

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Иркутский государственный университет путей сообщения»  
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА  
приказом ректора  
от «08» мая 2020 г. № 266-1

## Б1.Б.1.19 Безопасность операционных систем рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем

Специализация – Безопасность открытых информационных систем

Квалификация выпускника – специалист по защите информации

Форма обучения – очная

Нормативный срок обучения – 5 лет

Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 9

Формы промежуточной аттестации в семестрах:

Часов по учебному плану – 324

зачет (5), экзамен (6)

### Распределение часов дисциплины по семестрам

Семестр	5	6	Итого
Число недель в семестре	18	18	
Вид занятий	Часов по учебному плану	Часов по учебному плану	Часов по учебному плану
<b>Аудиторная контактная работа по видам учебных занятий</b>	<b>72</b>	<b>72</b>	<b>144</b>
– лекции	36	36	72
– практические (семинарские)	18	18	36
– лабораторные	18	18	36
<b>Самостоятельная работа</b>	<b>72</b>	<b>72</b>	<b>144</b>
<b>Экзамен</b>		<b>36</b>	<b>36</b>
<b>Итого</b>	<b>144</b>	<b>180</b>	<b>324</b>

ИРКУТСК

Электронный документ выгружен из ЕИС ФГБОУ ВО ИрГУПС и соответствует оригиналу

Подписант ФГБОУ ВО ИрГУПС Трофимов Ю.А.

00a73c5b7b623a969ccad43a81ab346d50 с 08.12.2022 14:32 по 02.03.2024 14:32 GMT+03:00

Подпись соответствует файлу документа



<b>1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ</b>	
<b>1.1 Цели освоения дисциплины</b>	
1	ознакомление с назначением, архитектурой и принципами функционирования современных операционных систем (ОС), методологией и практикой построения систем защиты информации в ОС
<b>1.2 Задачи освоения дисциплины</b>	
1	дать основы принципов функционирования ОС различной архитектуры;
2	оценить возможности штатных защитных механизмов обеспечения безопасности ОС;
3	изучить особенности методологии построения систем защиты информации в ОС;
4	освоить методы защиты от несанкционированного доступа к информации (НСДИ), обеспечения целостности и доступности информационных ресурсов ОС.
<b>1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины</b>	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.	
Цель достигается по мере решения в единстве следующих задач:	
– формирование сознательного отношения к выбранной профессии;	
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;	
– формирование психологии профессионала;	
– формирование профессиональной культуры, этики профессионального общения;	
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	

<b>2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП</b>	
<b>2.1 Требования к предварительной подготовке обучающегося</b>	
1	Б1.Б.1.13 Информатика
2	Б1.Б.1.22 Основы информационной безопасности
3	Б1.Б.1.24 Организация ЭВМ и вычислительных систем
4	Б1.Б.1.16 Языки программирования
<b>2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее</b>	
1	Б1.Б.1.20 Безопасность сетей ЭВМ
2	Б1.Б.1.21 Безопасность систем баз данных
3	Б1.Б.1.ДС.03 Информационная безопасность открытых систем
5	Б1.Б.1.28 Программно-аппаратные средства обеспечения информационной безопасности
6	Б1.Б.1.29 Разработка и эксплуатация защищенных автоматизированных систем
7	Б2.Б.02(П) Производственная – по получению профессиональных умений и опыта профессиональной деятельности
8	Б2.Б.03(П) Производственная - эксплуатационная
9	Б2.Б.05(П) Производственная - технологическая
10	Б2.Б.06(Пд) Производственная - преддипломная

<b>3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ</b>	
<b>ПК-23: способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа</b>	
<b>Минимальный уровень освоения компетенции</b>	
Знать	требования по обеспечению информационной безопасности (ИБ) ОС;
Уметь	оценить возможности штатных средств защиты ОС;
Владеть	навыками организации работ по формированию политики безопасности ОС;
<b>Базовый уровень освоения компетенции</b>	
Знать	возможности основных встроенных механизмов защиты ресурсов типовых ОС;
Уметь	оценить необходимость применения добавочных средств обеспечения ИБ ОС;
Владеть	навыками организации работ по реализации политики безопасности ОС;

<b>Высокий уровень освоения компетенции</b>	
Знать	особенности и порядок функционирования функционирующих встроенных механизмов защиты ресурсов типовых ОС.
Уметь	формировать общих принципов политики ИБ в организации;
Владеть	навыками формирования правил и процедур политики ИБ организации в части защиты ресурсов ОС;

<b>ПК-26: способность администрировать подсистему информационной безопасности автоматизированной системы</b>	
<b>Минимальный уровень освоения компетенции</b>	
Знать	основные штатные сервисы безопасности типовых ОС;
Уметь	администрировать штатные сервисы безопасности типовых ОС;
Владеть	основными навыками администрирования встроенных механизмов обеспечения ИБ ОС;
<b>Базовый уровень освоения компетенции</b>	
Знать	возможности подсистем администрирования штатных сервисов безопасности типовых ОС;
Уметь	выявлять уязвимости в настройках подсистем ОС, влияющие на уровень защищенности ОС;
Владеть	навыками анализа работы ОС и выявления наличия нештатных ситуаций;
<b>Высокий уровень освоения компетенции</b>	
Знать	детали функционирования сервисов безопасности типовых ОС;
Уметь	обеспечить эксплуатацию ОС при наличии средств защиты ресурсов;
Владеть	навыками настройки сервисов защиты ОС в соответствии с политикой ИБ.

