Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

СОГЛАСОВАНО

Декан ФИТ А.С. Авдеев

Рабочая программа дисциплины

Код и наименование дисциплины: Б1.О.37 «Методы принятия организационно-технических решений»

Код и наименование направления подготовки (специальности): 10.03.01 Информационная безопасность

Направленность (профиль, специализация): Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)

Статус дисциплины: обязательная часть

Форма обучения: очная

Статус	Должность	И.О. Фамилия
Разработал	старший преподаватель доцент	Л.Д. Алфёрова Е.В. Шарлаев
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	Е.В. Шарлаев

г. Барнаул

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
ОПК-2.2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК-2.2.1	Анализирует структуру объекта защиты и его функциональные процессы
		ОПК-2.2.2	Формулирует предложения по повышению устойчивости объекта защиты к деструктивным воздействиям в соответствии с заданными критериями

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Защита информации от утечки по техническим каналам, Методы и средства криптографической защиты информации, Ознакомительная практика, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации, Моделирование и анализ процессов, систем и объектов защиты информации, Организация и проведение аудита защищенности объекта информатизации, Организация и технологии защиты данных в информационных системах, Разработка организационно-распорядительной документации по защите информации, Технологическая практика

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 3 / 108
Форма промежуточной аттестации: Зачет

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	32	0	32	44	71

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Форма обучения: очная
Семестр: 5

Лекционные занятия (32ч.)

1. Общая теория систем. Структурная модель системы безопасности информации. Организация защиты конфиденциальной информации на объектах информатизации. Государственная система защиты информации {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7] Основы функционирования Государственной системы защиты информации. Уровни функционирования ГСЗИ

2. Модели и методы поддержки принятия решений. Методы принятия решений по ЗИ {лекция с разбором конкретных ситуаций} (6ч.)[1,2,3,4,5,6,7] Методика численной оценки вероятности обнаружения нарушителя. Методика численной оценки уровня защищённости. Методика численной оценки уровня защищённости информации на основе экономических показателей

3. Понятие, виды, структура и функциональные характеристики объектов защиты информации {лекция с разбором конкретных ситуаций} (6ч.)[1,2,3,4,5,6,7] Классификация объектов защиты. Основополагающие признаки

4. Угрозы безопасности информации в условиях цифровой трансформации общества {лекция с разбором конкретных ситуаций} (6ч.)[1,2,3,4,5,6,7] Виды угроз. Методика оценки угроз

5. Состав и выбор мер по повышению устойчивости объекта защиты к деструктивным воздействиям в соответствии с выбранными критериями {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7] Оптимизация структуры и функциональных процессов объекта защиты и его информационных составляющих.

6. Обеспечение защиты информации в ГИС. {лекция с разбором конкретных ситуаций} (6ч.)[1,2,3,4,5,6,7] Требования к системе защиты информации в ГИС. Организация управленческих решений и применение современных технологий по обеспечению катастрофоустойчивости объекта защиты

Практические занятия (32ч.)

1. Применение системного анализа для построения модели системы безопасности информации {работа в малых группах} (4ч.)[1,2,3,4,5,6,7] Определение системы, элементы системы, входы и выходы. Обобщенное представление системы. свойства и связи системы.

2. Анализ структуры объекта защиты и его функциональных процессов. {работа в малых группах} (4ч.)[1,2,3,4,5,6,7] Определение выполнения требований Руководящих документов по защите информации в автоматизированных системах от несанкционированного доступа, исходя из

класса АС

3. Анализ структуры объекта защиты и его функциональных процессов. {работа в малых группах} (6ч.)[1,2,3,4,5,6,7] Определение набора мер защиты исходя из класса ГИС.

4. Анализ структуры объекта защиты и его функциональных процессов критической информационной инфраструктуры и автоматизированных систем управления технологическими процессами {мини-лекция} (2ч.)[1,2,3,4,5,6,7] Подходы к оптимизации структуры и функциональных процессов объекта защиты на основе проведенного анализа

5. Решение задач на определение классов ИС (АС), УЗ {метод кейсов} (2ч.)[1,2,3,4,5,6,7]

6. Проведение мероприятий по аттестации объектов информатизации {работа в малых группах} (4ч.)[1,2,3,4,5,6,7] Аттестация помещений, рабочих мест, аппаратно-программных средств обработки информации и систем (каналов) ее передачи на соответствие требованиям по защите информации

7. Подбор средств защиты информации {работа в малых группах} (4ч.)[1,2,3,4,5,6,7] Формулирование предложения по повышению устойчивости объекта защиты к деструктивным воздействиям в соответствии с заданными или самостоятельно сформулированными критериями

8. Применение методики численной оценки вероятности обнаружения нарушителя. {работа в малых группах} (6ч.)[1,2,3,4,5,6,7] Изучение методик численной оценки уровня защищённости и численной оценки уровня защищённости информации на основе экономических показателей.

Самостоятельная работа (44ч.)

1. Подготовка к текущим занятиям, к контрольной работе, самостоятельное изучение материала {с элементами электронного обучения и дистанционных образовательных технологий} (38ч.)[1,2,3,4,5,6,7]

2. Подготовка к зачету {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[1,2,3,4,5,6,7]

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронной информационно-образовательной среде АлтГТУ:

1. Методические указания по выполнению практических работ по дисциплине «Нормативные акты и стандарты по информационной безопасности»/Л.Д. Алферова; АлтГТУ им. И.И. Ползунова.- Барнаул, 2015.- 21 с. - http://elib.altstu.ru/eum/download/ivtib/uploads/alferova-l-d-ivtiib-563b0b4c3de4a.pdf

6. Перечень учебной литературы

6.1. Основная литература

2. Загинайлов, Ю.Н. Организационно-правовое обеспечение информационной
безопасности. В 2-х частях. Правовое обеспечение информационной безопас-
ности: Учебное пособие. Ч. 1 /Ю. Н. Загинайлов.- Барнаул : Изд-во АлтГТУ , 2012 - 172 с. –Режим доступа: http://new.elib.altstu.ru/eum/download/vsib/zaginajlov-opobespet.pdf

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология
защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

6.2. Дополнительная литература

3. Аверченков, В. И. Организационная защита информации : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – Брянск : Брянский государственный технический университет, 2012. – 184 с. – ISBN 978-89838-489-0. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/7002.html (дата обращения: 21.05.2023).

4. Милославская, Н. Г. Управление информационной безопасностью. Конспект лекций : учебное пособие / Н. Г. Милославская, А. И. Толстой. – Москва : Национальный исследовательский ядерный университет «МИФИ», 2020. – 534 с. – ISBN 978-5-7262-2694-1. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/125513.html (дата обращения: 21.05.2023).

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

5. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: http:// www.fstec.ru.

6. Правовая справочная система «Гарант» [электронный ресурс]: -режим доступа: http://www.garant.ru

7. Официальный сайт Совета Безопасности Российской Федерации http://www.scrf.gov.ru/

8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

№пп	Используемое программное обеспечение
1	LibreOffice
2	Windows
3	Антивирус Kaspersky

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Национальная электронная библиотека (НЭБ) – свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/)

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы
учебные аудитории для проведения учебных занятий
помещения для самостоятельной работы

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».