка задачи метода опорных векторов. Уметь вывести постановку задачи SVM (рекомендуется помнить формулу постановки задачи).

22. Какая функция потерь используется в SVM? В логистической регрессии? Какие ещё функции потерь Вы знаете?

23. Что такое ядро в SVM? Зачем вводятся ядра? Любая ли функция может быть ядром?

24. Какое ядро порождает полимиальные разделяющие поверхности?

25. В каких алгоритмах классификации можно узнать не только классовую принадлежность классифицируемого объекта, но и вероятность того, что данный объект принадлежит каждому из классов?

26. Приведите пример выборки, которую невозможно классифицировать без ошибок с помощью линейного алгоритма классификации. Какова минимальная длина выборки, обладающая данным свойством? Какие существуют способы модифицировать линейный алгоритм так, чтобы данная выборка стала линейно разделимой?

27. Почему любая булева функция представима в виде нейронной сети? Сколько в ней слоёв?

28. Метод обратного распространения ошибок. Основная идея. Основные недостатки и способы их устранения.

<u>Задания 3-го типа</u>

Задание 1.

Задача на построение модели классификации

Дано: файл с исходными данными – матрица «объектов-признаков» с метками (для моделей типа «обучение с учителем») Необходимо:

а) выполнить предварительную обработку данных и проектирование признаков, при необходимости;

б) выполнить обучение модели классификации методом k-ближайших соседей при трех различных значения параметра k;

в) выполнить оценку точности модели методом кросс-валидации по 5 и 10 блокам, проанализировать результаты и сделать выводы о качестве построенной модели.

Задание 2.

Задача на построение модели регрессии

Дано: файл с исходными данными – матрица «объектов-признаков» с метками (для моделей типа «обучение с учителем») Необходимо:

а) выполнить предварительную обработку данных и проектирование признаков, при необходимости;

б) выполнить обучение линейной модели регрессии с использованием L2- регуляризации (гребневая регрессия) с тремя различными параметрами α;

в) выполнить прогноз значений меток для тестовой (отложенной) части матрицы «объектов-признаков»;

г) выполнить оценку точности модели отложенных данных, проанализировать результаты и сделать выводы о качестве построенной модели.

Задание 3

Требуется составить обзор международной литературы обзор международной литературы об использовании методов тензорной алгебры для автоматической обработки текстов: для каких целей и в каких задачах используются эти методы и приводит ли их использованию к повышению качества результатов.

Задание 4

Реализация web и/или desktop демонстраций работы алгоритмов планирования поведения человека на основе нейросетевых подходов и психологических теорий на примере работы коалиции квадрокоптеров.

С использованием научных пакетов для Python и/или Java: numpy, matplotlib, scikit, Weka, web-пакеты для Python и/или Java (Django, Wicket).

Задание 5

Разработка и реализация процедуры выявления похожих строк. Исходные данные: Текстовый файл, каждая строка которого содержит ФИО человека в следующем формате: Фамилия + пробел + Инициал1 + точка + Инициал2 + точка

Примечания: 1) фрагмент Инициал2 + точка может отсутствовать. 2) В исходном файле могут быть одинаковые строки

Результат работы процедуры: Текстовый файл, строки которого те же, что и у входного файла, но все они упорядочены по убыванию степени похожести.

Рекомендуемый план исследования:

1) Изучение методов нечеткого сравнения строк.

2) Изучение различных метрик для выявления похожих строк, включая (как минимум) - косинусное расстояние, - расстояние Левенштейна, - расстояние Жаккарда.

3) Выбор 2-х метрик, наиболее подходящих для решения

поставленной задачи.

4) Реализация процедур нечеткого сравнения строк для 2-х выбранных метрик.

5) Сравнение полученных результатов.

6) Подготовка отчета, где будут представлены - Постановка задачи. - Теоретическая часть (методы и метрики нечеткого сравнения строк). - Практическая часть (спецификация реализованных алгоритмов). - Экспериментальная часть (сравнение результатов). - Заключение (выводы и рекомендации по использованию разработанных процедур).