**В результате освоения дисциплины обучающийся должен**

<b>Знать</b>	
1	назначение и функции ОС;
2	архитектуру и классификацию ОС;
3	функционирование подсистемы управления процессами ОС;
4	механизмы управление памятью ОС (в том числе вспомогательной);
5	организацию файловых систем ОС;
6	назначение и возможности систем клона UNIX, систем группы Windows;
7	основные механизмы безопасности: средства и методы аутентификации в ОС, модели разграничения доступа, организацию и использование средств аудита;
8	администрирование в ОС: задачи и принципы сопровождения системного программного обеспечения, генерацию, настройку, измерение производительности, управление безопасностью ОС;
9	критерии (стандарты) оценки эффективности и надежности средств защиты ОС;
10	принципы организации и структуру подсистем защиты ОС семейств Windows и UNIX..
<b>Уметь</b>	
1	администрировать современные ОС;
2	выявлять уязвимости ОС;
3	использовать средства ОС для обеспечения эффективного и безопасного функционирования АС;
4	оценивать эффективность и надежность защиты ОС.
<b>Владеть</b>	
1	навыками работы с современными ОС, восстановления ОС после сбоев;
2	навыками установки и настройки современных ОС с учетом требований по обеспечению ИБ;
3	навыками эксплуатации и администрирования ОС (в части, касающейся разграничения доступа, аутентификации и аудита);
4	навыками анализа защищенности ОС.

**4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	<b>Раздел 1. Назначение и функции ОС. Эволюция ОС</b>				
1.1	Функции ОС. Структура ОС /Лек/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
1.2	Архитектура вычислительных систем /Пр/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2

1.3	Поколения ОС /Ср/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
<b>Раздел 2. Классификация ОС</b>					
2.1	Особенности алгоритмов управления ресурсами; аппаратных платформ; областей использования; методов построения /Лек/	5	3	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
2.2	ОС MS-DOS /Пр/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
2.3	Линейка ОС Linux /Пр/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
2.4	Внутренние команды ОС MS-DOS. Утилиты. Пакетные файлы. Команды пакетного файла /Лаб/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
2.5	Создание пакетных файлов ОС MS-DOS /Лаб/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
2.6	Сетевые ОС /Ср/	5	8	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
<b>Раздел 3. Архитектура, современные концепции и технологии проектирования ОС</b>					
3.1	Расширяемость. Переносимость. Совместимость. Безопасность. Монолитные системы и микроядро. Многоуровневые системы/Лек/	5	3	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
3.2	Разделяемые ресурсы ОС /Пр/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
3.3	Понятие и реализация политики аудита /Пр/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
3.4	ОС Windows 7. Установка с компакт-диска, обновление, выявление ошибок установки /Лаб/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
3.5	Модели клиент-сервер. Множественные прикладные среды /Ср/	5	8	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
<b>Раздел 4. Управление процессами</b>					
4.1	Понятия процесса и потока. Планирование задач, обработка прерываний. Состояния процессов/потоков. Тупиковые ситуации, обработка исключений Синхронизация процессов/потоков, стратегии и дисциплины планирования, наследование ресурсов. /Лек/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
4.2	Обеспечение корректности совместного доступа к данным. Разделение кода и данных между процессами /Ср/	5	8	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
<b>Раздел 5. Управление памятью</b>					
5.1	Распределение памяти фиксированными разделами. Распределение памяти разделами переменной величины. Перемещаемые разделы. Понятие виртуальной памяти. Страничное распределение. Сегментное распределение. Странично-сегментное распределение/Лек/	5	6	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
5.2	Иерархия запоминающих устройств. Принцип кэширования данных /Ср/	5	12	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
<b>Раздел 6. Управление вводом-выводом</b>					
6.1	Физическая организация устройств ввода-вывода. Организация программного обеспечения ввода-вывода. Обработка прерываний. Драйверы устройств/Лек/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
6.2	Независимый от устройств слой ОС. Пользовательский слой программного обеспечения/Ср/	5	8	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2

