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.3 «Технология проведения исследования защищенности объектов и средств защиты»**

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: **часть, формируемая участниками образовательных отношений**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	доцент	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
ПК-4	Способен участвовать в исследованиях защищенности объектов и средств защиты	ПК-4.1	Демонстрирует знание методов исследования защищенности объектов и средств защиты
		ПК-4.3	Способен оформлять результаты исследований защищенности

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Иностранный язык, Информатика, Программирование
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Преддипломная 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: 6 / 216

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	42	0	68	106	126

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

Форма обучения: очная

Семестр: 6

Объем дисциплины в семестре з.е. /час: 4 / 144

Форма промежуточной аттестации: Зачет

Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
32	0	48	64	90

Лекционные занятия (32ч.)

1. Наука. Основные положения. {лекция с разбором конкретных ситуаций} (4ч.)[2,4,5,6] Определение науки. Наука и другие формы освоения действительности. Основные этапы развития науки. Учёное звание и учёная степень. Организация работы в научном коллективе. Методы и средства управления научным коллективом. Основные принципы организации и управления научным коллективом.

2. Командная работа в научном коллективе. {беседа} (4ч.)[2,4,5,6] Методы сплочения научного коллектива. Психологические аспекты взаимоотношения руководителя и подчинённого. Организация научных исследований. Структура и организация научных учреждений. Управление, планирование и координация научных исследований. Подготовка научных и научно-педагогических кадров в России. Научно-исследовательская работа студентов.

3. Методология научного познания. {беседа} (4ч.)[2,4,5,6] Методология научного познания. Факты, их обобщение и систематизация. Научное исследование и его методология. Основные уровни научного познания Определение темы. Этапы проведения научного исследования. Методы выбора и оценки тем научных исследований. Классификация и этапы научно-исследовательских работ. Актуальность и научная новизна исследования.

4. Работа с научной информацией. {беседа} (4ч.)[2,4,5,6] Виды хранения научной информации, её поиск и обработка. Документальные источники информации. Анализ документов. Поиск и накопление научной информации. Электронные формы информационных ресурсов. Обработка научной информации, её фиксация и хранение. Составление обзора по вопросам обеспечения информационной безопасности. Систематизация научно-технической литературы. Основные темы научных исследований в области ИБ. Подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов. Реферирование научной и специальной литературы, использование реферативных журналов.

5. Выбор и обоснование научной исследовательской работы. {дискуссия} (4ч.)[2,4,5,6] Обсуждение темы НИР обучающихся с целью согласования ее содержания, структуры, названия, достаточности планируемого в ней объема работ и ее соответствия объектам и видам профессиональной деятельности. Это развивает у студента способность к самоорганизации и самообразованию, способствует формированию навыков оформления и представления результатов исследований

6. Методы сбора информации при исследованиях защищенности объектов и средств защиты {беседа} (4ч.)[2,4,5,6] Пассивный сбор информации (Passive Information Gathering). Активный сбор информации (Active Information Gathering).

Сканирование портов. Эксплуатация соединений удаленного доступа. Пентесты.

7. Технология проведения исследования защищенности объектов и средств защиты {с элементами электронного обучения и дистанционных образовательных технологий} (4ч.)[2,4,5,6] Методика теоретического и экспериментального исследования. Модели исследований. Экспериментальные исследования. Планирование эксперимента. Основы теории случайных ошибок и методов оценки случайных погрешностей в измерениях. Обработка и оформление результатов научного исследования. Методы графической обработки результатов измерений.

8. Внедрение и оформление результатов исследований защищенности, их внедрение и оценка эффективности {беседа} (4ч.)[2,4,5,6] Виды полезного эффекта научных исследований. Составление и оформление отчета о научно-исследовательской работе (НИР). Научные публикации и доклады. Подготовка научного доклада. Подготовка научной статьи. Подготовка тезисов выступлений. Подготовка презентации по научной работе. Внедрение результатов исследований. Оценка экономической эффективности НИР.

Практические занятия (48ч.)

1. Изучение методов исследования защищенности объектов и средств защиты {тренинг} (4ч.)[1,3,7,8,9,10] Пассивный сбор информации (Passive Information Gatheri ng). Активный сбор информации (Active Information Gathering). Сканирование портов. Эксплуатация соединений удалённого доступа.

