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.31 «Программно-аппаратные средства защиты информации»

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-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.3	Способен применять программно-аппаратные средства защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Аппаратные средства вычислительной техники, Защита информации от утечки по техническим каналам, Методы и средства криптографической защиты информации, Моделирование и анализ процессов, систем и объектов защиты информации, Организационное и правовое обеспечение информационной безопасности, Сети и системы передачи информации, Техническая защита информации
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации, Организация и технологии защиты данных в информационных системах, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Преддипломная практика, 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: 5 / 180

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	32	64	0	84	103

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

Форма обучения: очная

Семестр: 5

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	
16	32	0	24	52

Лекционные занятия (16ч.)

1. Введение {лекция с разбором конкретных ситуаций} (2ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Программы ВО в области информационной безопасности. Основная образовательная программа по направлению подготовки бакалавров «Информационная безопасность». Программа дисциплины «Программно-аппаратные средства защиты информации».

2. Общие сведения о сетях и системах передачи информации. {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Характеристики сетей. Операционные возможности сетей. Классификация информационно-вычислительных сетей (по назначению, по территориальному принципу, по сетевым операционным системам, по типу среды передачи данных, по функциональному назначению, по скорости передачи данных, по типу сетевой топологии, по необходимости поддержания постоянного соединения).

3. Принципы программно-аппаратной защиты информации от несанкционированного доступа {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Основные подходы к ПА защите данных от несанкционированного доступа (НСД). Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлам. Идентификация, аутентификация и авторизация. Аутентификация субъекта. Контроль и управление доступом средствами операционной системы.

4. Назначение и задачи программно-аппаратной защиты информации в сфере обеспечения информационной безопасности {лекция-пресс-конференция} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Цели и задачи программно-аппаратной защиты информации. Место программно-аппаратной (ПА) защиты информации в системе защиты информации на объектах информатизации. Классификация методов и средств ПА защиты информации.

5. Программно-аппаратные средства шифрования {лекция с разбором конкретных ситуаций} (2ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Аппаратные и программно-аппаратные средства криптозащиты данных. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, принцип главного ключа.

Лабораторные работы (32ч.)

1. Рассмотрение технологии VPN: определение и разновидности VPN-технологий. Построение VPN-сети; требования к VPN-технологиям {работа в

малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
2. Установка ПАСЗИ, идентификация, аутентификация и авторизация субъекта к объектам доступа
с помощью ПАСЗИ {работа в малых группах} (6ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
3. Изучение сетевых сканеров для анализа защищенности информационной системы и особенностей функционирования объекта защиты {работа в малых группах} (6ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
4. Установка и настройка сетевых сканеров и анализаторов {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
5. Создание изолированной программной среды с помощью ПАСЗИ {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
6. Программно-аппаратные методы защиты информации в условиях перехода к Индустрии 4.0. Угрозы безопасности информации и пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
7. Аппаратные и программно-аппаратные средства криптозащиты данных. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, принцип главного ключа {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

Самостоятельная работа (24ч.)
1. Подготовка к текущим занятиям, к контрольной работе, самостоятельное изучение материала. {с элементами электронного обучения и дистанционных образовательных технологий} (18ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
2. Подготовка к зачету. {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

Семестр: 6
Объем дисциплины в семестре з.е. /час: 3 / 108
Форма промежуточной аттестации: Экзамен

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
16	32	0	60	52

Лекционные занятия (16ч.)
1. Введение {лекция с разбором конкретных ситуаций} (2ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Программы ВО в области информационной безопасности. Основная образовательная программа по направлению подготовки бакалавров «Информационная безопасность». Программа

дисциплины «Программно-аппаратные средства защиты информации»

2. Классификация способов несанкционированного доступа и жизненный цикл атак {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI. Межсетевые экраны: понятие периметра сети; определение и функции межсетевого экранирования; фильтрация трафика; трансляция адресов; примеры межсетевых экранов. Обзор протоколов.

3. Технология VPN: определение и разновидности VPN-технологий {лекция с разбором конкретных ситуаций} (2ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Специфика построения VPN-сети; требования к VPN-технологиям; реализация VPN-технологий. Сканеры безопасности: классификация уязвимостей; применение сканеров безопасности; классификация сканеров безопасности.

4. Программно-аппаратная защита от разрушающих программных воздействий {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Компьютерные вирусы как особый класс разрушающих программных воздействий.

5. Создание изолированной программной среды {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14] Понятие изолированной программной среды. Формирование и поддержка изолированной программной среды

Лабораторные работы (32ч.)