	<b>Раздел 7. Файловые системы</b>				
7.1	Логическая организация файла. Физическая организация и адрес файла. Модели файловых систем/Лек/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
7.2	Современные архитектуры файловых систем /Ср/	5	8	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
	<b>Раздел 8. Семейство операционных систем Windows</b>				
8.1	Линейка ОС Windows. Концепции построения ОС Windows. Структура ОС Windows и обзор особенностей. Управление ресурсами. /Лек/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
8.2	Домены ОС Windows. Учетные записи пользователей и групп /Пр/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
8.3	Взлом паролей Windows NT и защита от взлома /Пр/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
8.4	Поиск программных закладок в заданной конфигурации ОС Windows /Пр/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
8.5	ОС Windows 7. Настройка среды: системных параметров, среды рабочего стола. /Лаб/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
8.6	Файловые системы ОС Windows /Ср/	5	8	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
	<b>Раздел 9. Семейство операционных систем UNIX</b>				
9.1	История и общая характеристика семейства ОС UNIX/Linux/ Управление процессами и памятью/ Файловые системы Система ввода-вывода./Лек/	5	4	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
9.2	Установка ОС Linux /Лаб/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
9.3	Базовый набор команд ОС UNIX (Linux). Основные команды работы с файлами /Лаб/	5	2	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
9.4	Коммерческие реализации ОС UNIX /Ср/	5	8	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
	<b>Раздел 10. Организация защиты ресурсов ОС</b>				
10.1	Типичные атаки на ОС. Понятие защищенной ОС. Защищенная ОС: административные меры защиты. Типовая архитектура подсистемы защиты ОС /Лек/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
10.2	Каноническая модель управления доступом. Структура диспетчера доступа. Модели управления доступом с взаимодействием субъектов доступа /Лек/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
10.3	Политика безопасности. Управление правами и привилегиями пользователей. Управление группами с ограниченными правами. Формулирование политики безопасности для заданных условий /Пр/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
10.4	Разработка защищенных приложений. Программное управление группами. Анализ привилегий пользователей /Пр/	6	2	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
10.5	Сканирование уязвимостей ОС Windows с помощью сканера безопасности. Способы устранения уязвимостей /Лаб/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
10.6	Локальная и доменная политики безопасности. Конфигурирование безопасности /Ср/	6	16	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3

	<b>Раздел 11. Основные механизмы безопасности ОС: средства и методы аутентификации, модели разграничения доступа, организация и использование средств аудита</b>				
11.1	Идентификация, аутентификация и авторизация субъектов доступа ОС. Модели разграничения доступа к объектам ОС. Политика аудита /Лек/	6	16	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
11.2	Симметричное шифрование и формирование ключа на основе пароля /Пр/	6	2	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
11.3	Цифровая подпись. Процедура оформления и проверки подписи /Пр/	6	2	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
11.4	Назначение прав пользователей в ОС Windows /Лаб/	6	2	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
11.5	Регистрация и аудит в ОС Windows /Лаб/	6	2	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
11.6	Шаблоны безопасности в ОС Windows /Лаб/	6	2	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
11.7	Требования и практическая реализация сервисов безопасности /Ср/	6	16	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
	<b>Раздел 12. Администрирование в ОС Windows и Unix</b>				
12.1	Защита в ОС Windows: права доступа и привилегии субъектов; маркер доступа; дескриптор защиты; алгоритм проверки прав доступа. /Лек/	6	5	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
12.2	Защита в ОС Windows: уровни подсистемы аутентификации; политика аудита /Лек/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
12.3	ОС Unix/Linux: защита файловой системы /Лек/	6	3	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
12.6	Реализации разграничения доступа в ОС Windows /Пр/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
12.7	Реализации разграничения доступа в ОС Linux /Пр/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
12.8	Настройка системы безопасности ОС Windows /Лаб/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
12.9	Настройка системы безопасности ОС Linux /Лаб/	6	4	ПК-23, ПК-26	Л1.2-Л1.4, Л1.2-Л1.4, Л2.3-Л2.7,

					ЛЗ.1, Л4.1, ЭЗЛ2.3- Л2.7, ЛЗ.1, Л4.1, ЭЗ
12.10	Оценка защищенности данной конфигурации ОС Windows: файловая система, реестр, список пользователей, политика безопасности в области паролей, политика аудита /Ср.	6	22	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, ЛЗ.1, Л4.1, ЭЗ
12.11	Задачи и принципы сопровождения системного программного обеспечения/Ср/	6	18	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, ЛЗ.1, Л4.1, ЭЗ
<b>Раздел 13. Аттестация</b>					
13.1	Подготовка к экзамену /Экзамен/	6	36	ПК-23, ПК-26	Л1.1-Л1.4, Л2.1-Л2.7, ЛЗ.1, Л 4.1, Э1-ЭЗ

### 5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине оформляется в виде приложения № 1 к рабочей программе дисциплины размещаются в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет.

### 6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

#### 6.1 Учебная литература

##### 6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
Л1.1	Online Training Solutions, Inc.	Операционная система Microsoft Windows XP: Учебная литература для ВУЗов; <a href="http://biblioclub.ru/index.php?page=book_red&amp;id=429091#">http://biblioclub.ru/index.php?page=book_red&amp;id=429091#</a>	М.: Национальный Открытый Университет «ИНТУИТ», 2016	100 % онлайн
Л1.2	Проскурин В.Г.	Защита в операционных системах: <a href="http://e.lanbook.com/books/element.php?pl1_id=63241">http://e.lanbook.com/books/element.php?pl1_id=63241</a>	Горячая линия-Телеком, 2014	100 % онлайн
Л1.3	Афанасьев А.А., Веденьев Л.Т., Воронцов А.А.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам; <a href="http://e.lanbook.com/books/element.php?pl1_id=5114">http://e.lanbook.com/books/element.php?pl1_id=5114</a> : для ВПО	Горячая линия-Телеком, 2012	100 % онлайн
Л1.4	Бирюков А.А.	Информационная безопасность: защита и нападение; <a href="http://e.lanbook.com/books/element.php?pl1_id=39990">http://e.lanbook.com/books/element.php?pl1_id=39990</a> : Учебник	М: ДМК Пресс, 2012	100 % онлайн