2. Изучение методов исследования защищенности объектов и средств защиты. Пассивный сбор информации (Passive Information Gatheri ng) {тренинг} (4ч.)[1,3,7,8,9,10] Сбор информации с помощью веб - источников: Использование Google. Сбор почтовых адресов (Email Harvesting) .

3. Изучение методов исследования защищенности объектов и средств защиты. Активный сбор информации (Active Information Gathering) {тренинг} (4ч.)[1,3,7,8,9,10] Перечисление DNS (DNS Enumeration). Взаимодействие с DNS-сервером. Автоматизация поиска. Метод прямого перебора. Метод обратного перебора (Reverse Lookup Brut e Force). Передача зоны DNS. Релевантные инструменты в Kali Linux. DNSRecon. DNSEnum. SubBrute. Перечисление SNMP (SNMP Enumeration). Дерево MIB. Сканирование SNMP. Атака усиления (амплификации) SNMP (SNMP amplification). Перечисление SMTP (SMTP Enumeration).

4. Изучение методов исследования защищенности объектов и средств защиты. Сканирование портов {тренинг} (4ч.)[1,3,7,8,9,10] Обнаружение хостов. Сканирование открытых портов и определение служб. Типы сканирования портов. Сканирование TCP. Connect-сканирование. SYN-сканирование (Стелс/stealth). Другие виды сканирования. Нулевое сканирование (NULL Scan). FIN-сканирование (FIN Scan). XMAS-сканирование (XMAS Scan). ACK-сканирование (TCP ACK Scan). Сканирование UDP. Определение версий служб. Получение отпечатков ОС (OS Fingerprinting). Методы обхода фаейрволов/IDS.

Техника таймингов. Фрагментированные пакеты. Изменение порта источника. Изменение значения MTU. Использование неверных контрольных сумм. Хосты — приманки. Сценарии Nmap Scripting Engine (NSE).

5. Изучение методов исследования защищенности объектов и средств защиты. Эксплуатация соединений удалённого доступа. {тренинг} (4ч.)[1,3,7,8,9,10] Общие особенности эксплуатации. Компрометация протокола RDP. Компрометация протокола SSH. Получение ключей хоста RSA и DSA. Поддерживаемые механизмы аутентификации. Подбор учётных данных. Компрометация протокола VNC, FTP. Определение FTP-служб. TFTP.

6. Приобретение навыков оформления результатов исследований защищенности объекта. {тренинг} (8ч.)[1,3,7,8,9,10] Теоретические методы исследования. Модели исследований. Экспериментальные исследования. Планирование эксперимента. Обработка и оформление результатов исследования. Внедрение результатов исследования и определение экономического эффекта НИР. Внедрение результатов исследования. Научные публикации и доклады. Подготовка научного доклада. Подготовка научной статьи. Подготовка тезисов выступлений. Подготовка презентации по научной работе.

7. Представление результатов исследований защищенности объектов и средств защиты. {творческое задание} (20ч.)[1,3,7,8,9,10] Доклады НИР. Представление результатов исследований защищенности объектов и средств защиты.

Самостоятельная работа (64ч.)

1. Подготовка к текущим занятиям {с элементами электронного обучения и дистанционных образовательных технологий} (56ч.)[1,2,3,4,5,6,7,8,9,10]

2. Подготовка к зачету {с элементами электронного обучения и дистанционных образовательных технологий} (8ч.)[1,2,3,4,5,6,7,8,9,10]

Семестр: 8

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	
10	0	20	42	36

Лекционные занятия (10ч.)

1. Выбор и обоснование темы ВКР. {дискуссия} (4ч.)[2,4,5,6] Обсуждение темы ВКР обучающихся с целью согласования ее содержания, структуры, названия, достаточности планируемого в ней объема работ и ее соответствия объектам и видам профессиональной деятельности.

2. Рекомендации в направлении реализации ВКР {дискуссия} (4ч.)[2,4,5,6] Состав и содержание выпускной квалификационной работы. Теоретические

работы. Научно-исследовательские работы. Работы связанные с решением прикладных задач. Выполнение и подготовка ВКР к защите. Выполнение аналитической части ВКР. Выполнение практической части ВКР. Внедрение результатов работы. Рецензирование ВКР.

3. Разработка сопутствующего материала ВКР. {дискуссия} (2ч.)[2,4,5,6] Составление демонстрационного материала ВКР.

Практические занятия (20ч.)

