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.34 «Основы управления информационной безопасностью»

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-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.3	Использует нормативные правовые акты, нормативные методические документы в профессиональной деятельности
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-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-10.3	Способен управлять процессом реализации комплекса мер по обеспечению информационной безопасности

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Организационное и правовое обеспечение информационной безопасности, Основы управления проектами
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации

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 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	32	0	32	80	71

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

Форма обучения: очная

Семестр: 7

Лекционные занятия (32ч.)

1. Назначение, структура и содержание управления информационной безопасностью {лекция с разбором конкретных ситуаций} (5ч.)[1,3,5] Понятие, сущность и цели управления информационной безопасностью. Принципы организации защиты информации ограниченного доступа. Принципы управления информационной безопасностью. Основные процессы, функции и задачи управления информационной безопасностью. Структура и содержание общей технологии управления информационной безопасностью. Основные стандарты по управлению информационной безопасностью.

2. Современные модели управления информационной безопасностью предприятия {лекция с разбором конкретных ситуаций} (5ч.)[1,3,5] Процессный подход. Модель "plan-do-check-act" (PDCA). Основные этапы работ по созданию и (или) внедрению системы управления информационной безопасностью. Система управления информационной безопасностью как компонент комплексной системы защиты информации на предприятии. Использование нормативных правовых актов, нормативных методических документов, в том числе документов ФСБ России и ФСТЭК России для организации защиты информации на предприятии.

3. Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности {лекция с разбором конкретных ситуаций} (5ч.)[1,4,6] Предпосылки разработки политики безопасности предприятия. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия. Формирование политики информационной безопасности на предприятии. Политика информационной безопасности предприятия. Управление процессом реализации комплекса мер по обеспечению информационной безопасности.

4. Методология управления рисками в области информационной безопасности {лекция с разбором конкретных ситуаций} (5ч.)[1,3,5] Основные

понятия и стандартизация в области менеджмента риска информационной безопасности. Составляющие процесса менеджмента риска. Установление контекста. Оценка риска. Обработка риска информационной безопасности. Принятие и коммуникация риска ИБ. Мониторинг и переоценка риска ИБ.

5. Менеджмент инцидентов информационной безопасности в организации {лекция с разбором конкретных ситуаций} (4ч.)[1,3,5] Инциденты информационной безопасности. Структурный подход к менеджменту инцидентов. Международная практика управления инцидентами. Этапы менеджмента инцидентов информационной безопасности: планирование и подготовка, использование, анализ, улучшение. Разработка политики и программы менеджментов информационной безопасности. Реагирование на инциденты.

6. Структура, задачи и функции подразделений, обеспечивающих информационную безопасность предприятия {лекция с разбором конкретных ситуаций} (4ч.)[1,3,5] Организационная структура подразделений, обеспечивающих информационную безопасность предприятия. Задачи и функции подразделений. Документальное обеспечение политики информационной безопасности. Внедрение средств защиты информации. Администрирование информационных систем и систем защиты информации. Аудит информационной безопасности. Охрана имущества предприятия. Управление процессом реализации комплекса мер по обеспечению информационной безопасности.

7. Управление информационной безопасностью на государственном уровне: общие принципы и российская практика {с элементами электронного обучения и дистанционных образовательных технологий} (4ч.)[1,4,5,6] Предпосылки развития государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в Российской Федерации.

Практические занятия (32ч.)

1. Назначение, структура и содержание управления информационной безопасностью {дискуссия} (5ч.)[2,3,4,5] Понятие, сущность и цели управления информационной безопасностью. Принципы управления информационной безопасностью. Основные процессы, функции и задачи управления информационной безопасностью. Основные стили управления. Структура и содержание общей технологии управления информационной безопасностью. Основные стандарты по управлению информационной безопасностью.

2. Современные модели управления информационной безопасностью предприятия {дискуссия} (5ч.)[2,3,4,5] Процессный подход. Модель «plan-do-check-act» " (PDCA). Модель Деминга. Этапы построения и использования

СУИБ в этой модели. Внедрение СМИБ. Основные этапы работ по созданию и (или) внедрению СУИБ. Алгоритм внедрения СУИБ. Основные задачи разработки, внедрения или совершенствования. Основные этапы работ по построению и внедрению СУИБ. СУИБ как компонент комплексной системы защиты информации на предприятии. КСЗИП и её структура. Подсистема управления КСЗИП. Нормативно-правовые и методические документы.

3. Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности {дискуссия} (5ч.)[2,3,4,5] Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия. Структура политики информационной безопасности и процесс ее разработки. Политика информационной безопасности предприятия: верхний уровень. Политика информационной безопасности предприятия: средний уровень.

4. Управление рисками в области информационной безопасности {дискуссия} (5ч.)[2,3,4,5] Основные понятия и стандартизация в области менеджмента риска информационной безопасности. Составляющие процесса менеджмента риска. Установление контекста. Оценка риска. Обработка риска. Принятие и коммуникация риска. Мониторинг и переоценка риска.

5. Менеджмент инцидентов информационной безопасности в организации {дискуссия} (4ч.)[2,3,4,5] Структурный подход к менеджменту инцидентов ИБ. Международная практика управления инцидентами ИБ. Этапы менеджмента инцидентов ИБ. Разработка политики и программы менеджмента инцидентов ИБ. Реагирование на инциденты ИБ.

6. Структура, задачи и функции подразделений, обеспечивающих информационную безопасность предприятия {дискуссия} (4ч.)[2,3,4,5] Организационная структура подразделений, обеспечивающих информационную безопасность предприятия. Примерная структура отдела ИБ и основные взаимодействующие подразделения. Комплектование специалистами подразделений. Задачи и функции подразделений, обеспечивающих информационную безопасность.

7. Управление информационной безопасностью на государственном уровне {дискуссия} (4ч.)[2,3,4,5] Предпосылки развития государственного управления в сфере информационной безопасности. Общая методология и структура организационного обеспечения информационной безопасности на уровне государства. Общая политика России в сфере информационной безопасности. Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.

Самостоятельная работа (80ч.)

1. **Подготовка к текущим занятиям(44ч.)[1,2,3,4,5,6]**
2. **Подготовка к экзамену(36ч.)[1,2,3,4,5,6]**

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. Управление информационной безопасностью : курс визуальных лекций / Ю.Н. Загинайлов; Алт.гос.техн.ун-т им.И.И.Ползунова.- Баранаул: Изд-во АлтГТУ.-2016- 128с. Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-586224a37ee70.pdf

2. Загинайлов Ю.Н. Методические рекомендации к семинарским занятиям и указания к самостоятельной работе студентов по дисциплине «Управление информационной безопасностью»/ Алт.гос.техн.ун-т им.И.И.Ползунова.-Барнаул; Изд-во АлтГТУ.-2015-140с. Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-54c8f9894b941.pdf

6. Перечень учебной литературы

6.1. Основная литература

3. 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: 24.04.2023). – Библиогр.: с. 127-129. – ISBN 978-5-8158-2165-1. – Текст : электронный.

4. Шилов, А. К. Управление информационной безопасностью : учебное пособие : [16+] / А. К. Шилов ; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 24.04.2023). – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный.

6.2. Дополнительная литература

5. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. – 3-е изд. – Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 211 с. – ISBN 978-5-4497-0328-6. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/89443.html (дата обращения: 24.04.2023). –

Режим доступа: для авторизир. пользователей

6. 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: 24.04.2023). – Режим доступа: для авторизир. пользователей

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

7. Интернет-издание о высоких технологиях - CNews https://www.cnews.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
4	Гарант
5	Яндекс.Браузер

№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».