##### 6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
Л2.1	Гордеев А.В.	Операционные системы	М.: Питер, 2007	4

Л2.2	Столлинс В.	Операционные системы: внутреннее устройство и принципы проектирования	М.: Вильямс, 2004	4
Л2.3	Мартемьянов Ю.Ф., Яковлев Ал.В., Яковлев Ан.В.	Операционные системы. Концепции построения и обеспечения безопасности <a href="http://e.lanbook.com/books/element.php?p11_id=5176">http://e.lanbook.com/books/element.php?p11_id=5176</a>	М.: Горячая линия – Телеком, 2011	100 % онлайн
Л2.4	Мельников В.П., Клейменов С.А., Петраков А.М.	Информационная безопасность и защита информации	М.: Академия, 2007	3
Л2.5	Домарев В.В.	Безопасность информационных технологий. Системный подход	М.: DiaSoft, 2004	3
Л2.6	Щеглов А.Ю.	Защита компьютерной информации от несанкционированного доступа	СПб.: Наука и Техника, 2004	2
Л2.7	Вебер К., Бадур Г., Козлов С.Н.	Безопасность в Windows XP. Готовые решения сложных задач защиты компьютеров	М.: Диа – Софт, 2003	1
<b>6.1.3 Методические разработки</b>				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия, учебное пособие.	Иркутск: ИргУПС, 2013.	67
<b>6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине</b>				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
Л4.1	Завгородний В.И.	«Комплексная защита информации в компьютерных системах»	Личный кабинет	
<b>6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»</b>				
Э1	Материалы "Основы операционных систем"	<a href="http://paramax.susu.ru/study/OS">http://paramax.susu.ru/study/OS</a> .		
Э2	Материалы "Операционные системы"	<a href="http://hi-news.ru/tag/operacionnyye-sistemy">http://hi-news.ru/tag/operacionnyye-sistemy</a>		
Э3	Материалы «Комплексная защита информации в компьютерных системах»	<a href="http://padaread.com/">http://padaread.com/</a>		
<b>6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)</b>				
<b>6.3.1 Перечень базового программного обеспечения</b>				
6.3.1.1	ОС Microsoft Windows XP Professional with Service Pack 2, лицензия Open License, Количество - 427			
6.3.1.2	ОС Microsoft Windows 7			
6.3.1.3	Офисный пакет Microsoft Office 2010, OpenLicense, Количество - 155			
6.3.1.4	ОС Linux Mandrake (бесплатное программное обеспечение (ПО))			
6.3.1.5	ОС Linux SUSE (бесплатное ПО)			
6.3.1.6	ОС Linux Red Hat (бесплатное ПО)			
<b>6.3.2 Перечень специализированных средств и программного обеспечения</b>				
6.3.2.1	Сканер MBSA (бесплатное ПО);			
6.3.2.2	«Сканер-BC» (бесплатное ПО для вузов);			
6.3.2.3	Персональные идентификаторы ruToken;			
6.3.2.4	VirtualBox (бесплатное ПО)			
<b>6.3.3 Перечень информационных справочных систем</b>				
6.3.3.1	Информационно-справочная система КонсультантПлюс <a href="http://www.consultant.ru">http://www.consultant.ru</a>			

**7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ,  
НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА  
ПО ДИСЦИПЛИНЕ**



1	Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории.
2	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечена доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: MicrosoftOffice 2010, OpenOffice 3.0.1, 7-zip, BorlandDelphi 7, AbodeReaderXI, MicrosoftSecurityEssentials, а также специализированное ПО.
3	<p>Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС.</p> <p>Помещения для самостоятельной работы обучающихся:</p> <ul style="list-style-type: none"> <li>– читальные залы;</li> <li>– учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.</li> </ul>

<b>8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ</b>	
Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	<p>Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторной работе.</p>
Практические (семинарские) занятия	<p>Обобщение, расширение и углубление пройденного материала на лекции. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы, анализа литературных источников, публичного выступления и аргументации собственного мнения.</p> <p>Обсуждение вопросов, вызвавших затруднение, с преподавателем.</p> <p>Участие в дискуссиях.</p> <p>Контроль качества усвоения пройденного материала.</p>
Лабораторная работа	<p>Один из видов практической работы, проводимой с целью углубления и закрепления теоретических знаний, развития навыков самостоятельной деятельности. Включает подготовку необходимых программно-аппаратных средств, составление плана работы, ее проведение и написание отчета.</p>
<p>Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.</p>	

**Приложение 1 к рабочей программе по дисциплине  
Б1.Б.1.19 Безопасность операционных систем**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ  
для проведения текущего контроля успеваемости  
и промежуточной аттестации по дисциплине  
Б1.Б.1.19 «Безопасность операционных систем»**

## 1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Дисциплина «Безопасность операционных систем» участвует в формировании компетенций:

