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.Б.21 «Программно-аппаратные средства защиты информации»**

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

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

Статус дисциплины: **обязательная часть (базовая)**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	старший преподаватель	Л.Д. Алфёрова
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
ОПК-4	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	- значение информационно - коммуникационных технологий в развитии современного общества, в том числе применительно к программно-аппаратным средствам защиты информациис применением информационных технологий	-применять программные и аппаратные средства при решении профессиональных задач по обработке информации, в том числе применительно к программно-аппаратным средствам защиты информации	
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	-основные угрозы безопасности информации; - методы анализа объекта информатизации на предмет выявления угроз безопасности и имеющихся уязвимостей	- определять элементы информационной инфраструктуры и информационные ресурсы организации, подлежащие защите; - разрабатывать модели угроз и нарушителей информационной безопасности ИС - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите	- навыками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; - методами выявления угроз и уязвимостей информационной безопасности информационных систем
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	разновидности, характеристики, принципы работы и правила эксплуатации программно-аппаратных средств защиты информации	- выполнять работы по установке, настройке и обслуживанию программных средств защиты информации	навыками установки, настройки и обслуживания средств защиты информации
ПК-6	способностью принимать участие в организации и проведении контрольных	- методы и средства контроля эффективности	- проверять работоспособность и эффективность	навыками проведения проверок работоспособности

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
	проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	различных видов средств защиты информации	применения средств защиты информации	средств защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Криптографические методы защиты информации, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, 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.	Информационная безопасность автоматизированных систем, Комплексное обеспечение защиты информации объекта информатизации, Организация системы обеспечения информационной безопасности, Технологии защиты информации в глобальных сетях, Технологическая практика, Эксплуатационная 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: 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	34	34	0	76	73

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

Форма обучения: очная
Семестр: 6

Лекционные занятия (34ч.)

1. Введение(2ч.)[2,3,4,7,13] Программы ВО в области информационной безопасности. Основная образовательная программа по направлению подготовки бакалавров «Информационная безопасность». Программа дисциплины «Программно-аппаратные средства защиты информации»

2. Принципы программно-аппаратной защиты информации от несанкционированного доступа(6ч.)[2,3,4,7,13] 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

3. Назначение и задачи программно-аппаратной защиты информации в сфере обеспечения информационной безопасности(4ч.)[2,3,4,7,13] 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

4. Программно-аппаратные средства шифрования(4ч.)[2,3,4,7,13] Аппаратные и программно-аппаратные средства криптозащиты данных. Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, принцип главного ключа. Криптон. Архитектура платы и организация интерфейса

5. Классификация способов несанкционированного доступа и жизненный цикл атак(6ч.)[2,3,4,7,13] Способы противодействия не-санкционированному межсетевому доступу. Функции меж-сетевого 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.

6. Технология VPN: определение и разновидности VPN-технологий(4ч.)[2,3,4,7,9,13] Специфика построения VPN-сети; требования к VPN-технологиям; реализация VPN-технологий. Сканеры безопасности: классификация уязвимостей; применение ска-неров безопасности; классификация сканеров безопасности

7. Программно-аппаратная защита от разрушающих программных воздействий(4ч.)[2,3,4,5,7,9,13] Компьютерные вирусы как особый класс

разрушающих программных воздействий

8. Создание изолированной программной среды(4ч.)[2,7,13] Понятие изолированной программной среды. Формирование и поддержка изолированной программной среды

Лабораторные работы (34ч.)

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

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

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

4. Выявление сетевых атак путем анализатора трафика {работа в малых группах} (4ч.)[1,2,3,4,7,9,13]

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

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

7. Применение сетевых сканеров для анализа защищенности информационной системы {работа в малых группах} (6ч.)[1,4,7,13]

8. Антивирусные программы.

Создание изолированной программной среды {работа в малых группах} (6ч.)[1,2,3,4,6,7,9,13]

Самостоятельная работа (76ч.)

1. Подготовка к текущим занятиям, к контрольной работе, к экзамену, самостоятельное изучение материала(31ч.)[1,2,3,4,5,6,7,9,10,11,12,13]

2. Подготовка к экзамену(45ч.)[1,2,3,4,5,6,7,8,9,10,11,12,13]

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. 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. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 552 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5114 — Загл. с экрана

3. Проскурин, В.Г. Защита в операционных системах [Электронный ресурс] : учебное пособие / В.Г. Проскурин. — Электрон. дан. — Москва : Горячая линия-Телеком, 2016. — 192 с. — Режим доступа: https://e.lanbook.com/book/111091

4. 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

6.2. Дополнительная литература

5. Благодаров, А.В. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем [Электронный ресурс] : монография / А.В. Благодаров [и др.]. — Электрон. дан. — Москва : Горячая линия-Телеком, 2015. — 116 с. — Режим доступа: https://e.lanbook.com/book/111019

6. Мартемьянов, Ю.Ф. Операционные системы. Концепции построения и обес-печения безопасности [Электронный ресурс] : учебное пособие / Ю.Ф. Мартемьянов, Яковлев Ал.В., Яковлев Ан.В. — Электрон. дан. — М. : Горячая линия-Телеком, 2011. — 332 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5176 — Загл. с экрана.

7. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. Учреждений высш.проф.образования/В.В.Платонов. — М. : Издательский центр «Академия», 2006. — 336 с.:15 экз.

8. 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.

9. 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

10. Правовая справочная система «Гарант» [электронный ресурс] http://www.garant.ru

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

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

13. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: http:// www.fstec.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	Linux
2	Windows
3	Windows Server
4	ViPNet client (демо-версия)
5	ViPNet Coordinator (демо-версия)
6	Гарант
7	Acrobat Reader
8	Kaspersky Endpoint Security для бизнеса Расширенный
9	LibreOffice
10	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

№пп	Используемые профессиональные базы данных и информационные справочные системы
	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 занятий семинарского типа
учебные аудитории для проведения групповых и индивидуальных консультаций
учебные аудитории для проведения текущего контроля и промежуточной аттестации
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».