

УТВЕРЖДАЮ  
 Декан факультета

« \_\_\_\_ » \_\_\_\_\_ 20\_\_

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Направление/специальность подготовки	09.03.02 Информационные системы и технологии
Специализация/профиль/программа подготовки	Информационная безопасность
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	И Робототехника и инновационная инженерия
Выпускающая кафедра	Н2 Программная инженерия и интеллектуальные системы
Кафедра-разработчик рабочей программы	Н2 Программная инженерия и интеллектуальные системы

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
2	4	4	144	68	34	0	34	76	0	0	76	ЭКЗ.
3	5	5	180	34	17	0	17	146	0	18	128	ЭКЗ.
ВСЕГО		9	324	102	51	0	51	222	0	18	204	

*ЛИСТ СОГЛАСОВАНИЯ*

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО  
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

**09.03.02 Информационные системы и технологии**

год набора группы: 2026

Программу составили:

Кафедра Н2 Программная инженерия и интеллектуальные системы  
Кузьмич Александр Александрович, к.т.н., доцент

\_\_\_\_\_

Кафедра Н2 Программная инженерия и интеллектуальные системы  
Устиновский Георгий Сергеевич, ассистент

\_\_\_\_\_

Программа рассмотрена  
на заседании кафедры-разработчика  
рабочей программы **Н2 Программная инженерия и интеллектуальные системы**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

\_\_\_\_\_

Программа рассмотрена  
на заседании выпускающей кафедры

**Н2 Программная инженерия и интеллектуальные системы**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

\_\_\_\_\_

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

### **Разделы рабочей программы**

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### **Приложения к рабочей программе дисциплины**

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-5 — Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем

ОПК-7 — Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем

Формированию компетенций служит достижение следующих результатов образования:

### **ОПК-5**

*знания:*

Знать назначение, состав и принципы функционирования системного программного обеспечения вычислительных систем, включая операционные системы, системные службы, драйверы, модули ядра, средства обновления, механизмы управления доступом, регистрации событий, мониторинга и сетевого взаимодействия;

*умения:*

Уметь выполнять базовую установку, настройку и проверку работоспособности системного программного обеспечения, анализировать параметры операционной системы, системных служб, драйверов, механизмов доступа, журналов событий, обновлений и сетевых компонентов вычислительной системы;

*навыки:*

Владеть навыками применения штатных средств операционной системы и инструментальных программных средств для проверки состояния системного программного обеспечения, выявления ошибок конфигурации, оценки параметров функционирования и подготовки выводов о работоспособности и защищенности вычислительной системы.

### **ОПК-7**

*знания:*

Знать основные виды операционных систем, системных платформ, программно-аппаратных средств и инструментальных средств, применяемых для функционирования, настройки, мониторинга, анализа и защиты информационных систем;

*умения:*

Уметь выбирать операционную систему, системные компоненты, программно-аппаратные средства и инструменты анализа с учетом назначения информационной системы, условий эксплуатации, требований к устойчивости, совместимости, производительности и защищенности;

*навыки:*

Владеть навыками обоснованного выбора и применения системных платформ, штатных средств операционной системы и инструментальных программно-аппаратных средств для анализа состояния, настройки, мониторинга и обеспечения защищенного функционирования информационных систем.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

Содержание дисциплины является логическим продолжением дисциплин: **ИНФОРМАТИКА: ОСНОВЫ ПРОГРАММИРОВАНИЯ, КОМПЬЮТЕРНЫЙ ПРАКТИКУМ, СТРУКТУРЫ И ОРГАНИЗАЦИЯ ДАННЫХ**.

Содержание дисциплины является основой для освоения дисциплин: **СЕТИ ЭВМ И ТЕЛЕКОММУНИКАЦИИ, АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-2 — Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
- ОПК-3 — Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- ОПК-6 — Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий
- ОПК-7 — Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем
- ПК-94 — Способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 9 з.е., 324 ч.

