

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.16 «Защита информации»**

Код и наименование направления подготовки (специальности): **09.03.01**

Информатика и вычислительная техника

Направленность (профиль, специализация): **Программно-техническое обеспечение автоматизированных систем**

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

Форма обучения: **заочная, очная**

Статус	Должность	И.О. Фамилия
Разработал	доцент	А.В. Санников
	доцент	А.В. Санников
	доцент	А.В. Санников
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	Л.И. Сучкова

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
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности	правовые основы обеспечения политики безопасности	использовать нормативно-правовые знания в различных сферах жизнедеятельности, в том числе в сфере информационных технологий, при решении задачи защиты информации	навыками поиска нормативно-правовой информации, необходимой для гражданской и профессиональной деятельности, в том числе при организации защиты информации
ОПК-1	способностью устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем	- методы инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем, в том числе предназначенного для защиты информации; - терминологию, состав, структуру и функции основных аппаратных и программных средств информационных и автоматизированных систем, в том числе предназначенных для защиты информации	устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем, в том числе предназначенное для защиты информации;	навыками инсталляции программного обеспечения, в том числе предназначенного для защиты информации
ОПК-5	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	способы и технологии решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	обеспечить информационную безопасность при решении профессиональных задач с применением информационно-коммуникационных технологий	навыками решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий, в том числе с соблюдением требований информационной безопасности
ПК-1	способностью разрабатывать модели	стандарты и	контролировать	

Код компетенции из УП и этап её формирования	Содержание компетенции	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
	компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек - электронно-вычислительная машина"	нормативные документы, регламентирующие проектно-конструкторскую деятельность, в том числе устанавливающие требования по информационной безопасности	соответствие проектов и технической документации нормативным документам, в том числе устанавливающим требованиям по информационной безопасности	

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Информатика, Операционные системы, Программирование, ЭВМ и периферийные устройства
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Администрирование глобальных вычислительных сетей, Системы и сети связи, Техническое обеспечение систем обработки и защиты информации

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 обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
заочная	6	10	0	92	19
очная	17	17	0	74	40

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

Форма обучения: заочная

Семестр: 8

Лекционные занятия (6ч.)

1. Понятие защиты информации. Объекты защиты информации. Угрозы защищаемой информации. {лекция с разбором конкретных ситуаций} (2ч.)[1,2,5] Понятие «защита информации». Цели и задачи защиты информации. Основные свойства информации с точки зрения её безопасности. Понятие и состав защищаемой информации. Понятие объекта защиты информации. Носители защищаемой информации как конечные объекты защиты. Средства и системы обработки информации, средства обеспечения объекта информатизации, помещения объектов информатизации как объекты защиты. Использование основ правовых знаний в различных сферах деятельности при решении задачи защиты информации. Понятие угрозы и её взаимосвязь с уязвимостью и рисками. Общая классификация угроз безопасности информации. Технические каналы утечки информации. Анализ угроз защищаемой информации. Виды защиты информации и сферы их действия. Общая классификация средств защиты информации. Определение требований информационной безопасности при разработке моделей компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек - электронно-вычислительная машина"

2. Технологии безопасности компьютерных систем.(2ч.)[2,4,5] Угрозы безопасности информации в компьютерных системах. Защита информации от случайных угроз. Защита информации от несанкционированного доступа. Модели управления доступом к объектам компьютерных систем. Классификация компьютерных вирусов, механизмы защиты от них. Защита информации от перехвата по техническим каналам утечки информации. Защита от несанкционированного доступа и копирования информации. Состав программного и аппаратного обеспечения, предназначенного для защиты информации. Особенности инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем, предназначенного для защиты информации.

3. Стандарты и нормативные акты в области информационной безопасности.(2ч.)[1,2,4,6,7] Состав стандартов и нормативных документов по информационной безопасности в компьютерных системах и автоматизированных системах. Документы в области защиты от вредоносного кода. Руководящие документы в области защиты автоматизированных систем. Специальные требования и рекомендации по технической защите конфиденциальной информации. Документы ФСТЭК России и ФСБ России. Состав нормативных актов по видам защищаемой информации. Решение стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Лабораторные работы (10ч.)