**ПК-23:** способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;

**ПК-26:** способность администрировать подсистему информационной безопасности автоматизированной системы.

**Таблица траекторий формирования у обучающихся компетенций ПК-23, ПК-26 при освоении образовательной программы**

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин/ практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-23	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Б1.Б.1.19 Безопасность операционных систем	5, 6	1
		Б1.Б.1.23 Криптографические методы защиты информации	7	2
		Б1.В.06 Комплексная защита в информационных системах персональных данных	9	3
		Б2.Б.06(Пд) Производственная - преддипломная	А	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	4
ПК-26	способность администрировать подсистему информационной безопасности автоматизированной системы	Б1.Б.1.19 Безопасность операционных систем	5, 6	1
		Б2.Б.02(П) Производственная - по получению профессиональных умений и опыта профессиональной деятельности	6	1
		Б1.Б.1.20 Безопасность сетей ЭВМ	6, 7	2
		Б1.Б.1.21 Безопасность систем баз данных	7, 8	2
		Б2.Б.03(П) Производственная - эксплуатационная	8	3
		Б1.Б.1.28 Программно-аппаратные средства обеспечения информационной безопасности	8, 9	4

**Таблица соответствия уровней освоения компетенций ПК-23, ПК-26**

**планируемым результатам обучения**

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-23	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Раздел 1. Назначение и функции ОС. Эволюция ОС. Раздел 2. Классификация ОС. Раздел 3. Архитектура, современные концепции и техно-	Минимальный уровень	Знать требования по обеспечению информационной безопасности (ИБ) операционных систем (ОС);
				Уметь оценить возможности штатных средств защиты ОС;
				Владеть навыками организации работ по формированию политики безопасности ОС.

		<p>логии проектирования ОС. Раздел 4. Управление процессами. Раздел 5. Управление памятью. Раздел 6. Управление вводом-выводом. Раздел 7. Файловые системы. Раздел 8. Семейство операционных систем Windows. Раздел 9. Семейство операционных систем UNIX. Раздел 10. Организация защиты ресурсов ОС. Раздел 11. Основные механизмы безопасности ОС: средства и методы аутентификации, модели разграничения доступа, организация и использование средств аудита. Раздел 12. Администрирование в ОС Windows и Unix.</p>	<p>Базовый уровень</p> <p>Высокий уровень</p>	<p>Знать возможности основных встроенных механизмов защиты ресурсов типовых ОС; Уметь оценить необходимость применения добавочных средств обеспечения ИБ ОС; Владеть навыками организации работ по реализации политики безопасности ОС.</p> <p>Знать особенности и порядок функционирования функционирующих встроенных механизмов защиты ресурсов типовых ОС. Уметь формировать общих принципов политики ИБ в организации; Владеть навыками формирования правил и процедур политики ИБ организации в части защиты ресурсов ОС</p>
ПК-26	способность администрировать подсистему информационной безопасности автоматизированной системы	<p>Раздел 1. Назначение и функции ОС. Эволюция ОС. Раздел 2. Классификация ОС. Раздел 3. Архитектура, современные концепции и технологии проектирования ОС. Раздел 4. Управление процессами. Раздел 5. Управление памятью. Раздел 6. Управление вводом-выводом. Раздел 7. Файловые системы. Раздел 8. Семейство операционных систем Windows. Раздел 9. Семейство операционных систем UNIX. Раздел 10. Организация защиты ресурсов ОС. Раздел 11. Основные механизмы без-</p>	<p>Минимальный уровень</p> <p>Базовый уровень</p> <p>Высокий уровень</p>	<p>Знать основные штатные сервисы безопасности типовых ОС; Уметь администрировать штатные сервисы безопасности типовых ОС; Владеть основными навыками администрирования встроенных механизмов обеспечения ИБ ОС.</p> <p>Знать возможности подсистем администрирования штатных сервисов безопасности типовых ОС; Уметь выявлять уязвимости в настройках подсистем ОС, влияющие на уровень защищенности ОС; Владеть навыками анализа работы ОС и выявления наличия нештатных ситуаций.</p> <p>Знать детали функционирования сервисов безопасности типовых ОС; Уметь обеспечить эксплуатацию ОС при наличии средств защиты ресурсов; Владеть навыками настройки сервисов защиты ОС в соответствии с политикой ИБ.</p>

		<p>опасности ОС:          средства и методы аутентификации, модели разграничения доступа, организация и использование средств аудита.          Раздел 12. Администрирование в ОС Windows и Unix.</p>		
--	--	--	--	--