#### 3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	
				ВСЕГО	Лекции	Практические занятия		ОПК-5	ОПК-7
2	4	Раздел 1. Введение в информационную безопасность вычислительных систем. 1.1 Введение в информационную безопасность вычислительных систем. Основные понятия. 1.2 Угрозы, уязвимости и риски. 1.3 Концепция доверенной вычислительной базы и механизмы безопасной загрузки.	30	12	6	6	18	17	17
2	4	Раздел 2. Архитектура операционных систем и безопасность. 2.1 Архитектура операционных систем как объект атак. 2.2 Механизмы автозапуска и закрепления программ в операционных системах. 2.3 Безопасность драйверов и модулей ядра операционной системы.	22	12	6	6	10	17	17
2	4	Раздел 3. Комплексный анализ атак и расследование инцидентов. 3.1 Жизненный цикл атаки в операционной системе. 3.2 Первичный анализ компьютерного инцидента по ограниченному набору системных данных. 3.3 Анализ и корреляция цифровых следов в операционной системе при расследовании инцидента. 3.4 Обобщение результатов расследования компьютерного инцидента и выработка решений.	36	16	8	8	20	17	17
2	4	Раздел 4. Управление доступом, регистрация событий безопасности и мониторинг в операционной системе. 4.1 Субъекты, объекты и правила управления доступом в операционной системе. 4.2 Контекст безопасности процесса и привилегии в операционной системе. 4.3 Регистрация событий безопасности в операционной системе. 4.4 Мониторинг состояния операционной системы и выявление отклонений.	34	16	8	8	18	17	17
2	4	Раздел 5. Средства обеспечения информационной безопасности вычислительных систем. 5.1 Архитектура средств защиты операционной системы. 5.2 Обновления и управление уязвимостями. 5.3 Комплексная защита системы.	22	12	6	6	10	16	16
Всего за 4 семестр			144	68	34	34	76	84	84
3	5	Раздел 6. Системы программирования. 1.1 Лексический анализ. 1.2 Синтаксический анализ. 1.3 Промежуточное представление кода.	163	17	7	10	146	6	6
3	5	Раздел 7. Утилиты операционной системы. 2.1 Классификация и назначение системных утилит. 2.2 Командные оболочки (shell): возможности и принципы работы. 2.3 Программирование на bash / PowerShell. 2.4 Системные вызовы и API ОС.	5	5	3	2	0	6	6
3	5	Раздел 8. Основы сетевого системного ПО. 3.1 Стек протоколов TCP/IP (обзор с точки зрения системного программиста). 3.2 Программирование сокетов (socket programming): TCP и UDP. 3.3 Разработка простейших сетевых сервисов и демонов.	12	12	7	5	0	4	4
Всего за 5 семестр			180	34	17	17	146	16	16
Всего по дисциплине			324	102	51	51	222	100	100

#### 3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Введение в информационную безопасность вычислительных систем.	Первичный анализ информационной безопасности вычислительной системы средствами операционной системы.	2
2		Моделирование угроз безопасности и оценка критичности уязвимостей	2
3		Доверенная вычислительная база (TCB). Как защитить компьютер на уровне железа.	2
4	Раздел 2. Архитектура операционных систем и безопасность.	Инструментальный анализ иерархии процессов и потоков. Выявление скрытых процессов и аномалий родительских связей.	2
5		Анализ методов персистентности (закрепления) ПО в системе: реестр, службы и планировщики задач.	2
6		Анализ драйверов и модулей ядра. Выявление угроз безопасности.	2
7	Раздел 3. Комплексный анализ атак и расследование инцидентов.	Определение этапа атаки в операционной системе по совокупности системных признаков.	2

8		Оценка достаточности системных данных для первичного анализа компьютерного инцидента.	2
9		Корреляционный анализ цифровых следов компьютерного инцидента в операционной системе.	2
10		Подготовка итогового аналитического заключения по результатам расследования компьютерного инцидента.	2
11	Раздел 4. Управление доступом, регистрация событий безопасности и мониторинг в операционной системе.	Анализ правил доступа к объектам операционной системы.	2
12		Анализ контекста безопасности процесса и его привилегий.	2
13		Анализ регистрации событий безопасности в операционной системе.	2
14		Выявление отклонений в состоянии операционной системы по данным мониторинга.	2
15	Раздел 5. Средства обеспечения информационной безопасности вычислительных систем.	Анализ механизмов защиты операционной системы средствами СЗИ.	2
16		Анализ уязвимостей и планирование обновлений вычислительной системы.	2
17		Комплексный анализ защищенности вычислительной системы.	2
Всего за 4 семестр			34
18	Раздел 6. Системы программирования.	Построение синтаксического анализатора.	5
19		Построение лексического анализатора.	5
20	Раздел 7. Утилиты операционной системы.	Виртуальная память. Замеры и анализ. Написание программы для анализа TLB-промахов и page-fault.	2
21	Раздел 8. Основы сетевого системного ПО.	Клиент-серверное приложение на сокетах.	5
Всего за 5 семестр			17