- 1. Антивирусные программы.(2ч.)[2,4]**
- 2. Организация VPN.(2ч.)[2,4]**
- 2. Межсетевые экраны.(2ч.)[2,4]**
- 3. Средства шифрования.(2ч.)[2,4]**
- 4. Электронная подпись.(2ч.)[2,4]**

Самостоятельная работа (92ч.)

- 1. Подготовка к выполнению и сдаче лабораторных работ.(20ч.)[1,2,3,4,5]**
- 2. Самостоятельное изучение тем "Криптографические методы защиты информации", "Комплексная система защиты информации на предприятии".(32ч.)[1,2,3,4,5]**
- 3. Выполнение контрольной работы.(20ч.)[1,2,3,4,5]**
- 4. Подготовка к экзамену.(20ч.)[1,2,4,5,6]**

Форма обучения: очная

Семестр: 5

Лекционные занятия (17ч.)

- 1. Понятие, сущность, цели и концептуальные основы защиты информации.(2ч.)[1,5]** Общий контекст защиты информации. Понятие «защита информации». Сущность и содержание защиты информации. Цели и задачи защиты информации. Концептуальная модель защиты информации. Основные свойства информации с точки зрения её безопасности. Понятие и состав защищаемой информации. Принципы отнесения информации к защищаемой. Правовое обеспечение защиты информации. Использование основ правовых знаний в различных сферах деятельности при решении задачи защиты информации
- 2. Объекты защиты информации.(2ч.)[1,2]** Понятие объекта защиты информации. Носители защищаемой информации как конечные объекты защиты. Средства и системы обработки информации как объекты защиты. Средства обеспечения объекта информатизации. Помещения объектов информатизации как объекты защиты. Защищаемые информационные процессы. Носители защищаемой информации.
- 3. Угрозы защищаемой информации. Виды, методы и средства защиты информации. {лекция с разбором конкретных ситуаций} (2ч.)[1,3,4]** Понятие угрозы и её взаимосвязь с уязвимостью и рисками. Общая классификация угроз безопасности информации. Технические каналы утечки информации. Цели и задачи оценки угроз защищаемой информации. Виды защиты информации и

сферы их действия. Общие способы защиты информации. Общая классификация средств защиты информации. Характеристика способов и средств по видам защиты информации.

4. Технологии безопасности компьютерных систем.(4ч.)[2,4,5] Угрозы безопасности информации в компьютерных системах. Защита информации от случайных угроз. Защита информации от несанкционированного доступа. Модели управления доступом к объектам компьютерных систем. Классификация компьютерных вирусов, механизмы защиты от них. Защита информации от перехвата по техническим каналам утечки информации. Защита от несанкционированного доступа и копирования информации. Состав программного и аппаратного обеспечения, предназначенного для защиты информации. Особенности инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем, предназначенного для защиты информации.

5. Криптографические методы защиты информации.(2ч.)[2,4,5] Классификация методов криптографического преобразования информации. Цели криптографии. Основные понятия. Алгоритмы шифрования с симметричным ключом. Алгоритмы шифрования с открытым ключом. Электронная подпись. Функции хеширования. Протоколы аутентификации.

6. Стандарты и нормативные акты в области информационной безопасности.(3ч.)[2,4,7] Состав стандартов и нормативных документов по информационной безопасности в компьютерных системах и автоматизированных системах. Документы в области защиты от вредоносного кода. Руководящие документы в области защиты автоматизированных систем. Специальные требования и рекомендации по технической защите конфиденциальной информации. Документы ФСТЭК России и ФСБ России. Состав нормативных актов по видам защищаемой информации. Решение стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

7. Комплексная система защиты информации на предприятии.(2ч.)[1,4,6,7] Понятие и общая структура системы защиты информации. Общеметодологические требования и принципы построения систем защиты. Понятие и общая структура комплексной системы защиты информации на предприятии. Компоненты комплексной системы защиты информации на предприятии их назначение и состав. Нормативно-методические документы и стандарты для реализации различных компонентов. Определение требований информационной безопасности при разработке моделей компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек - электронно-вычислительная машина".