**Программа контрольно-оценочных мероприятий  
за период изучения дисциплины**

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)	Наименование оценочного средства (форма проведения)
<b>5 семестр</b>				
1	2	Текущий контроль	Внутренние команды ОС MS-DOS. Утилиты. Пакетные файлы. Команды пакетного файла /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
2	4	Текущий контроль	Внутренние команды ОС MS-DOS. Утилиты. Пакетные файлы. Команды пакетного файла /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
3	6	Текущий контроль	Создание пакетных файлов ОС MS-DOS /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
4	8	Текущий контроль	Создание пакетных файлов ОС MS-DOS /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
5	10	Текущий контроль	ОС Windows 7. Установка с компакт-диска, обновление, выявление ошибок установки /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
6	12	Текущий контроль	ОС Windows 7. Настройка среды: системных параметров, среды рабочего стола. /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
7	14	Текущий контроль	ОС Windows 7. Настройка среды: системных параметров, среды рабочего стола. /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
8	16	Текущий контроль	Установка ОС Linux /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
9	18	Текущий контроль	Базовый набор команд ОС UNIX (Linux). Основные команды работы с файлами /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
10	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ПК-23, ПК-26 Сообщение, доклад (устно); наличие презентации
11	18	Промежуточная аттестация – зачет	Разделы 1 – 9 РПД	ПК-23, ПК-26 Собеседование (устно)
<b>6 семестр</b>				
1	2	Текущий контроль	Сканирование уязвимостей ОС Windows с помощью сканера безопасности. Способы устранения уязвимостей /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
2	4	Текущий контроль	Сканирование уязвимостей ОС Windows с помощью сканера безопасности. Способы устранения уязвимостей /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
3	6	Текущий контроль	Назначение прав пользователей в ОС Windows /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
4	8	Текущий контроль	Регистрация и аудит в ОС Windows /Лаб/	ПК-23, ПК-26 Защита лабораторной работы
5	10	Текущий контроль	Шаблоны безопасности в ОС	ПК-23, Защита лабораторной

			Windows /Лаб/	ПК-26	работы
6	12	Текущий контроль	Настройка системы безопасности ОС Windows /Лаб/	ПК-23, ПК-26	Защита лабораторной работы
7	14	Текущий контроль	Настройка системы безопасности ОС Windows /Лаб/	ПК-23, ПК-26	Защита лабораторной работы
8	16	Текущий контроль	Настройка системы безопасности ОС Linux /Лаб/	ПК-23, ПК-26	Защита лабораторной работы
9	18	Текущий контроль	Настройка системы безопасности ОС Linux /Лаб/	ПК-23, ПК-26	Защита лабораторной работы
10	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ПК-23, ПК-26	Сообщение, доклад (устно); наличие презентации
11	18	Тест	Разделы 1 – 12 РПД	ПК-23, ПК-26	Перечень тестовых заданий
12	18	Промежуточная аттестация – экзамен	Разделы 1 – 12 РПД	ПК-23, ПК-26	Собеседование (устно)

## 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите
2	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений

3	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к зачету
5	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к экзамену

**Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета и экзамена, а также шкала для оценивания уровня освоения компетенций**

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенций
«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

**Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости**

### Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash-презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash-презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

### Тест (структура теста по компетенциям)

Проверяемый уровень освоения компетенции компетенций (части компетенций, элементов компетенций)	Минимальное количество тестовых заданий на один раздел программы	Рекомендуемые формы тестовых заданий	Количество баллов за одно тестовое задание
Минимальный уровень освоения компетенции	19	Тестовые задания с выбором одного правильного ответа из нескольких	1
		Тестовые задания с выбором нескольких правильных ответов из множества ответов	
		Тестовые задания на установление соответствия	
		Тестовые задания на установление правильной последовательности	
Базовый уровень освоения компетенции	8	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)	4
Высокий уровень освоения компетенции	6	Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы	7

### Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся при тестировании набрал 86-93 баллов
«хорошо»		Обучающийся при тестировании набрал 69-85 баллов
«удовлетворительно»		Обучающийся при тестировании набрал 53-68 баллов



«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-52 баллов	Компетенция не сформирована
-----------------------	--------------	---	-----------------------------

### Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний.  Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами.  Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»	Лабораторная работа выполнена с задержкой, письменный отчет с недочетами.  Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	Лабораторная работа не выполнена, письменный отчет не представлен.  Результаты, полученные обучающимся не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений.  Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

## 3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

### 3.1 Перечень типовых тем докладов, сообщений

1. Архитектура вычислительных систем.
2. ОС MS-DOS.
3. Линейка ОС Linux.
4. Домены ОС Windows. Учетные записи пользователей и групп.
5. Взлом паролей Windows NT и защита от взлома.
6. Поиск программных закладок в заданной конфигурации ОС Windows.
7. Политика безопасности. Управление правами и привилегиями пользователей. Управление группами с ограниченными правами. Формулирование политики безопасности для заданных условий.
8. Разработка защищенных приложений. Программное управление группами. Анализ привилегий пользователей.
9. Симметричное шифрование и формирование ключа на основе пароля.
10. Цифровая подпись. Процедура оформления и проверки подписи.

11. Реализации разграничения доступа в ОС Windows.

12. Реализации разграничения доступа в ОС Linux.