### 3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Введение в информационную безопасность вычислительных систем.	Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	9
2		Подготовка к практическому занятию.	9
3	Раздел 2. Архитектура операционных систем и безопасность.	Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	5
4		Подготовка к практическому занятию.	5
5	Раздел 3. Комплексный анализ атак и расследование инцидентов.	Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	10
6		Подготовка к практическому занятию.	10
7	Раздел 4. Управление доступом, регистрация событий безопасности и мониторинг в операционной системе.	Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	9
8		Подготовка к практическому занятию.	9
9	Раздел 5. Средства обеспечения информационной безопасности вычислительных систем.	Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	5
10		Подготовка к практическому занятию.	5
Всего за 4 семестр			76

11	Раздел 6. Системы программирования.	Реализация трансляции с использованием файлов лексического и синтаксического анализаторов.	146
<b>Всего за 5 семестр</b>			146

### 3.4. Курсовая работа

СОДЕРЖАНИЕ ЭТАПА	ПЕРИОД ИСПОЛНЕНИЯ (недели семестра)	ПЛАНИРУЕМОЕ ВРЕМЯ (час)
Этап 1. Реализация лексического анализатора.	1 - 6	4
Этап 2. Реализация синтаксического анализатора.	6 - 12	4
Этап 3. Промежуточное представление кода.	12 - 15	5
Этап 4. Оформление пояснительной записки и защита курсовой работы.	15 - 17	5
<b>Всего за 5 семестр</b>		18

## 4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
4		КПос, Отч. по ПЗ			КПос, Отч. по ПЗ	ДР		КПос, Отч. по ПЗ		ДР			КПос, Отч. по ПЗ			ДР	КПос, Отч. по ПЗ
5			КПос, Отч. по ПЗ		КПос, КР	ДР	КПос, Отч. по ПЗ		КПос, КР	ДР		КР, КПос		КПос, Отч. по ПЗ		ДР	КР, КПос

Условные обозначения:

- ДР – диагностическая работа;
- КПос – контроль посещаемости;
- Отч. по ПЗ – отчет по практическому заданию;
- КР – курсовая работа.

**Текущий контроль успеваемости** студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- контроль посещаемости;
- отчет по практическому заданию;
- курсовая работа.

**Промежуточная аттестация** проводится в формах:

- экзамен.



## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. Основная литература по дисциплине:

1. . Сети и телекоммуникации. Москва: Юрайт, 2020, эл. рес.
2. А. А. Букатов, С. А. Гуда. . Компьютерные сети: расширенный начальный курс. Санкт-Петербург: Питер, 2020, эл. рес.
3. А. В. Гунько. . Системное программирование в среде Linux. Новосибирск: НГТУ, 2020, эл. рес.
4. А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009, 9 экз.
5. А. Н. Сергеев. . Основы локальных компьютерных сетей. Санкт-Петербург: Лань, 2022, эл. рес.
6. В. К. Волк. . Базы данных. Проектирование, программирование, управление и администрирование. Санкт-Петербург: Лань, 2022, эл. рес.
7. Е. А. Басыня. . Системное администрирование и информационная безопасность. Новосибирск: НГТУ, 2018, эл. рес.
8. Е. В. Глинская, Н. В. Чичварин. . Информационная безопасность конструкций ЭВМ и систем. Москва: ИНФРА-М, 2021, эл. рес.
9. Л. Кэмпбелл. . Базы данных. Инжиниринг надежности. Санкт-Петербург: Питер, 2020, эл. рес.
10. М. В. Рыбальченко. . Архитектура информационных систем. Москва: Юрайт, 2020, эл. рес.
11. Н. А. Староверова. . Операционные системы. Санкт-Петербург: Лань, 2022, эл. рес.
12. С. В. Белугина. . Архитектура компьютерных систем. Санкт-Петербург: Лань, 2020, эл. рес.
13. Э. Таненбаум, Т. Остин. . Архитектура компьютера. Санкт-Петербург: Питер, 2020, эл. рес.

### 5.2. Дополнительная литература по дисциплине:

не требуется.

### 5.3. Периодические издания:

1. Моделирование и анализ информационных систем.

### 5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <https://e.lanbook.com/> — ЭБС Лань;
2. <http://library.voenmeh.ru/jirbis2/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

### Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
- <http://www.rfbg.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

### Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. [http://library.voenmeh.ru/jirbis2/index.php?option=com\\_irbis&view=irbis&Itemid=457](http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457) - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

### 5.5. Программное обеспечение:

1. Офисный пакет Libre Office.

