

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.26 Аппаратные средства вычислительной техники»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная
промышленность)

(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2026

Рабочая программа дисциплины «Б1.Д.Б.26 Аппаратные средства вычислительной техники» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 10 от "06" июля 2026г.

Заведующий кафедрой

Кафедра вычислительной техники и защиты информации
наименование кафедры


подпись

В.В. Тугов
расшифровка подписи

Исполнители:

доцент кафедры ВТиЗИ
должность


подпись

Р.Р. Галимов
расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

10.03.01 Информационная безопасность

код наименование

личная подпись

расшифровка подписи

В.В. Тугов

Заведующий отделом формирования фонда и научной обработки документов

главный библиограф Точ. Т.С. Тасайтис
личная подпись расшифровка подписи

Уполномоченный по качеству факультета

личная подпись



С.Н. Морозова
расшифровка подписи

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель освоения дисциплины: формирование у студентов компетенций в области аппаратных средств вычислительной техники с учетом специфики их применения в автоматизированных системах (промышленных, критической инфраструктуры, электронной промышленности), а также навыков выявления и нейтрализации угроз, связанных с аппаратными закладками, недекларированными возможностями и уязвимостями встроенных систем.

Задачи:

- изучить классификацию вычислительных машин и основные характеристики различных классов ЭВМ, включая промышленные контроллеры;
- получить базовые представления об основных архитектурах, принципах построения и работы ЭВМ и их узлов с акцентом на безопасность;
- изучить типовые архитектуры промышленных контроллеров (PLC, PAC, IoT-шлюзов) и их уязвимости;
- определять направления использования ЭВМ определенного класса для решения задач в области информационной безопасности;
- иметь навыки работы с ЭВМ, микроконтроллерами и средствами аппаратной защиты.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.14 Физика, Б1.Д.Б.23 Информатика*

Постреквизиты дисциплины: *Б1.Д.Б.9 Сети и системы передачи информации, Б1.Д.Б.10 Программно-аппаратные средства защиты информации, Б1.Д.Б.18 Теория информации, Б1.Д.Б.33 Комплексные системы защиты информации на предприятии, Б1.Д.Б.38 Защита информации от утечки по техническим каналам, Б1.Д.В.5 Основы стеганографии, Б1.Д.В.8 Защита объектов критической информационной инфраструктуры, Б1.Д.В.9 Защита доступа в автоматизированных системах, Б1.Д.В.Э.4.2 Системы и сети связи, Б1.Д.В.Э.5.1 Аппаратно-программные средства цифровой обработки сигналов, Б1.Д.В.Э.5.2 Микропроцессорные системы, Б1.Д.В.Э.6.2 Проектирование локальных вычислительных сетей, Б2.П.Б.У.1 Ознакомительная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2-В-1 Выбирает, обосновывает и применяет современные эффективные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе - отечественного производства, для решения задач профессиональной деятельности	Знать: <u>принципы работы аппаратных средств вычислительной техники;</u> <u>архитектуру контроллеров, PLC, SCADA-систем;</u> Уметь: <u>обосновывать выбор аппаратной платформы для автоматизированных систем с учетом</u>

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		<u>защищенности;</u> Владеть: <u>навыками конфигурирования аппаратной защиты встроенных систем.</u>
ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4-В-1 Применяет современные методы и средства диагностирования и мониторинга автоматизированных систем	Знать: - знать принципы работы аппаратных средств защиты. Уметь: - осуществлять диагностику средств защиты. Владеть: - навыками мониторинга целостности прошивок и аппаратных ключей.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	2 семестр	всего
Общая трудоёмкость	108	108
Контактная работа:	51,25	51,25
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	16	16
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - выполнение индивидуального творческого задания (ИТЗ); - самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий); - изучение разделов курса в системе электронного обучения; - подготовка к лабораторным занятиям; - подготовка к практическим занятиям; - подготовка к рубежному контролю)	56,75	56,75
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	экзамен	

Разделы дисциплины, изучаемые в 2 семестре

№ раздела	Наименование разделов	Количество часов			
		всего	аудиторная работа		
			Л	ПЗ	ЛР
					внеауд. работа

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Элементы и узлы ЭВМ. Основные характеристики ВТ	19	4	3	2	10
2	Микропроцессор. Микропроцессорная система	22	4	3	5	10
3	Система ввода-вывода ЭВМ	17	4	2	1	10
4	Микроконтроллеры и микроЭВМ. Платформа Arduino	25	4	4	3	14
5	Аппаратные аспекты безопасности автоматизированных систем и электронной промышленности	25	2	4	5	14
	Итого:	108	18	16	16	58
	Всего:	108	18	16	16	58

4.2 Содержание разделов дисциплины

№ 1. Элементы и узлы ЭВМ. Основные характеристики ВТ. Структура ЭВМ и назначение ее элементов. Общая структура центрального процессора. Назначение и основные элементы центрального процессора. ПЭВМ. Архитектура современных ПЭВМ. Системная плата, ее назначение, основные элементы и их взаимодействие. Системная магистраль. Основные стандарты системных магистралей (шин). Системы исчисления. Форматы представления чисел в ЭВМ. Основные характеристики ВТ. Критерии выбора аппаратных средств для автоматизированных систем с учетом требований безопасности.

№ 2. Микропроцессор. Микропроцессорная система. Понятие микропроцессора (МП); виды технологии производства МП, поколения МП и их основные характеристики; обобщенная структура МП; перспективные МП ПЭВМ. Микропроцессорные комплекты. Организация и структура памяти. Элементы памяти, их назначение, возможности и принцип работы. Структура памяти ПЭВМ. Кэш-память и атаки по побочным каналам. Защита памяти.