### 3.2. Тест

1. «Несанкционированный доступ к информации» - это:
  - доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
  - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;
  - доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;
  - доступ к информации, реализуемый путём уничтожения технических средств информационной системы.
2. При реализации системой защиты мандатного принципа контроля доступа субъект осуществляет запись в объект, только если классификационный уровень субъекта \_\_\_\_\_, чем классификационный уровень объекта:
  - больше;
  - меньше;
  - не больше;
  - не меньше.
3. Средство, осуществляющее перехват всех обращений субъектов к объектам и разграничивающее доступ, называется \_\_\_\_\_ :
  - монитором безопасности субъектов;
  - диспетчером доступа;
  - диспетчером учетных записей безопасности.
4. При реализации системой защиты мандатного принципа контроля доступа субъект может читать объект, только если иерархическая классификация субъекта \_\_\_\_\_, чем иерархическая классификация объекта:
  - больше;
  - меньше;
  - не больше;
  - не меньше.
5. Начиная с класса \_\_\_\_\_ требований ГТК РФ по защите информации в многопользовательских АС с различным уровнем доступа, необходимо управление потоками информации:
  - 1Г
  - 2Б
  - 1В
  - 3А
  - 1Б
  - 2А
  - 3Б
6. Какие из приведенных ниже терминов являются синонимами?
  - привилегированный режим
  - защищенный режим
  - режим супервизора
  - пользовательский режим
  - реальный режим
  - режим ядра

7. Известно, что программа А выполняется в монопольном режиме за 10 минут, а программа В — за 20 минут, т.е., при последовательном выполнении они требуют 30 минут. Если Т — время выполнения обеих этих задач в режиме мультипрограммирования, то какое из неравенств, приведенных ниже, справедливо?
- A)  $T < 10$
  - B)  $10 < T < 20$
  - C)  $20 < T < 30$
  - D)  $T > 30$ .
8. Какой из следующих методов распределения памяти может рассматриваться как частный случай виртуальной памяти?
- распределение фиксированными разделами
  - распределение динамическими разделами
  - страничное распределение
  - сегментное распределение
  - сегментно-страничное распределение.
9. Операционная система выделяет файлам пространство на диске:
- секторами
  - дорожками
  - кластерами
  - цилиндрами
10. Порядок регистрации событий аудита в ОС WinNT при доступе субъектов к данному объекту определяется с помощью списка \_\_\_\_\_ :
- SACL
  - DACL.
11. Если в ОС WinNT список избирательного контроля доступа имеется, но пуст, то:
- всем субъектам предоставляются все права доступа к объекту
  - доступ к объекту запрещен всем субъектам
  - доступ разрешен только членам группы администраторов.
12. В ОС WinNT процесс WinLogon.exe находится на \_\_\_\_\_ уровне подсистемы аутентификации:
- верхнем
  - среднем
  - нижнем.
13. Для ОС UNIX используются следующий способ кодирования строки матрицы доступа:
- вектор доступа
  - список доступа/
14. При монтировании файловой системы суперблок в ОС UNIX записывается в оперативную память по команде:
- unmount
  - root
  - setgit
  - mount
15. При аутентификации в ОС WinNT провайдер передает учетную информацию пользователя на средний уровень подсистемы аутентификации с помощью системного вызова \_\_\_\_\_ :
- Userlnit
  - LogonUser
  - msv1\_0.
16. Должна ли с точки зрения безопасности ОС предоставляться привилегия работы с подсистемой аудита администраторам?
- Нет
  - Да

17. Информация о привилегиях пользователя ОС содержится:
  - в дескрипторе защиты
  - в журнале безопасности
  - в маркере доступа.
18. Следующий метод доступа в ОС WinNT является стандартным и поддерживается для объектов всех типов:
  - ACCESS SYSTEM SECURITY
  - Создание поддиректории
  - Получение контекста.
19. Защищает ли изолированная программная среда от утечки информации?
  - Нет
  - Да.
20. В ОС WinNT \_\_\_\_\_ (дескриптор) защиты объекта содержит, в частности, следующую информацию:
  - список избирательного контроля доступа
  - идентификатор сеанса работы пользователя
  - идентификатор владельца объекта.
21. С помощью системной переменной \_\_\_\_\_ (umask) в ОС UNIX устанавливаются по умолчанию права доступа к файлу при его создании.
22. Локальный распорядитель безопасности LSA в ОС WinNT представляет собой процесс по имени \_\_\_\_\_ (lsass.exe).
23. В ОС UNIX \_\_\_\_\_ (индексный) дескриптор содержит информацию, необходимую для того, чтобы любой процесс имел возможность обратиться к файлу.
24. На нижнем уровне подсистемы аутентификации ОС WinNT для извлечения учетной информации из реестра локального компьютера используется \_\_\_\_\_ (SAM, Security Account Manager).
25. В ОС UNIX механизм SUID/SGID позволяет пользователю запустить программу от имени \_\_\_\_\_ (другого) пользователя.
26. Если в ОС UNIX четвертый бит, определяющий права на выполнение исполняемого файла, установлен в группе битов прав доступа владельца (setuid), то данная программа выполняется для любого пользователя с правами \_\_\_\_\_ (владельца).
27. Процесс назначения прав пользователю, успешно прошедшему процедуру аутентификации, называется \_\_\_\_\_ (авторизацией).
28. Дайте краткую характеристику понятию «привилегия пользователя».
29. Дайте краткую характеристику понятию «маркер пользователя».
30. Для какой цели используется дескриптор защиты объекта в ОС WinNT?
31. Коротко охарактеризуйте базовые требования к политике аудита в ОС.
32. Опишите структуру индексного дескриптора в ОС Linux.
33. Приведите основные методы подбора (компрометации) паролей в ОС.

