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.В.5 «Информационная безопасность автоматизированных систем»**

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

Направленность (профиль, специализация): **Организация и технология защиты информации**

Статус дисциплины: **часть, формируемая участниками образовательных отношений (вариативная)**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	старший преподаватель	А.В. Циклаков
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 планируемыми результатами освоения образовательной программы

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	знать отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, в том числе знать документы в области построения защищенных автоматизированных систем	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, в том числе в целях построения защищенных автоматизированны х систем	навыками применения стандартов в области компьютерной безопасности для оценки защищённости компьютерных систем, в том числе стандартов в области построения автоматизированных систем с учетом требований регуляторов по защите информации
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации	методы и средства и /или физические основы проведения экспериментальных исследований систем защиты информации, в том числе методы и средства проведения экспериментальных исследований по оценке защищенности компьютерных систем	экспериментально выявлять уязвимости систем защиты информации, в том числе эксплуатируемых в автоматизированны х системах	методами выявления уязвимостей автоматизированных систем, в том числе с использованием специализированного программного обеспечения
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты	методы и приемы администрирования подсистем информационной безопасности объекта защиты, в том числе методы администрирования средств защиты информации автоматизированных систем	применять методы и приемы администрирования подсистем информационной безопасности объекта защиты, в том числе методы конфигурирования средств защиты информации автоматизированны х систем	навыками администрирования подсистемы информационной безопасности объекта защиты, в том числе навыками эксплуатации средств защиты информации компьютерных систем
ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических	действующие нормативные и методические документы в области информационной безопасности, в том	Оформлять рабочую техническую документацию с учетом действующих нормативных и	методами формирования требований по защите информации в соответствии с нормативными

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
	документов	числе документы в области построения защищенных автоматизированных систем	методических документов, в том числе с учетом положений нормативных актов и методических документов ФСБ и ФСТЭК России	актами и стандартами, в том числе методами формирования требований по защищенности автоматизированных систем

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Информационные технологии, Организационное и правовое обеспечение информационной безопасности, Программно-аппаратные средства защиты информации, Сети и системы передачи информации, Техническая защита информации, Технологии хранения и защиты информации в базах данных
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексное обеспечение защиты информации объекта информатизации, Технико-экономическое обоснование проектных решений

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	11	33	0	64	54

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 (11ч.)

1. Введение. Информационная безопасность автоматизированных систем. {лекция с разбором конкретных ситуаций} (2ч.)[4] Программы высшего образования в области информационной безопасности. Основная образовательная программа по направлению подготовки бакалавров «Информационная безопасность». Программа дисциплины «Информационная безопасность автоматизированных систем». Анализ информационной безопасности объектов и систем на соответствие требованиям стандартов.

2. Угрозы безопасности информации. {лекция с разбором конкретных ситуаций} (3ч.)[5] Задачи защиты информации в автоматизированных системах. Основные угрозы информации в АС и специфика их возникновения. Основные виды и источники угроз безопасности информации в КС. Понятие угрозы. Общая классификация угроз. Виды и источники угроз. Структура угрозы. Уязвимости и специфика их возникновения. Понятие уязвимости. Причины возникновения уязвимости. Методики проведения экспериментальных исследований системы защиты информации АС.

3. Модели безопасности информации в КС и АС. {лекция с разбором конкретных ситуаций} (4ч.)[2] Дискреционная политика и модели безопасности. Мандатная политика и модели безопасности. Ролевая политика и модели безопасности. Определение политики и модели безопасности АС. Дискреционная политика безопасности. Варианты задания матрицы доступа. Проблема доказательства безопасности КС с дискреционной политикой. Модель Харрисона-Рузо-Ульмана. Достоинства и недостатки дискреционных моделей безопасности. Состав средств защиты. Аспекты администрирования подсистемы информационной безопасности АС.

4. Автоматизированные системы в защищенном исполнении. {лекция с разбором конкретных ситуаций} (2ч.)[3] Создание информационных автоматизированных систем в защищенном исполнении. Общие положения по созданию АСЗИ. Типовое содержание работ по защите информации. Роль стандартов информационной безопасности для защиты информации в АС. Основные понятия, используемые в стандартах защищенности АС. Оформление рабочей технической документации с учетом действующих нормативных и методических документов.