1. Установка, настройка и обслуживание программно-аппаратного средства защиты информации Secret Net. Установка, настройка и обслуживание программно-аппаратного комплекса «Соболь» {работа в малых группах} (6ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

2. Установка, настройка и обслуживание программно-аппаратного комплекса МДЗ «Аккорд» {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

3. Установка, настройка и обслуживание программно-аппаратного комплекса «Криптон» {работа в малых группах} (2ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

4. Выявление сетевых атак путем анализатора трафика {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

5. Развертывание защищенного рабочего места клиента VPN-сети на основе ПО ViPNet {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

6. Создание и модификация защищенной виртуальной сети ViPNet {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

7. Изучение Антивирусных программы. Вирусы, их классификация. Основные угрозы. Способы противодействия вирусам в условиях

современного развития информационных технологий. Антивирусные программы, принцип их действия {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
8. Продемонстрировать работу программных и программно-аппаратных средств защиты данных (по выбору) {творческое задание} (4ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

Самостоятельная работа (60ч.)
1. Подготовка к текущим занятиям, к контрольной работе, самостоятельное изучение материала. {с элементами электронного обучения и дистанционных образовательных технологий} (24ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]
2. Подготовка к экзамену {с элементами электронного обучения и дистанционных образовательных технологий} (36ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13,14]

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

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

1. Грозов В.И. Учебно-методическое пособие «Программно-аппаратная защита информации»/Грозов В.И., Алт. гос. техн. ун-т им. И. И. Ползунова.-Барнаул: Изд-во АлтГТУ, 2012. Режим доступа: tp://elib.altstu.ru/eum/download/vsib/grozov-pazi.pdf

6. Перечень учебной литературы

6.1. Основная литература

2. Учебно-методическое пособие по дисциплине Методы и средства защиты компьютерной информации / составители А. Г. Симонян. — Москва : Московский технический университет связи и информатики, 2016. — 32 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/61498.html (дата обращения: 21.05.2023)

3. Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства : практикум / Д. В. Фомин. — Саратов : Вузовское образование, 2021. — 218 с. — ISBN 978-5-4487-0795-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/110329.html (дата обращения: 21.05.2023). — Режим доступа: для авторизир. пользователей. - DOI:

https://doi.org/10.23682/110329
4. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – 2-е изд. – Саратов : Профобразование, 2019. – 543 c. – ISBN 978-5-4488-0074-0. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/87992.html (дата обращения: 21.05.2023).

6.2. Дополнительная литература

5. Долозов, Н. Л. Программные средства защиты информации : конспект лекций / Н. Л. Долозов, Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2015. – 63 c. – ISBN 978-5-7782-2753-8. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/91683.html (дата обращения: 21.05.2023).
6. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. – Москва : Издательский Дом МИСиС, 2018. – 21 c. – ISBN 978-5-906953-22-3. – Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. – URL: https://www.iprbookshop.ru/98199.html (дата обращения: 15.06.2021). – Режим доступа: для авторизир. Пользователей
7. Акимова, О. Ю. Хранение и защита компьютерной информации : лабораторный практикум / О. Ю. Акимова. – Москва : Издательский Дом МИСиС, 2020. – 76 c. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/106895.html (дата обращения: 21.05.2023).
8. Гуц, А. К. Теория игр и защита компьютерных систем : учебное пособие / А. К. Гуц, Т. В. Вахний. – Омск : Омский государственный университет им. Ф.М. Достоевского, 2013. – 160 c. – ISBN 978-5-7779-1655-6. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/24947.html (дата обращения: 21.05.2023).
9. Проскурин В.Г. Защита программ и данных : учеб. пособие для студ. учреждений высш. проф. образования / В.Г.Проскурин. – 2-е изд., стер. – М. : Издательский центр «Академия», 2012. – 208 с.:10 экз.
10. Спицын, В. Г. Информационная безопасность вычислительной техники: учебное пособие / В. Г. Спицын. - Томск: Эль Контент, 2011. - 148 с. - [Электронный ресурс]. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=208694&sr=1.

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

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

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

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

14. Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: http://protect.gost.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	Linux
2	Windows
3	ViPNet client (демо-версия)
3	Антивирус Kaspersky
4	ViPNet Coordinator (демо-версия)
5	ViPNet CSP

№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/)
2	Научные ресурсы в открытом доступе (http://www.prometeus.nsc.ru/sciguide/page0607.ssi)
3	Электронная библиотека Институт инженеров по электротехнике и электронике (IEEE) и его партнеров в сфере издательской деятельности. Коллекция включает в себя более 3 миллионов полнотекстовых документов с

№пп	Используемые профессиональные базы данных и информационные справочные системы
	самыми высокими индексами цитирования в мире. Часть материалов находится в свободном доступе. Для поиска таких документов нужно выбрать расширенный поиск «Advanced Search», ввести в поисковое окно ключевые слова и поставить фильтр «Open Access» (https://ieeexplore.ieee.org/Xplore/home.jsp)
4	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
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».