### **3.3. Перечень теоретических вопросов к зачету**

1. Функции ОС.
2. Структура ОС.
3. Особенности алгоритмов управления ресурсами; аппаратных платформ; областей использования; методов построения.
4. Расширяемость ОС. Переносимость ОС. Совместимость ОС.
5. Безопасность. Монолитные системы и микроядро. Многоуровневые системы.
6. Понятия процесса и потока.
7. Планирование задач, обработка прерываний.

8. Состояния процессов/потоков.
9. Тупиковые ситуации, обработка исключений.
10. Синхронизация процессов/потоков, стратегии и дисциплины планирования, наследование ресурсов.
11. Обеспечение корректности совместного доступа к данным.
12. Распределение памяти фиксированными разделами.
13. Распределение памяти разделами переменной величины. Перемещаемые разделы.
14. Понятие виртуальной памяти.
15. Страничное распределение .
16. Сегментное распределение.
17. Странично-сегментное распределение.
18. Иерархия запоминающих устройств. Принцип кэширования данных
19. Организация программного обеспечения ввода-вывода. Обработка прерываний. Драйверы устройств.
20. Логическая организация файла.
21. Физическая организация и адрес файла. Модели файловых систем.
22. Линейка ОС Windows. Структура ОС Windows и обзор особенностей.
23. Файловые системы ОС Windows.
24. История и общая характеристика семейства ОС UNIX/Linux/

### **3.4. Перечень типовых простых практических заданий к зачету**

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

### **3.5. Перечень типовых практических заданий к зачету**

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

### **3.6. Перечень теоретических вопросов к экзамену**

1. Функции ОС.
2. Структура ОС.
3. Особенности алгоритмов управления ресурсами; аппаратных платформ; областей использования; методов построения.
4. Расширяемость ОС. Переносимость ОС. Совместимость ОС.
5. Безопасность. Монолитные системы и микроядро. Многоуровневые системы.
6. Понятия процесса и потока.
7. Планирование задач, обработка прерываний.
8. Состояния процессов/потоков.
9. Тупиковые ситуации, обработка исключений.
10. Синхронизация процессов/потоков, стратегии и дисциплины планирования, наследование ресурсов.
11. Обеспечение корректности совместного доступа к данным.
12. Распределение памяти фиксированными разделами.
13. Распределение памяти разделами переменной величины. Перемещаемые разделы.
14. Понятие виртуальной памяти.
15. Страничное распределение .
16. Сегментное распределение.
17. Странично-сегментное распределение.
18. Иерархия запоминающих устройств. Принцип кэширования данных.

19. Организация программного обеспечения ввода-вывода. Обработка прерываний. Драйверы устройств.
20. Логическая организация файла.
21. Физическая организация и адрес файла. Модели файловых систем.
22. Линейка ОС Windows. Структура ОС Windows и обзор особенностей.
23. Файловые системы ОС Windows.
24. История и общая характеристика семейства ОС UNIX/Linux/
25. Типичные атаки на ОС.
26. Понятие защищенной ОС. Защищенная ОС: административные меры защиты.
27. Типовая архитектура подсистемы защиты ОС.
28. Каноническая модель управления доступом. Структура диспетчера доступа.
29. Модели управления доступом с взаимодействием субъектов доступа.
30. Идентификация, аутентификация и авторизация субъектов доступа ОС.
31. Модели разграничения доступа к объектам ОС.
32. Политика аудита.
33. Защита в ОС Windows: права доступа и привилегии субъектов.
34. Защита в ОС Windows: маркер доступа; дескриптор защиты.
35. Защита в ОС Windows: алгоритм проверки прав доступа к объекту.
36. Защита в ОС Windows: уровни подсистемы аутентификации;
37. Защита в ОС Windows: политика аудита.
38. ОС Unix/Linux: защита файловой системы.

### 3.7. Перечень типовых простых практических заданий к экзамену

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

## 4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Сообщение, доклад	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Защита лабораторной работы	Обучаемый самостоятельно, под руководством преподавателя выполняет лабораторную работу на заданную тему. Тема (задание) предлагается в конкретном виде. Методы и инструменты для ее разработки предлагаются преподавателем. После выполнения задания обучаемый готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования (защиты). Оценка

	ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
--	---

Для организации и проведения промежуточной аттестации (в форме зачета/экзамена) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

- перечень теоретических вопросов к зачету/экзамену для оценки знаний;
- перечень типовых простых практических заданий к зачету/экзамену для оценки умений;
- перечень типовых практических заданий к зачету/экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету/экзамену обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

### **Описание процедур проведения промежуточной аттестации в форме зачета и оценивания результатов обучения**

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

### **Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)**

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Оценка
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

### **Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения**

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что в каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к эк-


замену); третье практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления.

### Образец экзаменационного билета

	<b>Экзаменационный билет № 1</b>  по дисциплине « _____ » _____ семестр	Утверждаю: Заведующий кафедрой « _____ » ИрГУПС _____
1. .... 2. .... 3. .... 4. .... 5. .... Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм		

В разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы» приведены типовые контрольные задания, для оценки результатов освоения образовательной программы. Задания, по которым проводятся контрольно-оценочные мероприятия, оформляются в соответствии с формами оформления оценочных средств, приведенными ниже, и не выставляются в электронную информационно-образовательную среду ИрГУПС, а хранятся на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.