№ 3. Система ввода-вывода ЭВМ.

Назначение, состав и технические характеристики периферийного оборудования ЭВМ. Периферийное оборудование ПЭВМ. Средства ввода информации. Адаптеры внешних устройств (платы расширения). Системы прерываний. Назначение, принцип работы и организация системы прерываний. Безопасность обработчиков прерываний в реальном времени.

№ 4. Микроконтроллеры и микроЭВМ. Платформа Arduino.

Назначение, состав и технические характеристики микроконтроллеров. Области применения микроконтроллеров. Платформа Arduino. Применение платформы Arduino для создания мобильной системы экологического мониторинга. Использование микроконтроллеров для защиты БПЛА от НСД на основе навигационного ключа. Мобильная антивирусная система на базе Raspberry Pi. Средства мониторинга и диагностики автоматизированных систем. Отечественные микроконтроллеры: встроенные механизмы защиты памяти, аппаратная криптография, изолированные области выполнения.

№ 5. Аппаратные аспекты безопасности автоматизированных систем и электронной промышленности

Промышленные автоматизированные системы (АСУ ТП). Архитектура PLC (программируемых логических контроллеров), промышленные сети (Profinet, Modbus TCP, EtherCAT). Уязвимости промышленных контроллеров: незащищенные отладочные интерфейсы (JTAG, SWD), недостатки защиты памяти, возможность перепрошивки без аутентификации. Доверенные аппаратные платформы для автоматизированных систем. TPM 2.0, Secure Element, Trusted Execution Environment (TEE). Применение в промышленных контроллерах и IoT-устройствах. Secure Boot, измерение доверия (remote attestation). Аппаратная защита встроенных систем (embedded security). Изоляция памяти (MPU), защита от переполнения буфера на уровне процессора, шифрование внешней памяти, защита от снятия дампов.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1,2	Машинный формат команд. Анализ дизассемблированного кода контроллера	2
2	2	Регистр флагов и обработка прерываний в реальном времени	2
3	1,2	Стек и переполнение буфера	2
4	2,5	Передача параметров через стек. Имитация атаки на интерфейс отладки	2
5	3,5	Команды ввода-вывода. Анализ Modbus-трафика	2
6	4,5	Знакомство с платформой Arduino (прототип промышленного датчика). Безопасная загрузка	2
7	4	Подключение цифрового датчика. Реализация аутентификации по аппаратному ключу	2
8	5	Использование TPM для защиты ключей в АСУ ТП	2
		Итого:	16

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1,2	Системы исчисления и форматы представления чисел	4
2	1,2	Анализ уязвимостей архитектуры x86 vs ARM для встраиваемых систем	2
3	3	Система прерываний в реальном времени. Безопасность обработчиков прерываний	2
4	4	Изучение архитектуры промышленного контроллера	2
5	4	Подключение цифрового датчика. Анализ возможности подмены данных по шине I2C	2
6	5	Настройка Secure Boot на одноплатном компьютере	2
7	5	Применение TPM в АСУ ТП: аттестация удаленного узла	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Техническое и программное обеспечение вычислительных машин и систем : учебное пособие : [16+] / О. В. Конюхова, Э. А. Кравцова, П. В. Лукьянов, А. Ю. Ужаринский. – Москва ; Вологда : Инфра-Инженерия, 2023. – 200 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=725699> (дата обращения: 13.04.2026). – Библиогр. в кн. – ISBN 978-5-9729-1186-8. – Текст : электронный.

2. Программно-аппаратные средства защиты информации : учебное пособие : в 3 частях / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2024. – Часть 3. – 82 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=723472> (дата обращения: 13.04.2026). – Библиогр. в кн. – ISBN 978-5-8265-2795-5 (ч. 3). – ISBN 978-5-8265-2464-0. – Текст : электронный.

5.2 Дополнительная литература

1. Аппаратные средства вычислительной техники [Электронный ресурс] : метод. указания / Р. Р. Галимов; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники. - Электрон. текстовые дан. (1 файл: 0.87 Мб). - Оренбург : ОГУ, 2012. - 57 с. - Загл. с тит. экрана. - Adobe Acrobat Reader 6.0. - Режим доступа: http://artlib.osu.ru/web/books/metod_all/3049_20120322.pdf.

2. Параскевов, А. В. Микропроцессоры : учебник : [16+] / А. В. Параскевов. – Изд. 2-е, испр. и доп. – Москва ; Вологда : Инфра-Инженерия, 2023. – 136 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=727462> (дата обращения: 12.05.2026). – Библиогр. в кн. – ISBN 978-5-9729-1291-9. – Текст : электронный.

5.3 Периодические издания

1. Журнал «Мир ПК» : журнал. - Москва : Агентство "Роспечать", 2013-2015
2. Информационно-измерительные и управляющие системы : журнал. - Москва : Радиотехника, 2018, 2019.

5.4 Интернет-ресурсы

1. <http://arduino.ru/> - сайт посвященный платформе Arduino.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. 1. Операционная система РЕД ОС.
2. Пакет офисных приложений «МойОфис Образование»
3. Для работы с ресурсами Интернет - веб-браузер Яндекс <https://yandex.ru/>.
4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ <http://garant.net.osu.ru>
5. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа - <http://aist.osu.ru>.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется лаборатория компьютерный класс.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.