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.35 «Комплексная защита объектов информатизации»

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	доцент старший преподаватель	А.В. Санников В.В. Нечаева
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	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИДК-ОПК-2.1	Применяет информационно-коммуникационные технологии для решения задач профессиональной деятельности
		ИДК-ОПК-2.2	Применяет программные средства системного и прикладного назначения при решении задач профессиональной деятельности
		ИДК-ОПК-2.3	Применяет отечественное программное обеспечение
ОПК-6	Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1	Выбирает нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской федерации, Федеральной службы по техническому и экспортному контролю
		ОПК-6.2	Способен организовать защиту информации ограниченного доступа при решении профессиональных задач
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1	Выбирает и анализирует научно-техническую литературу, нормативные и методические документы для решения задач профессиональной деятельности
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1	Формулирует принципы политики информационной безопасности
		ОПК-10.2	Способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности объекта защиты
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1	Готовит исходные данные проектирования подсистем, средств обеспечения защиты информации
ОПК-2.3	Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-2.3.1	Способен разрабатывать и внедрять комплекс мер по обеспечению информационной безопасности объекта защиты

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, Организационное и правовое обеспечение информационной безопасности, Основы управления информационной безопасностью, Особенности защиты информации объектов критической информационной инфраструктуры, Программно-аппаратные средства защиты информации
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Подготовка к процедуре защиты и защита выпускной квалификационной работы, Преддипломная 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: 5 / 180
Форма промежуточной аттестации: Экзамен

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	30	40	0	110	81

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

Форма обучения: очная
Семестр: 8

Лекционные занятия (30ч.)

1. Комплексная система защиты информации {лекция с разбором конкретных ситуаций} (2ч.)[1,3,4,5,6] Принципы организации и этапы разработки комплексной системы защиты информации. Методологические основы организации КСЗИ. Цели, задачи и принципы построения КСЗИ. Требования, предъявляемые к КСЗИ. Этапы разработки КСЗИ. Выбор и анализ научно-технической литературы, нормативных и методических документов для решения задачи построения КСЗИ.

2. Факторы, влияющие на организацию КСЗИ {лекция с разбором

конкретных ситуаций} (2ч.)[1,3,4,5,6] Факторы, влияющие на организацию комплексной системы защиты информации. Перечень факторов, влияющих на организацию КСЗИ. Факторы, определяющие особенности защиты информации ограниченного доступа. Факторы, оказывающие влияние на построение КСЗИ.

3. Состав защищаемой информации {с элементами электронного обучения и дистанционных образовательных технологий} (2ч.)[1,3,4,5,6] Определение и нормативное закрепление состава защищаемой информации. Нормативно-правовые аспекты определения состава защищаемой информации. Методика определения состава защищаемой информации и её нормативное закрепление. Выбор нормативных правовых актов, нормативных и методических документов Федеральной службы безопасности Российской федерации, Федеральной службы по техническому и экспортному контролю.

4. Объекты защиты информации {лекция с разбором конкретных ситуаций} (3ч.)[1,3,4,5,6] Функциональный процесс и определение объектов защиты информации. Виды и типы объектов информатизации. Функциональный процесс и его информационные составляющие. Объекты защиты информации. Методика определения объектов комплексной защиты информации.

5. Угрозы безопасности информации {лекция с разбором конкретных ситуаций} (3ч.)[1,3,4,5,6] Анализ и оценка угроз безопасности информации для объекта информатизации. Цели и задачи оценки угроз безопасности информации. Основные методики анализа и оценки угроз безопасности информации. Источники, способы и результаты воздействия на информацию.

6. Каналы и методы несанкционированного доступа к информации {лекция с разбором конкретных ситуаций} (3ч.)[1,3,4,5,6] Определение потенциальных каналов и методов несанкционированного доступа к информации. Методика выявления каналов несанкционированного доступа к информации. Определение вероятных методов несанкционированного доступа к защищаемой информации. Определение вероятных методов НСД к ИСПДн и ГИС.

7. Модель нарушителя {лекция с разбором конкретных ситуаций} (3ч.)[1,3,4,5,6] Определение возможностей несанкционированного доступа к защищаемой информации. Методика выявления нарушителей и состава интересующей их информации. Определение возможностей НСД к защищаемой информации внутренними нарушителями. Определение возможностей НСД к защищаемой информации внешними нарушителями. Модель нарушителя.

8. Компоненты комплексной системы защиты информации {лекция с разбором конкретных ситуаций} (3ч.)[1,3,4,5,6] Определение компонентов комплексной системы защиты информации. Компоненты КСЗИ. Методы определения компонентов КСЗИ. Синтез КСЗИ. Применение информационно-коммуникационных технологий для решения задачи построения КСЗИ. Применение программных средств системного и прикладного назначения, в том числе отечественного программного обеспечения.