Лабораторные работы (17ч.)

1. Антивирусные программы.(2ч.)[2,4]
2. Организация VPN.(2ч.)[2,4]
3. Средства шифрования.(2ч.)[2,4]
4. Электронная подпись.(2ч.)[2,4]
5. Межсетевые экраны.(2ч.)[2,4]
6. Системы защиты информации от несанкционированного доступа.(3ч.)[2,4]
7. Системы обнаружения вторжений.(2ч.)[2,5]
8. Программные продукты для анализа рисков информационной безопасности.(2ч.)[4,5]

Самостоятельная работа (74ч.)

1. Подготовка к выполнению и сдаче лабораторных работ.(20ч.)[1,2,3,4,5,6]
2. Изучение профильной литературы(34ч.)[1,2,3,4,5,6]
3. Подготовка к экзамену.(20ч.)[1,2,3,4,5,6]

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. Загинайлов Ю. Н. Основы информационной безопасности: учебное пособие / Ю. Н. Загинайлов ; Алт. гос. техн. ун-т им. И. И. Ползунова. – Барнаул : АлтГТУ, 2016. – 172с. [электронный ресурс]:- режим доступа: <http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-58622357c10ad.pdf>

6. Перечень учебной литературы

6.1. Основная литература

2. Шаньгин, Владимир Федорович. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - Электрон.изд. - Электрон. текстовые дан. - Саратов : Профобразование, 2017. - 544 с. Режим доступа: <http://www.iprbookshop.ru/63592.html>
3. Торокин, А.А. Инженерно-техническая защита информации : учеб. пособие для вузов по специальностям в обл. информ. безопасности / А. А. Торокин. - Москва : Гелиос АРВ, 2005. - 958 с. : ил. - 30 экз.
4. Завгородний, В.И. Комплексная защита информации в компьютерных системах : учеб. пособие для вузов / В. И. Завгородний. - Москва : Логос, 2001. - 264 с. - 21 экз.
5. Мельников В.П. Информационная безопасность и защита информации : [учеб. пособие для вузов по специальности 230201 "Информ. системы и

технологии"] / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 4-е изд., стер. - Москва : Академия, 2009. - 330, [1] с. : ил. - 20 экз.

6.2. Дополнительная литература

6. Васильев В.И. Интеллектуальные системы защиты информации [Электронный ресурс] : [учебное пособие для студентов высших учебных заведений, обучающихся по специализациям специальности «Комплексное обеспечение информационной безопасности автоматизированных систем»] / В. И. Васильев. - Изд. 2-е, испр. - Электрон. текстовые дан. - Москва : Машиностроение, 2013. - 172 с. : ил. - (Для вузов). - Библиогр.: с. 161-171. - ISBN 978-5-94275-667-3 : Б. ц. Режим доступа: <https://e.lanbook.com/book/5792>

7. Загинайлов Ю. Н. Правовое обеспечение компьютерной безопасности : учебно-методическое пособие.-2-е изд., испр. и доп. / Ю. Н. Загинайлов; Алт.гос.техн.ун-т им.И.И.Ползунова.- Баранаул: Изд-во АлтГТУ.- 2018 – 116 с. [электронный ресурс]:- режим доступа: <http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-5a6ae9603068e.pdf>

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

8. Официальный сайт федеральной службы по техническому и экспортному контролю [электронный ресурс]:- режим доступа: <https://fstec.ru>

9. Официальный сайт интернет-журнала "Информационная безопасность" [электронный ресурс]:- режим доступа: <http://www.itsec.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	Kaspersky Endpoint Security для бизнеса Расширенный
2	RStudio Desktop Open Source Edition
3	Wireshark
4	Microsoft Office
5	ViPNet CSP
6	ViPNet client (демо-версия)
7	ViPNet Coordinator (демо-версия)
8	Windows
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 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
помещения для самостоятельной работы
лаборатории

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».