Лабораторные работы (33ч.)

1. Исследование политик безопасности. {работа в малых группах} (8ч.)[1] Установка и настройка СЗИ. Исследование политик безопасности.

2. Защита информации на уровне операционной системы. {работа в малых группах} (8ч.)[1] Защита информации на уровне ОС в локальных и глобальных сетях. Определение требований к защищённости межсетевого экрана в АС,

обрабатывающей информацию ограниченного доступа.
3. Гарантированное удаление данных. {работа в малых группах} (6ч.)[1] Безопасное удаление данных. Затирание информации с применением специализированного программного комплекса.
4. Контроль устройств. {работа в малых группах} (6ч.)[1] Контроль устройств средствами защиты информации. Поиск и удаление информации о подключенных технических средствах.
5. Анализ трафика в вычислительных сетях. {работа в малых группах} (5ч.)[1] Прослушивание трафика, аудит событий, сканирование объектов информатизации.

Самостоятельная работа (64ч.)
1. Подготовка к текущему контролю успеваемости (выполнение и защита лабораторных работ) {с элементами электронного обучения и дистанционных образовательных технологий} (30ч.)[5,9,11]
2. Подготовка к промежуточной аттестации (зачёт) {с элементами электронного обучения и дистанционных образовательных технологий} (10ч.)[2,3,4,5,6,7,8]
3. Подготовка к текущим занятиям, самостоятельное изучение материала {с элементами электронного обучения и дистанционных образовательных технологий} (24ч.)[7]

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. Методические указания по выполнению лабораторных работ по дисциплине «Информационная безопасность автоматизированных систем/Л.Д. Алферова; АлтГТУ им. И.И. Ползунова.- Барнаул, 2015.- 21 с.: http://new.elib.altstu.ru/eum/download/ivtib/uploads/alferova-l-d-ivtiib-55ed5d9c36f70.pdf

6. Перечень учебной литературы

6.1. Основная литература

2. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учебное пособие / П.Н. Девянин. — Электрон. дан. — Москва : Горячая линия-Телеком, 2017. — 338 с. — Режим доступа: https://e.lanbook.com/book/111049

3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях /

В. Ф. Шаньгин. – М. : ДМК Пресс, 2012. – 512 с. – [Электронный ресурс]. – Режим доступа: https://e.lanbook.com/book/3032

4. Методологические основы построения защищенных автоматизированных систем : учебное пособие / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежская государственная лесотехническая академия, 2013. - 258 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-89448-981-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255851

6.2. Дополнительная литература

5. Организация безопасной работы информационных систем : учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=277794

6. Сабанов, А.Г. Защита персональных данных в организациях здравоохранения [Электронный ресурс] : учебное пособие / А.Г. Сабанов, В.Д. Зыков, Р.В. Мещеряков. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 206 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5194 — Загл. с экрана.

7. Афанасьев А.А., Веденьев Л.Т., Воронцов А.А. и др.; под ред. Шелупанова А.А., Груздева С.Л., Нехаева Ю.С. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов/М.: Горячая линия-Телеком, 2012.- 550 с.: ил.- [Электронный ресурс] -URL: https://e.lanbook.com/book/5114

8. Васильев В.И. Интеллектуальные системы защиты информации: учеб. пособие/М.: Машиностроение, 2013.- 172 с.- [Электронный ресурс] -URL: https://e.lanbook.com/book/5792

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

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

10. Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: http://protect.gost.ru

11. Правовая справочная система «Гарант» [электронный ресурс]: -режим доступа: 1. Ауд.94 ПК АлтГТУ. (Платформа F1 Гарант); 2. http://www.garant.ru

12. 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.

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	Windows
2	Microsoft Office
3	Chrome
4	Kaspersky Endpoint Security для бизнеса Расширенный
5	Wireshark
6	LibreOffice
7	Антивирус Kaspersky

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru)
2	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 занятий лекционного типа
учебные аудитории для проведения групповых и индивидуальных консультаций
учебные аудитории для проведения текущего контроля и промежуточной аттестации

Наименование специальных помещений и помещений для самостоятельной работы
помещения для самостоятельной работы
лаборатории в области программно-аппаратных средств обеспечения информационной безопасности

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».