### 5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

## **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **6.1. Лекционные занятия:**

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

### **6.2. Практические занятия:**

1. Проектор;
2. Интерактивная доска;
3. Офисный пакет Libre Office.

### **6.3. Прочее:**

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

### Аннотация рабочей программы

Дисциплина **СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *Н Робототехника и инновационная инженерия* БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой *Н2 Программная инженерия и интеллектуальные системы*.

Дисциплина нацелена на формирование *компетенций*:

ОПК-5 Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем;

ОПК-7 Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем.

Содержание дисциплины охватывает круг вопросов, связанных с системным программным обеспечением вычислительных систем, его архитектурой, механизмами функционирования и ролью в обеспечении устойчивой и защищенной работы информационных систем.

В рамках дисциплины системное программное обеспечение рассматривается как совокупность программных средств, обеспечивающих управление ресурсами вычислительной системы, выполнение пользовательских и служебных процессов, взаимодействие с аппаратными компонентами, хранение и обработку данных, сетевое взаимодействие, регистрацию событий и контроль доступа.

Особое внимание уделяется операционным системам как ключевому виду системного программного обеспечения. Рассматриваются архитектура ОС, процессы и службы, механизмы автозапуска, драйверы и модули ядра, управление доступом, контекст безопасности процессов, регистрация событий, мониторинг состояния системы, обновления, управление уязвимостями и средства защиты вычислительной системы.

Практические занятия направлены на анализ состояния системного программного обеспечения средствами операционной системы, оценку параметров безопасности, выявление ошибок конфигурации, анализ системных событий, сетевых взаимодействий и подготовку обоснованных выводов о состоянии вычислительной системы.

Программой дисциплины предусмотрены следующие **виды контроля**:

**Текущий контроль успеваемости** студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- контроль посещаемости;
- отчет по практическому заданию;
- курсовая работа.

**Промежуточная аттестация** проводится в формах:

- экзамен.

Общая трудоемкость освоения дисциплины составляет **9 з.е., 324 ч.** Программой дисциплины предусмотрены лекционные занятия (**51 ч.**), практические занятия (**51 ч.**), самостоятельная работа студента (**222 ч.**).

## ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

### Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 324 ч., из них 102 ч. аудиторных занятий, и 222 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
<b>Раздел 1. Введение в информационную безопасность вычислительных систем.</b>		
Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	А. А. Букатов, С. А. Гуда. . Компьютерные сети: расширенный начальный курс: Санкт-Петербург: Питер, 2020 (2,4) А. В. Гунько. . Системное программирование в среде Linux: Новосибирск: НГТУ, 2020 (2,3,4,5) Н. А. Староверова. . Операционные системы: Санкт-Петербург: Лань, 2022 (2,3,9) Е. А. Басыня. . Системное администрирование и информационная безопасность: Новосибирск: НГТУ, 2018 (1,2,3)	9
Подготовка к практическому занятию.		9
Итого по разделу 1		18
<b>Раздел 2. Архитектура операционных систем и безопасность.</b>		
Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	М. В. Рыбальченко. . Архитектура информационных систем: Москва: Юрайт, 2020 (1-6) Э. Таненбаум, Т. Остин. . Архитектура компьютера: Санкт-Петербург: Питер, 2020 (2,6) С. В. Белугина. . Архитектура компьютерных систем: Санкт-Петербург: Лань, 2020 (1,2,3,5)	5
Подготовка к практическому занятию.		5
Итого по разделу 2		10
<b>Раздел 3. Комплексный анализ атак и расследование инцидентов.</b>		
Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	Е. В. Глинская, Н. В. Чичварин. . Информационная безопасность конструкций ЭВМ и систем: Москва: ИНФРА-М, 2021 (2,3)	10
Подготовка к практическому занятию.		10
Итого по разделу 3		20
<b>Раздел 4. Управление доступом, регистрация событий безопасности и мониторинг в операционной системе.</b>		
Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	. Сети и телекоммуникации: Москва: Юрайт, 2020 (5,6) Э. Таненбаум, Т. Остин. . Архитектура компьютера: Санкт-Петербург: Питер, 2020 (6,7) А. Н. Сергеев. . Основы локальных	9
Подготовка к практическому занятию.		9

