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.ДВ.5.2 «Техническое обеспечение систем организации и защиты информации»**

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

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

Статус дисциплины: **дисциплины (модули) по выбору**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	заведующий кафедрой	А.Г. Якунин
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-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, правила настройки и обслуживания технических средств защиты информации, в том числе на базе программно–аппаратных комплексов	выполнять работы по установке, настройке и обслуживанию технических средств защиты информации , включая системы контроля и управления доступом	навыками установки, настройки и обслуживания средств защиты информации, в том числе систем контроля и управления доступом
ПК-6	способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	методы и средства контроля эффективности различных видов средств защиты информации, в том числе средств с применением программно–аппаратных комплексов	проверять работоспособность и эффективность применения средств защиты информации, включая средства на основе программно-аппаратных комплексов	навыками проведения проверок работоспособности средств защиты информации, в том числе средств с применением программно-аппаратных комплексов

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Аппаратные средства вычислительной техники, Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения, Микроконтроллерные системы в информационной безопасности, Нормативные акты и стандарты по информационной безопасности, Физика, Электроника и схемотехника, Электротехника
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Выпускная квалификационная работа, Комплексное обеспечение защиты информации объекта информатизации, Преддипломная практика, Проектно-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: 4 / 144
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	17	17	17	93	65

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 (17ч.)

1. Введение. Система охранных мер по защите информации. {беседа} (3ч.)[3,4,5] виды технического обеспечения безопасности как одна из мер защиты информации. Общие правила выполнения работ по установке, настройке технических средств защиты информации. Общий порядок участия в организации и проведении контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.

2. Система мер (режимов) по обеспечению сохранности материальных ценностей {беседа} (3ч.)[3,4,5] Основные виды мер по обеспечению сохранности материальных ценностей. Защита информационных ресурсов от несанкционированного доступа, утечек и разрушения (уничтожения) информации. Разработка технических заданий на оснащение отделов, лабораторий системами технической защиты информации. Разработка, настройка и наладка программно-аппаратных комплексов технических средств защиты информации, в том числе с использованием современных инструментальных средств и технологий программирования.

3. Системы физической защиты (безопасности) материальных объектов {беседа} (2ч.)[3,4,5] Основные виды систем физической защиты и их краткая характеристика. Связь между системами физической и технической защиты. Системы физической защиты на основе программно-аппаратных комплексов.

4. Системы охранно-пожарной сигнализации {лекция с разбором конкретных ситуаций} (3ч.)[3,4,5] Основные виды систем охранно-пожарной сигнализации,

их состав, структурная схема и принцип работы. Интерфейсы, используемые в системах охраны.

5. Системы контроля и управления доступом {лекция с разбором конкретных ситуаций} (3ч.)[3,4,5,6,8,14] Основные виды систем контроля и управления доступом (СКУД), их состав, структурная схема и принцип работы. Параметры и характеристики систем в целом и их основных компонентов. Примеры серийно выпускаемых СКУД.

6. Системы видеонаблюдения {лекция с разбором конкретных ситуаций} (3ч.)[3,4,5] Основные виды систем видеонаблюдения, их разновидности, состав, структурная схема и принцип работы. Параметры и характеристики систем в целом и их основных компонентов.

Практические занятия (17ч.)

1. Разработка модели угроз и оценка уязвимостей объекта информатизации с позиции развертывания на нем средств технической защиты {имитация} (2ч.)[3,4,5,6] В соответствии с предоставленным описанием предприятия определяются:

1. Источники угроз (потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности)
2. Вызываемые источниками конкретные угрозы с разделением на потенциальные и реально существующие
3. Уязвимости, обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.
4. Возможные последствия реализации угроз при взаимодействии источника угрозы через имеющиеся уязвимости и возможность минимизации или исключения таких последствий за счет развертывания средств технической защиты информации

2. Проведение аудита на соответствие используемых средств технической защиты по стандарту СТО БР ИББС 1.2 – 2014 {имитация} (2ч.)[3,10,12,13] Рассмотрение методики оценки соответствия СТО БР ИББС-1.2-2014 частных и групповых показателей, касающихся технической защиты и порядок выставления восьми оценок на соответствие степени выполнения этих требований и итоговой R-оценки

3. Составление паспорта предприятия для развертывания на нем системы охранных мер с применением средств технической защиты {работа в малых группах} (2ч.)[6,7,12] В зависимости о проведенного на предыдущих занятиях анализа виртуального предприятия выбирается набор технических средств безопасности, виды, типы и способы охраны, необходимые для защиты объекта с учетом количества сил и средств физической охраны, используемых на объекте.

4. Оценка риска информационной безопасности, обусловленного отсутствием средств технической защиты {деловая игра} (2ч.)[3,5,6] На занятии

рассматриваются методы определения ценности информационных активов, вероятности реализации реализации угрозы по отношению к информационному активу как при наличии, так и отсутствии средств технической защиты с применением качественных, трехуровневых (низкий, средний, высокий уровень) и числовых шкал.

