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.2.2 «Защита информации в киберфизических системах»**

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: **элективные дисциплины (модули)**

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 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-4.2	Предлагает методы исследования объектов информатизации с учетом их особенностей

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Защита информации от утечки по техническим каналам, Информационные процессы и системы, Моделирование и анализ процессов, систем и объектов защиты информации, 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, Преддипломная практика, Технология проведения исследования защищенности объектов и средств защиты

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 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	32	48	0	100	90

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 (32ч.)

1. Введение {беседа} (2ч.)[2,4,7,9,10,12] Общее представление о киберфизических системах. АСУ ТП. Интернет вещей - IoT и IIoT системы. SCADA – системы

2. Примеры киберфизических систем {лекция с разбором конкретных ситуаций} (3ч.)[4,7,9] Киберфизические системы в автомобилестроении. Киберфизические системы в строительстве, сельском хозяйстве, машиностроении, ЖКХ. СКУД как киберфизическая система. Коллективы автономных роботов как пример киберфизических систем в наземном, воздушном и водном транспорте

3. Характеристики мониторинга безопасности киберфизических систем {лекция с разбором конкретных ситуаций} (3ч.)[4,5,6] Таксономия аварий и катастроф. Методы исследования защищенности киберфизических систем с учетом их особенностей, способы описания и анализа их свойств безопасности. Проблемы, связанные с обеспечением безопасности сложных энергонасыщенных систем. Показатели и критерии безопасности систем. Киберфизическая система как объект управления информационной безопасностью и ее модель угроз с точки зрения теории управления. Характеристики мониторинга безопасности

4. Интерфейсы киберфизических систем {лекция с разбором конкретных ситуаций} (4ч.)[2,3,4,7,9] Field – интерфейсы. Проводные интерфейсы RS – 232, RS – 422, RS – 485, Microlan. Беспроводные интерфейсы Wi-Fi, ZigBee, GSM, WiMax, NFC

5. Информационно-измерительные преобразователи киберфизических систем {лекция с разбором конкретных ситуаций} (4ч.)[2,8] Классификация измерительных преобразователей. Принцип работы основных видов измерительных преобразователей. Исполнительные устройства

6. Стандарты, платформы и технологии IoT {лекция с разбором конкретных ситуаций} (4ч.)[4,7,9] Архитектура IoT и IIoT систем. LoRaWan, LTE-M, Sigfox, NB-IoT, BLE, Z-Wave - краткая характеристика и особенностей распространения радиосигнала

7. SCADA-системы {лекция с разбором конкретных ситуаций} (4ч.)[2,8,10] Архитектура SCADA-систем. Программируемые логические контроллеры (ПЛК). Промышленные компьютеры. Краткая характеристика современных SCADA систем

8. Основы методологии обоснования требований к безопасности технических систем и обеспечения этих требований {лекция с разбором конкретных ситуаций} (4ч.)[4,5,6] Закономерности развития технических систем. Фундаментальная система факторов, определяющих качество и безопасность системы. Системотехнический анализ развития системы. Модель функционирования технических систем. Вероятностные модели исследования состояний технических систем. Методы обеспечения безопасности киберфизических систем. Управление и регулирование безопасностью и рисками

9. Методы выявления аномального поведения в работе киберфизических

систем {лекция с разбором конкретных ситуаций} (4ч.)[5,6,12] Методы предсказания на основе анализа многомерных временных рядов. Использование механизма NEAT-гиперкуба для обнаружения кибератак на системы IoT. Обнаружение аномалий в киберфизических си-стемах с использованием графовых нейронных сетей. Выявление аномальных ситуаций в сетевых сегментах Интернета вещей на основе ансамбля классификаторов. Применение технологии Honeypot с адаптивным поведением для отслеживания и анализа атак на сети Интернета вещей. Обеспечение устойчивости киберфизических систем (КФС) на основе теории графов. Выявление аномального функционирования устройств индустрии 4.0 на основе поведенческих паттернов

Лабораторные работы (48ч.)