	компьютерных сетей: Санкт-Петербург: Лань, 2022 (1,2,6)	
Итого по разделу 4		18
<b>Раздел 5. Средства обеспечения информационной безопасности вычислительных систем.</b>		
Усвоение материала лекции - изучение предусмотренных программой дидактических единиц по рекомендуемой литературе.	В. К. Волк. . Базы данных. Проектирование, программирование, управление и администрирование: Санкт-Петербург: Лань, 2022 (4) А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости: М.: Академия, 2009 (2,3) Л. Кэмпбелл. . Базы данных. Инжиниринг надежности: Санкт-Петербург: Питер, 2020 (5,6)	5
Подготовка к практическому занятию.		5
Итого по разделу 5		10
<b>Раздел 6. Системы программирования.</b>		
Реализация трансляции с использованием файлов лексического и синтаксического анализаторов.	С. В. Белугина. . Архитектура компьютерных систем: Санкт-Петербург: Лань, 2020 (3,4,5) М. В. Рыбальченко. . Архитектура информационных систем: Москва: Юрайт, 2020 (2,3)	146
Итого по разделу 6		146

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- контроль посещаемости;
- отчет по практическому заданию;
- курсовая работа;
- экзамен;
- экзамен.

### Критерии оценивания

#### Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

#### Контроль посещаемости

Контроль посещаемости осуществляется в течение семестра на лекционных и практических занятиях. Посещение занятий учитывается при допуске к промежуточной аттестации. Пропущенные практические занятия подлежат отработке в форме выполнения соответствующего практического задания, представления отчета и защиты результатов перед преподавателем. При оценивании учитываются регулярность посещения занятий, своевременность выполнения практических работ и наличие отчетов по предусмотренным разделам дисциплины.

#### Отчет по практическому заданию

Отчет по практическому заданию сдается в электронной форме. Отчет должен содержать исходные данные варианта, результаты выполнения заданий, таблицы анализа, промежуточные выводы и итоговое заключение по теме практического занятия. При оценивании учитываются полнота выполнения задания, корректность анализа системных данных, обоснованность выводов, правильность использования терминологии, соответствие отчета требованиям к оформлению и способность обучающегося ответить на вопросы преподавателя по выполненной работе. Во время защиты отчета обучающийся отвечает на вопросы преподавателя по теме практического занятия, используемым системным механизмам, полученным результатам и сделанным выводам.

#### Курсовая работа

Курсовая работа представляет собой разработку транслятора (компилятора или интерпретатора) для заданного минимального языка команд/выражений. Обязательно наличие минимального интерфейса (консольного или графического) и сохранение истории обращений – то есть всех введенных программ (или команд) и результатов их трансляции/выполнения. Критерий оценивания:

Отлично – даны полные и ясные ответы на более чем 50% вопросов от преподавателя, наличие интерфейса и истории обращений.

Хорошо – даны не полные, не четкие ответы на более чем 50% вопросов от преподавателя, наличие интерфейса и истории обращений. Удовлетворительно – даны ответы на не менее 2-х вопросов, ответы не полные, наличие интерфейса и истории обращений.

#### Экзамен (семестр 4)

Экзаменационный билет содержит три теоретических вопроса из перечня вопросов к экзамену. Вопросы охватывают содержание разделов 1–5 дисциплины: основы информационной безопасности вычислительных систем, угрозы, уязвимости и риски, доверенную вычислительную базу и безопасную загрузку, архитектуру операционных систем, процессы, службы, механизмы автозапуска, драйверы и модули ядра, анализ системных данных, управление доступом, контекст безопасности процессов, регистрацию событий, мониторинг состояния операционной системы, обновления, управление уязвимостями и средства защиты вычислительных систем.

Критерии оценивания:

Отлично – обучающийся дает полные, точные и логически связанные ответы на все вопросы билета, свободно использует профессиональную терминологию, объясняет назначение и принципы работы системных механизмов, приводит корректные примеры, показывает понимание связи системного программного обеспечения с устойчивостью и защищенностью вычислительной системы.

Хорошо – обучающийся отвечает на все вопросы билета, демонстрирует достаточное понимание основных понятий и механизмов системного программного обеспечения, но допускает отдельные неточности, неполные формулировки или недостаточно подробно раскрывает отдельные элементы ответа.

Удовлетворительно – обучающийся отвечает не менее чем на два вопроса билета, показывает общее понимание основных понятий дисциплины, но допускает существенные пробелы, неполные объяснения, слабую связь между теоретическими положениями и практическими механизмами операционной системы.

Неудовлетворительно – обучающийся не раскрывает содержание большинства вопросов билета, допускает грубые ошибки в основных понятиях, не понимает назначение ключевых механизмов системного программного обеспечения и не может объяснить их роль в функционировании вычислительной системы.

