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.Д.3 «Методы и системы защиты информации, информационная безопасность»**

Код и наименование направления подготовки (специальности): **2.3.6. Методы и системы защиты информации, информационная безопасность**

Направленность (профиль, специализация):

Статус дисциплины: **дисциплины**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	заведующий кафедрой	А.Г. Якунин
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	

г. Барнаул

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
		- основные термины, понятия и их определения в области профиля научной специальности; - технологии обеспечения информационной безопасности и защиты информации; - современные программно-аппаратные средства и новейшие достижения в области обеспечения информационной безопасности; - порядок решения ряд конкретных практических задач, связанных с обеспечением информационной безопасности для различных объектов и систем, в том числе киберфизических систем и объектов критической информационной инфраструктуры	- применять технологии и методы обеспечения информационной безопасности при решении задач в сфере профессиональной деятельности; - применять современные программно-аппаратные средства и новейшие достижения в области информационной безопасности; - применять полученные знания и опыт при решении конкретных практических задач, связанных с с обеспечением информационной безопасности для различных объектов и систем, в том числе киберфизических систем и объектов критической информационной инфраструктуры	- навыками решения конкретных задач, связанных с разработкой, проектированием и внедрением аппаратных, программных, организационных средств и методов обеспечения информационной безопасности и защиты информации как для отдельных автоматизированных систем и рабочих мест, так и на уровне предприятия , в том числе для киберфизических систем и для объектов критической информационной инфраструктуры

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Научно-исследовательская практика
Дисциплины (практики), для которых результаты освоения	Научная деятельность, направленная на подготовку диссертации к защите

данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	

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: 4 / 144

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	0	0	35	109	51

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

Форма обучения: очная

Семестр: 4

Объем дисциплины в семестре з.е. /час: 2 / 72

Форма промежуточной аттестации: Зачет

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
0	0	17	55	25

Практические занятия (17ч.)

1. Тема 1: Теория и методология обеспечения информационной безопасности и защиты информации {дискуссия} (7ч.)[3,4,9,10,11,12,13,14] -Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.

-Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида

-Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.

-Модели и методы оценки защищенности информации и информационной

безопасности объекта.

-Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.

-Методы и модели выявления и противодействия распространению ложной и вредоносной информации.

2. Тема 2: Организационно-правовые аспекты обеспечения информационной безопасности и защиты информации {дискуссия} (6ч.)[2,6,9,10] -Методы и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.

-Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации

-Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования

-Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.

-Модели, методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.

-Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих организационных методов защиты информации и обеспечения информационной безопасности.

-Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем.

3. Тема 3: Обеспечение безопасности в компьютерных сетях {дискуссия} (4ч.)[1,3,5,7,9,10,12,14] -Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

-Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях.

-Методы, модели и средства, а также комплексы средств противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет

-Модели, методы и средства противодействия отказам в обслуживании и другим видам компьютерных атак

-Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.

Самостоятельная работа (55ч.)

4. Подготовка к практическим занятиям {творческое задание} (45ч.)[1,2,3,4,5,6,7,9,10,11,12,13,14] Углубленное изучение выносимого на практические занятия теоретического материала.

Оценка возможности применения полученных знаний на практике,в частности, ск теме научной диссертации

Оценка возможности применения современных новейших достижений в области обеспечения информационной безопасности при разработке и внедрении организационных, программно-технических и иных средств и мер на предприятиях и организациях

Применение полученных знаний и опыта при решении конкретных практических задач по теме диссертации.

А также:

после овладения научно-предметной областью знаний научиться профессионально излагать результаты своих исследований и представлять их в виде научных публикаций, информационно-аналитических материалов и презентаций

5. Подготовка к зачёту {тренинг} (10ч.)[1,3,4,6] Повторение и закрепление пройденного в семестре учебного материала

Семестр: 5

Объем дисциплины в семестре з.е. /час: 2 / 72

Форма промежуточной аттестации: Экзамен

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
0	0	18	54	26

Практические занятия (18ч.)

1. Тема 4: Программно-аппаратные средства обеспечения информационной безопасности и защиты информации {дискуссия} (4ч.)[3,5,6,8,9,10,11,12,13,14]

-Методы и аппаратно-программные средства для защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.

-Принципы и решения по созданию новых и совершенствованию существующих программно-аппаратных средств защиты информации и обеспечения информационной безопасности.

-Современные тенденции развития программно-аппаратных средств защиты информации и обеспечения информационной безопасности

-Тема: Инженерно-технические средства обеспечения информационной безопасности и защиты информации – 6 ч

-Новые подходы и методы, используемые при создании извещателей пожарно-

охранной сигнализации

-Общие принципы построения и тенденции развития современных средств контроля и управления доступом

2. Инженерно-технические средства обеспечения информационной безопасности и защиты информации {дискуссия} (6ч.)[5,7,8,9,11,12,13,14] -Новые подходы и методы, используемые при создании извещателей пожарно-охранной сигнализации

-Общие принципы построения и тенденции развития современных средств контроля и управления доступом

3. Информационная безопасность объектов критической информационной инфраструктуры (КИИ) {дискуссия} (4ч.)[3,9,10,11,12,13,14] -Объекты и субъекты КИИ и их категорирование