Процедура должна быть реализована на языке Java или C++

Индийский филиал
Автономной некоммерческой организации высшего образования
«Московский университет «Синергия»

Рассмотрено
на заседании Ученого совета
Университета «Синергия»
протокол № 11 от 28.11.2025 г.

УТВЕРЖДАЮ
Ректор Университета «Синергия»
кандидат экономических наук, доцент
А. И. Васильев
01.12.2025 г.

Рабочая программа дисциплины «Организация добровольческой (волонтерской) деятельности и взаимодействие с социально-ориентированными НКО»

Направление подготовки: 10.04.01 Информационная безопасность
Профиль подготовки: Безопасность информационного и программного обеспечения автоматизированных систем
Квалификация выпускника: Магистр
Форма обучения: очная

2025

Содержание

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ 3

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ТЕМАТИЧЕСКИЙ ПЛАН 5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ....**ОШИБКА! ЗАКЛАДКА НЕ ОПРЕДЕЛЕНА.**

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 6

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 8

1. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Организация добровольческой (волонтерской) деятельности и взаимодействие с социально-ориентированными НКО» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от № 1455 от 26.11.2020.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в обязательную часть Блока 1 учебных планов по программам подготовки магистров по направлению 10.04.01 Информационная безопасность.

Дисциплина изучается на 2 курсе во 3 семестре.

Цели и задачи дисциплины

получение обучающимися теоретических знаний о добровольчестве (волонтерстве) как ресурсе личностного роста и общественного развития;

формирование представлений о многообразии добровольческой (волонтерской) деятельности и мотивации добровольцев (волонтеров);

приобретение практических навыков в сфере организации труда добровольцев (волонтеров), взаимодействия с социально ориентированными некоммерческими организациями, органами власти и подведомственными им организациям.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	Код компетенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	

Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	**УК-3**	УК-3.2. Уметь разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту	методы организации команды и приемы руководства работой команды, методики выработки командной стратегии для достижения поставленной цели	разрабатывать командную стратегию; применять эффективные стили руководства командой для достижения поставленной цели	умением анализировать, проектировать и организовывать межличностные, групповые и организационные коммуникации в команде для достижения поставленной цели	Контактная работа: Лекции Семинары Самостоятельная работа

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической подготовки		
Очная форма											
Раздел 1. Волонтерство как ресурс личностного роста и общественного развития. Многообразие форм добровольческой (волонтерской) деятельности	4	4								10	Контрольная работа /50
Раздел 2. Организация работы с волонтерами. Взаимодействие с социально-ориентированными НКО, инициативными группами, органами власти и иными организациями	4	4								10	Контрольная работа/50
Всего:	**8**	**8**								**20**	**100**
Контроль, час											**Зачет**
Объем дисциплины (в академических часах)	**36**										
Объем дисциплины (в зачетных единицах)	**1**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Волонтерство как ресурс личностного роста и общественного развития. Многообразие форм добровольческой (волонтерской) деятельности

Волонтерство как ресурс личностного роста и общественного развития. Многообразие форм добровольческой (волонтерской) деятельности

Раздел 2. Организация работы с волонтерами. Взаимодействие с социально-ориентированными НКО, инициативными группами, органами власти и иными организациями

Организация работы с волонтерами. Взаимодействие с социально-ориентированными НКО, инициативными группами, органами власти и иными организациями

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

Основы волонтерской деятельности : учебное пособие / С. Л. Балова, И. А. Безденежных, Е. Водолеева [и др.] ; под редакцией И. А. Фирсовой, Р. К. Крайневой. — Москва : Прометей, 2020. — 214 с. — ISBN 978-5-907244-73-3. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/125670/details

Дополнительная литература:

1. Зозуля, О. А. Организация волонтерской деятельности : учебное пособие / О. А. Зозуля. — Новосибирск : Новосибирский государственный технический университет, 2024. — 80 с. — ISBN 978-5-7782-5324-7. — Текст : электронный // Цифровой образовательный ресурс IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/155741/details

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1	Специализированный сайт по тематике информационной безопасности, противодействие вредоносному программному коду	http://z-oleg.com/index.php
2	Электронный фонд правовой и нормативно-технической документации	https://docs.cntd.ru/
3	Официальный сайт журнала «Директор по безопасности»	http://www.s-director.ru/

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в

себя:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, подтверждающая наличие материально-технического обеспечения, с перечнем основного оборудования:

мебель аудиторная (столы, стулья, доска аудиторная), стол преподавателя, стул преподавателя; персональный компьютер; набор демонстрационного оборудования (проектор, экран).