Обучающийся имеет право получить оценку за экзамен по результатам работы в семестре на основании набранных баллов в соответствии с балльно-рейтинговой системой оценивания.

### **Экзамен (семестр 5)**

Экзаменационный билет содержит три вопроса из 30.

Критерий оценивания:

Отлично - Даны ответы на все вопросы.

Ответы полные, ясные, понятные.

В процессе ответа студент показывает глубокие знания по системным программным продуктам, способам взаимодействия системного и пользовательского ПО, взаимодействию с базами данных и периферийными устройствами.

На вопросы по основным понятиям и разделам курса отвечает полно и ясно, используя профессиональную терминологию, отражающую глубокие знания и понимание.

Хорошо -

Даны ответы на все вопросы.

Ответы полные, не четкие.

В процессе ответа студент показывает достаточные знания по системным программным продуктам

На вопросы по основным понятиям и разделам курса отвечает не полно, не достаточно используя профессиональную терминологию. Удовлетворительно -

Даны ответы на не менее 2-х вопросов.

Ответы не полные.

В процессе ответа студент показывает слабые знания

На вопросы по основным понятиям и разделам курса отвечает плохо, не использует профессиональную терминологию, показывает слабое понимание.

Обучающийся имеет право получить оценку за экзамен по результатам работы в семестре на основании набранных баллов в соответствии с балльно-рейтинговой системой оценивания.

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %		НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ОПК-5	ОПК-7	
2	4	Раздел 1. Введение в информационную безопасность вычислительных систем.	30	12	6	6	18	17	17	Контроль посещаемости
2	4	Раздел 2. Архитектура операционных систем и безопасность.	22	12	6	6	10	17	17	Отчет по практическому заданию, Контроль посещаемости
2	4	Раздел 3. Комплексный анализ атак и расследование инцидентов.	36	16	8	8	20	17	17	Отчет по практическому заданию, Контроль посещаемости
2	4	Раздел 4. Управление доступом, регистрация событий безопасности и мониторинг в операционной системе.	34	16	8	8	18	17	17	Отчет по практическому заданию, Контроль посещаемости
2	4	Раздел 5. Средства обеспечения информационной безопасности вычислительных систем.	22	12	6	6	10	16	16	Отчет по практическому заданию, Контроль посещаемости
Всего за 4 семестр			144	68	34	34	76	84	84	
3	5	Раздел 6. Системы программирования.	163	17	7	10	146	6	6	Отчет по практическому заданию, Контроль посещаемости, Курсовая работа
3	5	Раздел 7. Утилиты операционной системы.	5	5	3	2	0	6	6	Отчет по практическому заданию, Контроль посещаемости
3	5	Раздел 8. Основы сетевого системного ПО.	12	12	7	5	0	4	4	Отчет по практическому заданию, Контроль посещаемости
Всего за 5 семестр			180	34	17	17	146	16	16	
Всего по дисциплине			324	102	51	51	222	100	100	



**ОПК-5 - Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем**

№ 1 Прочитайте текст и установите соответствие

Установите соответствие между системным компонентом и его назначением.

1. Драйвер	А. Фиксация сведений о событиях в системе
2. Системная служба	Б. Обеспечение взаимодействия ОС с устройством или низкоуровневым компонентом
3. Журнал событий	В. Выполнение фоновой системной функции
4. Механизм управления доступом	Г. Ограничение операций пользователей и процессов с объектами ОС

№ 2 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Что относится к системному программному обеспечению вычислительной системы?

**Варианты ответа:**

1. Текстовый документ пользователя
2. Операционная система и системные службы
3. Изображение, созданное пользователем
4. Презентация учебного доклада

№ 3 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие действия относятся к проверке корректности установки и настройки системного программного обеспечения?

**Варианты ответа:**

1. Проверка состояния системных служб
2. Проверка наличия и состояния драйверов устройств
3. Анализ журналов событий операционной системы
4. Изменение содержания пользовательского документа
5. Проверка сетевых параметров системы

№ 4 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

**Вопрос:**

Какой системный компонент обеспечивает подключение вычислительной системы к сети на уровне операционной системы?

**Варианты ответа:**

1. Сетевой интерфейс и его драйвер
2. Текстовый редактор
3. Архивный файл пользователя
4. Таблица электронных данных

№ 5 Прочитайте текст и запишите развернутый обоснованный ответ

Почему после установки системного программного обеспечения необходимо проверять состояние служб, драйверов, прав доступа и журналов событий?