1. ВКР как результат соответствия профпригодности. Разработка ВКР {с элементами электронного обучения и дистанционных образовательных технологий} (10ч.)[1,3,7,8,9,10] Поиск и составление обзора научной литературы по теме научного исследования на примере ВКР. Литературный обзор по теме ВКР. Определение объекта, предмета, цели и задач научного исследования на примере ВКР. То есть осуществлять поиск и анализ необходимой информации, уметь составлять устные и письменные отчеты, презентовать и защищать результаты своей работы, а также применять профессиональную терминологию, составлять аналитические обзоры по вопросам обеспечения безопасности информационных систем и организации защиты информации на объектах информатизации.

2. Применение знаний в области информационной безопасности по теме ВКР {тренинг} (4ч.)[1,3,7,8,9,10] Определение и правовое обоснование состава защищаемой информации организации. Определение и характеристика объектов защиты информации по теме ВКР. Разработка модели угроз безопасности объекту информатизации организации по теме ВКР. Разработка элементов концепции КСЗИ объекта информатизации и политики информационной безопасности организации на примере ВКР.

3. Технология публичных презентаций. {тренинг} (6ч.)[1,3,7,8,9,10] Технология публичных презентаций. Разработка и написание тезисов доклада публичного выступления по теме ВКР на научной конференции. Разработка графических средств научного исследования на примере презентации для ВКР.

Самостоятельная работа (42ч.)

1. Подготовка к текущим занятиям, самостоятельное изучение материала {с элементами электронного обучения и дистанционных образовательных технологий} (34ч.)[1,2,3,4,5,6,7,8,9,10]

2. Подготовка к промежуточной аттестации {с элементами электронного обучения и дистанционных образовательных технологий} (8ч.)[1,2,3,4,5,6,7,8,9,10]

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. Кошелев А.А., Шарлаев Е.В. Игровой тренинг - имитации, поиск, эксплуатации и устранения уязвимостей. Лабораторный практикум: учебнометодическое пособие; Алт. гос. техн. ун – т им. И.И. Ползунова, - Барнаул: 2017. -41 с. Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/KoshelevSharlaev_IgrTrenIEUU_ump.pdf

2. Загинайлов Ю.Н. Основы научных исследований: учебно-методическое пособие / Ю.Н. Загинайлов, Алт. гос. тех. ун-т им. И.И. Ползунова. – Барнаул: АлтГТУ. – 2015. -138 с. [электронный ресурс]: http://elib.altstu.ru/eum/download/ivtib/uploads/zaginaylov-yu-n-ivtiib-56288fb9d524b.pdf

6. Перечень учебной литературы

6.1. Основная литература

3. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд. — Москва : ДМК Пресс, 2017. — 434 с. — ISBN 978-5-97060-435-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/93278 (дата обращения: 17.09.2021).

4. Рыжков, И. Б. Основы научных исследований и изобретательства : учебное пособие / И. Б. Рыжков. — 4-е изд., стер. — Санкт-Петербург : Лань, 2020. — 224 с. — ISBN 978-5-8114-5697-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/145848

6.2. Дополнительная литература

5. Основы научных исследований и патентоведение: учебно-методическое пособие /Новосиб. гос. аграр. ун-т, Инженер. ин-т; [сост.: С. Г. Щукин и др.].- Новосибирск: НГАУ, 2013- 228с.- Режим доступа:http://biblioclub.ru/index.php?page=book&id= 230540&sr=1

6. Горелов, С.В. Основы научных исследований : учебное пособие / С.В. Горелов, В.П. Горелов, Е.А. Григорьев ; под ред. В.П. Горелова. - 2-е изд., стер. - Москва ; Берлин : Директ-Медиа, 2016. - 534 с. : ил., табл. - Библиогр. в кн. - ISBN 978-5-4475-8350-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=443846 (31.01.2019).

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

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

8. Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/

9. Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/

10. Интернет-издание о высоких технологиях https://www.cnews.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	CentOS Linux
2	Chrome
3	Dia
4	DOSBox
5	FAR Manager
6	GIMP
7	Git
8	Inkscape
9	LibreOffice
10	Microsoft Office Visio Standard 2007
11	Mozilla Firefox
12	Python
13	Windows
14	Антивирус Kaspersky

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Бесплатная электронная библиотека онлайн "Единое окно к образовательным

№пп	Используемые профессиональные базы данных и информационные справочные системы
	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 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».