Помещение для самостоятельной работы обучающихся

Основное оборудование:

оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Университета из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

• Windows Professional 10 Russian Upgrade OLP NL AcademicEdition;

• Office Professional Plus Education ALng LSA OLVS E 3Y;

• Kaspersky Total Security для бизнеса Russian Edition (отечественное программное обеспечение);

• Антивирусная программа Dr.Web (отечественное программное обеспечение);

• ПО для видеоконференцсвязи и внутренних коммуникаций: ВКурсе (отечественное программное обеспечение https://vkurse.ru/)

свободно-распространяемое программное обеспечение:

• 7-ZIP – архиватор (https://www.7-zip.org/)

• OpenOffice (https://www.openoffice.org/ru/)

• PDF24 Toolbox (https://www.pdf24.org/ru/)

• GIMP (редактор растровой графики) (https://www.gimp.org/)

• Логином (Loginom) (отечественное программное обеспечение; https://loginom.ru/platform/pricing)

• Inkscape (векторная графика) (https://www.inkscape.org)

электронно-библиотечная система:

• Электронная библиотечная система (ЭБС) IPR BOOKS http://www.iprbookshop.ru

современные профессиональные базы данных и информационные справочные системы:

• Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.

Электронная библиотека научных публикаций eLIBRARY (https://elibrary.ru)

• Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/)

• Архив научных журналов НЭИКОН (https://arch.neicon.ru/xmlui/)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Контрольная работа	50–48 – верные ответы составляют более 90% от общего количества; 47–25 – верные ответы составляют 80-50% от общего количества; 24–0 – менее 50% правильных ответов.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

<u>Типовые задания к контрольным работам</u>

1. Понятие НКО, СО НКО, НКО - поставщики услуг в социальной сфере, НКо - исполнители общественно полезных услуг,

примеры.

2. Организационно-правовые формы НКО.

3. Количественные характеристики сектора негосударственных некоммерческих организаций в России.

4. Примеры добровольных объединений граждан России.

5. Примеры добровольных объединений граждан за рубежом.

6. Волонтерство как практика гражданского общества: понятие и явление.

7. Особенности функционирования СОНКО, отличия от государственных организаций и коммерческих компаний.

8. Виды ресурсов СОНКО, ресурсы как объект управления.

9. Технологии взаимодействия с частными и корпоративными донорами.

10. Мотивирование волонтеров и сотрудников СОНКО.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачета.

Краткая характеристика оценочного средства	Критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0–30 баллов Задание 2: 0–30 баллов Задание 3: 0–40 баллов «Зачтено» – 90–100 – ответ правильный, логически выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50–69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. «Не зачтено» – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Задания для проведения промежуточной аттестации обучающихся

1. Миссия и роли волонтерства.
2. Трудный и вдохновляющий опыт волонтерства.
3. Волонтерство как образ жизни современной молодежи.
4. Границы ответственности волонтера.
5. Методы поощрения волонтеров.

1. Волонтерство и его роль в системе социокультурных институтов.
2. Организация волонтерской службы в учреждениях разных типов и видов.
3. Система подготовки волонтеров и добровольцев по программе первичной профилактики наркозависимости, табакокурения и употребления ПАВ.
4. Методика работы волонтеров в условиях учреждений разных типов и видов. Семейное волонтерство.
5. Психолого-педагогическая специфика работы волонтеров с разновозрастной аудиторией.
6. Волонтерская служба в рамках реализации национальной программы развития молодежи.

1. Теория и практика волонтерского движения.
2. Концепция программы развития добровольческого движения.
3. Нормативно-правовая база деятельности волонтерской службы.
4. Основные направления волонтерской деятельности в учреждениях разных типов и видов.
5. Технология уличной работы.
6. Понятия, признаки и формы НКО.