№ 6 Прочитайте текст и запишите развернутый обоснованный ответ

Какие проверки необходимо выполнить после настройки межсетевого экрана на вычислительной системе?

№ 7 Прочитайте текст и установите последовательность

Расположите действия в правильной последовательности при проверке установленного системного компонента.

**Элементы последовательности:**

1. Определить назначение системного компонента
2. Проверить состояние службы, драйвера или модуля
3. Проверить параметры конфигурации и права доступа
4. Проанализировать связанные журналы событий
5. Сделать вывод о корректности установки и настройки

№ 8 Прочитайте текст и установите последовательность

Расположите действия в правильной последовательности при проверке защищенного удаленного доступа к вычислительной системе.

**Элементы последовательности:**

1. Определить используемую службу удаленного доступа
2. Проверить открытый порт и связанный процесс
3. Проверить параметры аутентификации и права пользователей
4. Проанализировать правила фильтрации трафика
5. Проверить журналы подключений и ошибок
6. Сформулировать вывод о безопасности настройки

№ 9 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие параметры необходимо проверить при настройке сетевого взаимодействия вычислительной системы?

**Варианты ответа:**

1. IP-адрес и сетевую маску
2. Маршрут по умолчанию
3. Открытые порты и связанные процессы
4. Правила фильтрации входящего и исходящего трафика
5. Цвет рабочего стола пользователя

№ 10 Прочитайте текст и установите соответствие

Установите соответствие между сетевым элементом и его назначением.

- |                     |   |
|---------------------|---|
| 1. IP-адрес         | А. Точка взаимодействия процесса с сетью          |
| 2. Порт             | Б. Логический номер сетевой службы или приложения |
| 3. Сокет            | В. Идентификатор узла в сети                      |
| 4. Межсетевой экран | Г. Средство фильтрации сетевого трафика           |

№ 11 Прочитайте текст и запишите развернутый обоснованный ответ

Почему при установке и сопровождении системного программного обеспечения необходимо учитывать обновления, уязвимости и состояние средств защиты вычислительной системы?

№ 12 Прочитайте текст и установите соответствие

Установите соответствие между элементом системного программного обеспечения и проверяемым параметром.

- |                            |   |
|----------------------------|---|
| 1. Средство обновления     | А. Наличие установленных исправлений и актуальность компонентов |
| 2. Системная служба защиты | Б. Состояние запуска и корректность работы защитного механизма  |
| 3. Драйвер устройства      | В. Соответствие назначению устройства или системной функции     |

№ 13 Прочитайте текст и установите последовательность

Расположите действия в правильной последовательности при проверке состояния системного программного обеспечения после установки обновлений.

1. Определить, какие системные компоненты были изменены.
2. Проверить факт установки обновлений.
3. Проанализировать журналы событий на наличие ошибок.
4. Проверить состояние служб и драйверов после обновления.
5. Сделать вывод о корректности обновления и состоянии системы.
6. Проверить сохранность основных параметров безопасности и доступа.

№ 14 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Что является основной целью установки обновлений системного программного обеспечения?

**Варианты ответа:**

1. Исправление ошибок, уязвимостей и повышение стабильности работы системы
2. Изменение цвета рабочего стола
3. Создание пользовательских презентаций
4. Удаление всех системных журналов

№ 15 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие действия относятся к сопровождению системного программного обеспечения вычислительной системы?

**Варианты ответа:**

1. Проверка актуальности обновлений
2. Контроль состояния системных служб
3. Анализ журналов событий
4. Проверка прав доступа к системным объектам
5. Удаление учебных материалов пользователя без необходимости

**ОПК-7 - Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем**

№ 1 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой критерий является наиболее важным при выборе операционной системы для информационной системы?

**Варианты ответа:**

1. Назначение системы и требования к ее эксплуатации
2. Только внешний вид пользовательского интерфейса
3. Только размер установочного файла
4. Только наличие стандартных обоев рабочего стола

№ 2 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой инструмент наиболее уместен для анализа сетевого трафика вычислительной системы?

**Варианты ответа:**

1. Средство анализа сетевых пакетов

2. Графический редактор
3. Архиватор файлов
4. Программа для создания презентаций

№ 3 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой критерий наиболее важен при выборе системной платформы для информационной системы?

**Варианты ответа:**

1. Соответствие назначению системы, условиям эксплуатации и требованиям защищенности
2. Только внешний вид интерфейса
3. Только название операционной системы
4. Только размер установочного файла

№ 4 Прочитайте текст и запишите развернутый обоснованный ответ

Почему при выборе инструментов анализа состояния операционной системы необходимо учитывать не только удобство, но и полноту получаемых данных?