На основании определенных ценности информационного актива, вероятности реализации угрозы, возможности реализации угрозы находится оценка об уровне риска по пятибалльной и десятибалльной шкале. При определении уровня риска используются эталонные таблицы, связывающие различные комбинации показателей (ценность, вероятность, возможность) с величиной риска. В процессе занятия рассматриваются варианты расчета риска не только по методикам ФСТЭК, но и по альтернативным методикам

5. Расчет оценки эффективности применения мер по организации системы технической защиты объекта информатизации {творческое задание} (2ч.)[3,5,6,7] Рассматривается методика расчета эффективности принятия мер по развертыванию средств технической защиты, и делается расчет такой эффективности по полученным на предыдущем занятии данным

6. Проведение аттестации АС ЗП {имитация} (2ч.)[7,10] Рассматривается порядок проведения и документального оформления следующих видов работ:

- инженерный анализ с целью выявления потенциальных каналов утечки информации;
- проверка достаточности и полнота организационно-распорядительной документации по защите информации;
- инструментальное обследование объекта информатизации с использованием специальной контрольно-измерительной аппаратуры и оценка защищенности обрабатываемой на объекте информатизации защищаемой информации от утечки по техническим каналам;
- оценка соответствия объекта информатизации требованиям безопасности по защите от НСД к информации

7. Разработка технического задания на оснащение объекта информатизации средствами и системами технической защиты информации {творческое задание} (2ч.)[4,6] Составляется техническое задание на выполнение проектных работ по оснащению объекта информатизации средствами и системами технической защиты информации

8. Разработка проекта системы технической защиты объекта информатизации с учетом имеющегося технического задания и ранее выполненного для него анализа угроз и уязвимостей {разработка проекта} (3ч.)[3,6,8] Проект составляется по техническому заданию, разработанному на предыдущем занятии. Последний час занятия отводится на написание контрольной работы

Лабораторные работы (17ч.)

1. Установка и настройка адресного звукового извещателя "С2000-СТ"

{тренинг} (4ч.)[1,3] Разработка технического задания на оснащение адресным звуковым излучателем отделов, лабораторий, разработка, настройка и наладка адресного звукового излучателя, при использовании современных инструментальных средств и технологий программирования

2. Система аналогового видеонаблюдения {творческое задание} (5ч.)[2] Разработка технического задания на оснащение отделов, лабораторий системами аналогового видеонаблюдения, разработка, настройка и наладка программно-аппаратных комплексов аналогового видеонаблюдения, при использовании современных инструментальных средств и технологий программирования

3. Система цифрового видеонаблюдения {работа в малых группах} (4ч.)[2] Разработка технического задания на оснащение отделов, лабораторий системами цифрового видеонаблюдения, разработка, настройка и наладка программно-аппаратных комплексов цифрового видеонаблюдения, при использовании современных инструментальных средств и технологий программирования

4. Система гибридного видеонаблюдения {творческое задание} (4ч.)[2] Разработка технического задания на оснащение отделов, лабораторий системами гибридного видеонаблюдения, разработка, настройка и наладка программно-аппаратных комплексов гибридного видеонаблюдения, при использовании современных инструментальных средств и технологий программирования

Самостоятельная работа (93ч.)

1. Самостоятельное изучение и закрепление теоретического материала {тренинг} (33ч.)[3,4,5,6,7,8,9,10,11,12,13,14,15] Самостоятельная работа студентов (СРС) заключается в изучении и закреплении теоретического материала, представленного в лекциях, дополнительных источниках (как из списка рекомендованной литературы, так и самостоятельно найденных в web - ресурсах).

2. Подготовка к текущим занятиям, текущему контролю(50ч.)[1,2,3,4,6,7,10,12] Выполнение отчетов по лабораторным работам, изучение документации по используемому в лабораторных работах оборудованию и нормативных и методических документов при подготовке к практическим занятиям

3. Подготовка к промежуточной аттестации {тренинг} (10ч.)[3,4,5] Подготовка к зачету

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. Кемпф В.А. Техническая защита информации. Методические указания к лабораторным работам: учеб. пособие /Кемпф В.А., Алт. гос. техн. ун-т им. И. И. Ползунова.-Барнаул: Изд-во АлтГТУ, 2014. Прямая ссылка: http://elib.altstu.ru/eum/download/vsib/Kempf-tzi.pdf

2. Шарлаев Е.В. Системы видеонаблюдения. Лабораторный практикум/ /А.А. Погудин, Е.В. Шарлаев, Алт. гос. техн. ун-т им. И. И. Ползунова.-Барнаул: Изд-во АлтГТУ, 2017.-52 с.- Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/PogudinSharlaev_SystVideonablLP_ump.pdf

6. Перечень учебной литературы

6.1. Основная литература

3. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс] : учебник / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2018. — 442 с. — Режим доступа: https://e.lanbook.com/book/111057. — Загл. с экрана

4. Сердюк В. А. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Национальный исследовательский университет – Высшая школа экономики. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285 (28.04.2019)

5. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Е.Б. Белов [и др.]. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 558 с. — Режим доступа: https://e.lanbook.com/book/111016. — Загл. с экрана

6.2. Дополнительная литература

6. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193 - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93351(10.05.2019).

7. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356 (28.04.2019)

8. Титов, А.А. Инженерно-техническая защита информации : учебное пособие / А.А. Титов. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208567 (28.04.2019)

9. Иванов, А.В. Защита речевой информации от утечки по акустоэлектрическим каналам : учебное пособие / А.В. Иванов, В.А. Трушин ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2012. - 43 с. : ил.,табл., схем. - ISBN 978-5-7782-1888-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228846(28.04.2019)

10. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245 (28.04.2019)

11. 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

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

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

14. Компания PERCo — ведущий российский производитель систем и оборудования безопасности: официальный сайт [электронный ресурс]: режим доступа: https://www.perco.ru/ (01.05.2019)

15. Электронный курс национального открытого университета «Интуит» «Правовые и организационные основы технической защиты информации» [электронный ресурс]: режим доступа: https://www.intuit.ru/studies/courses/3617/859/info (01.05.2019)

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	Chrome
3	Acrobat Reader
4	Microsoft Office Visio
5	LibreOffice
6	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 занятий семинарского типа
учебные аудитории для проведения групповых и индивидуальных консультаций
учебные аудитории для проведения текущего контроля и промежуточной аттестации
помещения для самостоятельной работы
лаборатории в области технической защиты информации

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».