-Особенности обеспечения информационной безопасности объектов КИИ

-Общие принципы построения системы обеспечения информационной безопасности КИИ

-Правовое регулирование в области обеспечения безопасности значимых объектов КИИ

4. Особенности обеспечения информационной безопасности киберфизических систем {дискуссия} (4ч.)[5,7,8,9,10,11,12,13] -Методы выявления и прогнозирования появления нештатных ситуаций в киберфизических истемах

-Управление информационной безопасностью и управление рисками в киберфизической системе

-Особенности обеспечения информационной безопасности беспроводного сетевого взаимодействия самоорганизующихся киберфизических систем и компонентов IoT

-Принципы, решения (технические, математические, организационные и др.) и тенденции развития методов защиты информации и обеспечения информационной безопасности киберфизических систем.

Самостоятельная работа (54ч.)

5. Подготовка к практическим занятиям {творческое задание} (27ч.)[1,5,7,8,9,10,11,12,13,14] Углубленное изучение выносимого на практические занятия теоретического материала.

Оценка возможности применения полученных знаний на практике,в частности, ск теме научной диссертации

Оценка возможности применения современных новейших достижений в области обеспечения информационной безопасности при разработке и внедрении организационных, программно-технических и иных средств и мер на предприятиях и организациях

Применение полученных знаний и опыта при решении конкретных практических задач по теме диссертации.

А также:
после овладения научно-предметной областью знаний научиться профессионально излагать результаты своих исследований и представлять их в виде научных публикаций, информационно-аналитических материалов и презентаций
6. Подготовка к экзамену {тренинг} (27ч.)[3,4,5,6,7,8] Повторение и закрепление пройденного учебного материала, а также
подготовка презентации и научной статьи по теме изученного материала и связанных с ним результатов научных исследований

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

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Шарлаев Е.В. Вычислительные сети. Учебно-методическое пособие/ Е.В. Шарлаев; Алт. гос. техн. ун – т им. И.И. Ползунова, - Барнаул: 2015. - 86 с. Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/uploads/sharlaev-e-v-ivtiib-569e03fec1d87.pdf
2. 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

3. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 19.01.2023). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный

4. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 19.01.2023). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный

5. Гаенко, В. П. Безопасность технических систем. Методологические аспекты теории, методы анализа и управления безопасностью : монография / В. П. Гаенко, В. Е. Костюков, В. Н. Фомченко. — Саров : Российский федеральный

ядерный центр – ВНИИЭФ, 2020. — 329 с. — ISBN 978-5-9515-0452-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/101918.html (дата обращения: 19.01.2023). — Режим доступа: для авторизир. пользователей

6.2. Дополнительная литература

6. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие : [16+] / Е. Н. Чекулаева, Е. С. Кубашева ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2020. – 156 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612591 (дата обращения: 19.01.2023). – Библиогр.: с. 127-129. – ISBN 978-5-8158-2165-1. – Текст : электронный

7. Петров, В. В. Комплексные системы безопасности современного города : учебное пособие / В. В. Петров, В. В. Коробкин, А. Б. Сивенко ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 158 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499967 (дата обращения: 19.01.2023). – Библиогр.: с. 136-144. – ISBN 978-5-9275-2587-4. – Текст : электронный

8. Александровская, Л. Н. Безопасность и надежность технических систем : учебное пособие / Л. Н. Александровская, И. З. Аронов, В. И. Круглов. — Москва : Логос, 2008. — 376 с. — ISBN 978-5-98704-115-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/9055.html (дата обращения: 19.01.2023). — Режим доступа: для авторизир. пользователей

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

9. Периодический рецензируемый научный журнал «Безопасность информационных технологий».-URL: https://bit.mephi.ru/index.php/bit

10. Журнал «Проблемы информационной безопасности. Компьютерные системы». -URL: https://jisp.ru/

11. Официальный сайт Совета Безопасности Российской Федерации .-URL: http://www.scrf.gov.ru/

12. 12.□Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России.-URL: https://fstec.ru/

13. Официальный сайт Федеральной службы безопасности (ФСБ) России.-URL: http://www.fsb.ru

14. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).-URL: https://rkn.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.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

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	Foxit Reader
3	Mozilla Firefox
4	ViPNet CSP
5	Windows
6	Антивирус Kaspersky
7	Гарант

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	IEEE Xplore - Интернет библиотека с доступом к реферативным и полнотекстовым статьям и материалам конференций. Бессрочно без подписки (https://ieeexplore.ieee.org/Xplore/home.jsp)
2	Springer - Издательство с доступом к реферативным и полнотекстовым материалам журналов и книг (https://www.springer.com/gp https://link.springer.com/)
3	«Базовые нормативные документы» ООО «Группа компаний Кодекс», программные продукты «Кодекс» и «Техэксперт» (https://kodeks.ru)
4	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru)
5	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/)
6	Электронный фонд правовой и научно-технической документации - (http://docs.cntd.ru/document)

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

Наименование специальных помещений и помещений для самостоятельной работы
лаборатории
учебные аудитории для проведения групповых и индивидуальных консультаций
учебные аудитории для проведения текущего контроля и промежуточной аттестации
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».