№ 5 Прочитайте текст и запишите развернутый обоснованный ответ

Какие параметры необходимо учитывать при выборе инструментов для комплексного анализа защищенности сетевого взаимодействия вычислительной системы?

№ 6 Прочитайте текст и установите последовательность

Расположите действия в правильной последовательности при выборе инструментального средства для анализа состояния операционной системы.

**Элементы последовательности:**

1. Определить цель анализа
2. Определить тип системных данных, которые необходимо получить
3. Сравнить доступные штатные и дополнительные инструменты
4. Оценить ограничения выбранного инструмента
5. Выбрать инструмент и обосновать выбор

№ 7 Прочитайте текст и установите последовательность

Расположите действия в правильной последовательности при выборе платформы для размещения сетевой службы.

**Элементы последовательности:**

1. Определить назначение сетевой службы
2. Определить требования к производительности, доступности и защищенности
3. Оценить совместимость службы с операционной системой
4. Проверить возможности журналирования, фильтрации трафика и управления доступом
5. Сравнить возможные платформы
6. Обосновать выбранное решение

№ 8 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие факторы необходимо учитывать при выборе системной платформы для информационной системы?

**Варианты ответа:**

1. Совместимость с используемым программным обеспечением
2. Требования к производительности
3. Возможности управления доступом и регистрации событий
4. Условия эксплуатации и сопровождения
5. Случайное предпочтение пользователя

№ 9 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие критерии важны при выборе средства фильтрации сетевого трафика?

**Варианты ответа:**

1. Возможность настройки правил входящего и исходящего трафика
2. Поддержка учета состояния соединений
3. Возможность ведения журналов событий фильтрации
4. Совместимость с используемой операционной системой
5. Наличие музыкального сопровождения интерфейса

№ 10 Прочитайте текст и запишите развернутый обоснованный ответ

Почему при выборе платформы для информационной системы необходимо учитывать возможности обновления, мониторинга, управления доступом и регистрации событий?

№ 11 Прочитайте текст и установите последовательность

Расположите действия в правильной последовательности при выборе системной платформы для защищенной информационной системы.

1. Сравнить доступные платформы по выбранным критериям.
2. Оценить поддержку обновлений, средств защиты и сетевых механизмов.
3. Обосновать выбор системной платформы.
4. Определить назначение информационной системы.
5. Определить требования к управлению доступом, журналированию и мониторингу.
6. Определить требования к производительности, совместимости и устойчивости.

№ 12 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие параметры следует учитывать при выборе системной платформы и инструментальных средств для информационной системы?

**Варианты ответа:**

1. Совместимость с используемым программным обеспечением
2. Поддержка обновлений и сопровождения
3. Возможности управления доступом и регистрации событий
4. Средства мониторинга и анализа состояния системы
5. Случайный выбор без учета назначения системы

№ 13 Прочитайте текст и установите соответствие

Установите соответствие между задачей и подходящим инструментальным средством.

- |                           |   |
|---------------------------|---|
| 1. Анализ процессов       | А. Журнал событий операционной системы              |
| 2. Анализ служб           | Б. Средства просмотра и управления процессами       |
| 3. Анализ прав доступа    | В. Средства управления службами                     |
| 4. Анализ событий системы | Г. Средства просмотра разрешений файлов и каталогов |

№ 14 Прочитайте текст и установите соответствие

Установите соответствие между задачей сетевого анализа и подходящим средством.

- |   |  |
|---|--|
| 1. Просмотр активных сетевых соединений | А. Средство просмотра параметров сертификата |
| 2. Анализ сетевых пакетов               | Б. Средство просмотра соединений и портов    |
| 3. Проверка сертификата TLS             | В. Средство анализа сетевого трафика         |

4. Проверка  
правил  
фильтрации  
трафика

Г. Средство управления межсетевым экраном

№ 15 Прочитайте текст и установите соответствие

Установите соответствие между требованием к информационной системе и критерием выбора системной платформы.

1.

Необходимость  
контроля  
действий  
пользователей

А. Наличие механизмов регистрации событий и аудита

2.

Необходимость  
защиты сетевого  
взаимодействия

Б. Поддержка фильтрации трафика и защищенных соединений

3.

Необходимость  
стабильной  
работы служб

В. Возможность управления системными службами и мониторинга состояния

4.

Необходимость  
своевременного  
устранения  
уязвимостей

Г. Наличие механизма обновлений и поддержки исправлений