1. Изучение характеристик и возможностей промышленных автоматических регуляторов {творческое задание} (6ч.)[1,2,3] В соответствии с индивидуальным заданием изучить принципы настройки, программирования и интерфейсы промышленных автоматических регуляторов фирмы ОВЕН

2. Изучение учебной SCADA –системы и языков программирования в ее среде {тренинг} (6ч.)[1,2,3] Изучить основные возможности и характеристики SCADA –системы Trave Mode и получить общее представление о визуальных языках FBD (стандарт МЭК 6-1131/3); SFC (стандарт МЭК 6-1131/3); LD (стандарт МЭК 6-1131/3); ST (стандарт МЭК 6-1131/3) и о процедурном языке IL (стандарт МЭК 6-1131/3). Написать простейшую программу на языке IL.

3. Инсталляция SCADA – системы Trace Mode и изучение её интерфейса {разработка проекта} (6ч.)[1,2,3] Установить на виртуальной машине SCADA - систему и на тестовых примерах научиться создавать основные компоненты проектов автоматизации производственных процессов.

4. Создание тестового проекта в интегрированной среде разработки SCADA-системы TRACE MODE {разработка проекта} (6ч.)[1,2,3] Используя инструментальную систему и набора исполнительных модулей создать типовой проект по тестовому примеру. Оценить уязвимости при работе с проектом.

5. Исследование характеристик и параметров защищенности проводных коммуникационных сетей {творческое задание} (6ч.)[1,2,3] Выполнение пен-тестов с целью оценки степени защищенности проводной сети

6. Исследование характеристик и параметров защищенности беспроводных коммуникационных сетей {творческое задание} (6ч.)[1,2,3] Выполнение пен-тестов с целью оценки степени защищенности беспроводной сети

7. Выявление аномальных ситуаций в сетевых сегментах киберфизических систем на основе анализа многомерных временных рядов методом Хольта-Винтерса {творческое задание} (6ч.)[1,2,3] Использование готовых инструментов и разработка и реализация собственных алгоритмов для выполнения задания

8. Выявление аномальных ситуаций и оценка защищенности в сетевых сегментах киберфизических систем на ос-нове поведенческих проектов

{творческое задание} (6ч.)[1,2,3] Использование готовых инструментов и разработка и реализация собственных алгоритмов для выполнения задания

Самостоятельная работа (100ч.)

1. Изучение дополнительной информации по теме дисциплины {с элементами электронного обучения и дистанционных образовательных технологий} (20ч.)[7,8,9,10,11,12] Самостоятельная работа студентов (СРС) заключается в изучении теоретического материала не только по лекциям но и по дополнительным источникам (как из списка рекомендуемой литературы, так и самостоя-тельно найденных в интернет при одобрении преподавателем).

2. Подготовка к лабораторным работам {с элементами электронного обучения и дистанционных образовательных технологий} (44ч.)[1,2,3] Включает изучение методической литературы и интернет источников по теме работы и оформление по ней отчета

3. Подготовка к экзамену {с элементами электронного обучения и дистанционных образовательных технологий} (36ч.)[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. Якунин А.Г. Лабораторный практикум по курсу «Информационноизмерительные и управляющие системы»: Методические указания для студентов специальности «Вычислительные машины, комплексы, системы и сети» / Алт. гос. техн. ун-т им. И.И. Ползунова. – Барнаул, 2010. - 58 с., ил. - pdf-файл 1.12МБ. - URL: http://elib.altstu.ru/eum/download/avs/Jakunin-IIUS.pdf

2. Сучкова Л.И., Якунин А.Г. Информационно-измерительные и управляющие системы: Учебное пособие / Алт. гос. техн. ун-т им. И.И. Ползунова. – Барнаул, 2014. - 145 с., ил. - pdf-файл 1.78МБ. - URL: http://elib.altstu.ru/eum/download/vsib/Sutkova-iiup.pdf