9. Концепция комплексной системы защиты информации {лекция с разбором конкретных ситуаций} (3ч.)[1,3,4,5,6] Определение условий

функционирования и разработка концепции комплексной системы защиты информации. Основные условия функционирования КСЗИ определяемые при её создании или модернизации. Содержание концепции построения КСЗИ. Основные положения концепции относительно объектов, целей, задач защиты и угроз безопасности информации. Основные положения концепции по обеспечению безопасности информации. Организация защиты информации ограниченного доступа, поддержание выполнения комплекса мер по обеспечению информационной безопасности объекта защиты.

10. Создание комплексной системы защиты информации {лекция с разбором конкретных ситуаций} (3ч.)[1,3,4,5,6] Технологическое и организационное построение КСЗИ. Общее содержание работ по организации КСЗИ. Характеристика основных стадий создания КСЗИ. Назначение и структура задания на проектирование, технического задания, технического проекта.

11. Функциональная модель КСЗИ. Аттестация объекта информатизации {лекция с разбором конкретных ситуаций} (3ч.)[1,3,4,5,6] Разработка модели КСЗИ и аттестация объекта информатизации. Понятие модели объекта, основные виды моделей и их характеристики. Модель как инструмент количественного и качественного анализа КСЗИ. Функциональная модель КСЗИ. Организационная модель КСЗИ. Информационная модель КСЗИ. Организация аттестации объекта информатизации.

Лабораторные работы (40ч.)

1. Состав защищаемой информации {работа в малых группах} (10ч.)[1,2,3,4,5,6,7,8] Определение и нормативное закрепление состава защищаемой информации организации.

2. Объекты защиты {работа в малых группах} (10ч.)[1,2,3,4,5,6,7,8] Анализ функционального процесса и определение объектов защиты при проектировании КСЗИ. Подготовка исходных данных для проектирования подсистем КСЗИ, средств обеспечения защиты информации.

3. Угрозы безопасности информации {работа в малых группах} (10ч.)[1,2,3,4,5,6,7,8] Разработка модели угроз безопасности объектам информатизации организации.

4. Концепция КСЗИ {работа в малых группах} (10ч.)[1,2,3,4,5,6,7,8] Разработка элементов концепции КСЗИ объекта информатизации и политики информационной безопасности организации. Формулировка принципов политики информационной безопасности. Разработка и внедрение комплекса мер по обеспечению информационной безопасности объекта защиты.

Самостоятельная работа (110ч.)

1. Подготовка к текущим занятиям(34ч.)[1,2,3,4,5,6,7,8]

2. Написание курсовой работы и подготовка к ее защите.(40ч.)[1,2,3,4,5,6,7,8] Тема выбирается из списка, составленного преподавателем.

3. Подготовка к экзамену(36ч.)[1,2,3,4,5,6,7,8]

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

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

1. Загинайлов Ю.Н. Информационная безопасность предприятия (организации): курс визуальных лекций / Ю.Н. Загинайлов; Алт.гос.техн.ун-т им. И.И.Ползунова.- Барнаул: Изд-во АлтГТУ.-2016-90с.
Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-58622503493eb.pdf

2. Загинайлов Ю.Н. Методические рекомендации к выполнению лабораторных работ по дисциплине «Информационная безопасность предприятия» / Ю.Н. Загинайлов, О.С. Лесковец, Алт. гос. тех. ун-т им. И.И. Ползунова. – Барнаул: АлтГТУ. – 2015. -74 с. Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-54c1f980e1ae4.pdf

6. Перечень учебной литературы

6.1. Основная литература

3. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. : ил., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 24.04.2023). – Библиогр. в кн. – ISBN 978-5-9765-1271-9. – Текст : электронный.

4. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации : учебное пособие / С. И. Козьминых ; Финансовый университет при Правительстве Российской Федерации. – Москва : Юнити-Дана, 2020. – 544 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 24.04.2023). – Библиогр. в кн. – ISBN 978-5-238-03200-9. – Текст : электронный.

6.2. Дополнительная литература

5. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. – Саров : Российский федеральный ядерный центр –

ВНИИЭФ, 2019. – 224 с. – ISBN 978-5-9515-0429-6. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/101925.html (дата обращения: 24.04.2023). – Режим доступа: для авторизир. пользователей

6. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум : [16+] / авт.-сост. М. А. Лапина, Д. М. Марков, Т. А. Гиш, М. В. Песков [и др.]. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 242 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=458012 (дата обращения: 24.04.2023). – Библиогр. в кн. – Текст : электронный.

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

7. Официальный сайт Федеральной службы по техническому и экспортному контролю Российской Федерации https://fstec.ru/

8. Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.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

№пп	Используемые профессиональные базы данных и информационные справочные системы
	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».