3. Шарлаев Е.В. Вычислительные сети. Учебно-методическое пособие/ Е.В. Шарлаев; Алт. гос. техн. ун – т им. И.И. Ползунова, - Барнаул: 2015. - 86 с. Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/uploads/sharlaev-e-v-ivtiib-569e03fec1d87.pdf

6. Перечень учебной литературы

6.1. Основная литература

4. Петров, В. В. Комплексные системы безопасности современного города :

учебное пособие / В. В. Петров, В. В. Коробкин, А. Б. Сивенко ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 158 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499967 (дата обращения: 24.06.2021). – Библиогр.: с. 136-144. – ISBN 978-5-9275-2587-4. – Текст : электронный.

5. Александровская, Л. Н. Безопасность и надежность технических систем : учебное пособие / Л. Н. Александровская, И. З. Аронов, В. И. Круглов. — Москва : Логос, 2008. — 376 c. — ISBN 978-5-98704-115-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/9055.html (дата обращения: 04.08.2021). — Режим доступа: для авторизир. пользователей

6. Гаенко, В. П. Безопасность технических систем. Методологические аспекты теории, методы анализа и управления безопасностью : монография / В. П. Гаенко, В. Е. Костюков, В. Н. Фомченко. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2020. — 329 c. — ISBN 978-5-9515-0452-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/101918.html (дата обращения: 04.08.2021). — Режим доступа: для авторизир. пользователей

6.2. Дополнительная литература

7. Ли, П. Архитектура интернета вещей / П. Ли ; перевод с английского М. А. Райтман. — Москва : ДМК Пресс, 2019. — 454 с. — ISBN 978-5-97060-672-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112923 (дата обращения: 24.06.2021). — Режим доступа: для авториз. пользователей

8. Сафьянников, Н. М. Информационно-измерительные преобразователи киберфизических систем : учебное пособие для вузов / Н. М. Сафьянников, О. И. Буренева, А. Н. Алипов. — Санкт-Петербург : Лань, 2020. — 236 с. — ISBN 978-5-8114-5402-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152596 (дата обращения: 04.08.2021). — Режим доступа: для авториз. пользователей

9. Кабалдин, Ю. Г. Управление киберфизическими и механообрабатывающими системами в цифровом производстве на основе искусственного интеллекта и облачных технологий : учебное пособие / Ю. Г. Кабалдин, Д. А. Шатагин, П. В. Колчин. — Москва : Машиностроение, 2019. — 293 с. — ISBN 978-5-907104-17-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/151072 (дата обращения: 04.08.2021). — Режим доступа: для авториз. пользователей.

10. Кангин, В. В. Разработка SCADA-систем : учебное пособие / В. В. Кангин, М. В. Кангин, Д. Н. Ямолдинов. — Москва, Вологда : Инфра-Инженерия, 2019. — 564 с. — ISBN 978-5-9729-0319-1. — Текст : электронный // Элек-тронно-библиотечная система IPR BOOKS : [сайт]. — URL:

https://www.iprbookshop.ru/86632.html (дата обращения: 04.08.2021). — Режим доступа: для авторизир. пользователей

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

11. Периодический рецензируемый научный журнал «Безопасность информационных технологий» URL: https://bit.mephi.ru/index.php/bit

12. Журнал «Проблемы информационной безопасности. Компьютерные системы». -URL: https://jisp.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	Foxit Reader
2	LibreOffice
3	SCADA TRACE MODE бесплатная версия
4	Windows
5	Антивирус Kaspersky
6	7-Zip

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	IEEE Xplore - Интернет библиотека с доступом к реферативным и полнотекстовым статьям и материалам конференций. Бессрочно без подписки (https://ieeexplore.ieee.org/Xplore/home.jsp)
2	Springer - Издательство с доступом к реферативным и полнотекстовым материалам журналов и книг (https://www.springer.com/gp https://link.springer.com/)
3	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)
4	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».