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.В.04 Безопасность операционных систем

рабочая программа дисциплины

Направление подготовки – 10.03.01 Информационная безопасность
Профиль – "Безопасность автоматизированных систем"
Квалификация выпускника – бакалавр
Форма обучения – очная
Нормативный срок обучения – 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 8
Часов по учебному плану – 288

Формы промежуточной аттестации в семестрах:
экзамен (5), курсовая работа

Распределение часов дисциплины по семестрам

Семестр	5	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**126**	**126**
– лекции	54	**54**
– практические (семинарские)	36	**36**
– лабораторные	36	**36**
Самостоятельная работа	**126**	**126**
Экзамен	**36**	**36**
Итого	**288**	**288**

ИРКУТСК

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цели освоения дисциплины

1	ознакомление с назначением, архитектурой и принципами функционирования современных операционных систем (ОС), методологией и практикой построения систем защиты информации в ОС

1.2 Задачи освоения дисциплины

1	освоить основы функционирования базовых механизмов ОС;
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.

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Научно-образовательное воспитание обучающихся

Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.

Цель достигается по мере решения в единстве следующих задач:
– формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности;
– создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками;
– популяризация научных знаний среди обучающихся;
– содействие повышению привлекательности науки, поддержка научно-технического творчества;
– создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества;
– совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности

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 психологи профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1 Требования к предварительной подготовке обучающегося

1	Б1.Б.07 Информатика
2	Б1.Б.11 Основы информационной безопасности
3	Б1.Б.12 Аппаратные средства вычислительной техники
4	Б1.Б.19 Языки программирования
5	Б1.В.02 Теоретические основы компьютерной безопасности
6	Б1.В.ДВ.03.01 Основы программирования

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б1.Б.13 Программно-аппаратные средства защиты информации
2	Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем
3	Б1.В.03 Безопасность вычислительных сетей
4	Б1.В.05 Комплексная защита в информационных системах персональных данных
5	Б1.В.06 Безопасность систем баз данных
6	Б1.В.08 Методология построения защищенных автоматизированных систем

7	Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта
8	Б1.В.ДВ.06.01 Информационная безопасность открытых систем
9	Б2.В.03(П) Производственная практика - эксплуатационная
	Б2.В.04(Пд) Производственная практика - преддипломная

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

Минимальный уровень освоения компетенции	
Знать	возможности основных встроенных механизмов защиты ресурсов типовых ОС;
Уметь	выполнять работы по установке ОС, имеющей в своем составе подсистему защиты ресурсов;
Владеть	навыками эксплуатации подсистемы управления механизмов защиты ОС на уровне системного администратора.
Базовый уровень освоения компетенции	
Знать	методы настройки параметров подсистемы защиты информации ОС;
Уметь	выполнять работы по настройке ОС, имеющей в своем составе подсистему защиты ресурсов;
Владеть	навыками эксплуатации подсистемы управления механизмов защиты ОС в составе группы сопровождения.
Высокий уровень освоения компетенции	
Знать	методики технического сопровождения функционирования подсистемы защиты ОС,
Уметь	выполнять работы по эксплуатации ОС, имеющей в своем составе подсистему защиты ресурсов;
Владеть	навыками самостоятельной эксплуатации подсистемы управления механизмов защиты ОС на уровне администратора безопасности.

ПСК4-2: способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей

Минимальный уровень освоения компетенции	
Знать	основные штатные сервисы безопасности типовых ОС;
Уметь	администрировать штатные сервисы безопасности типовых ОС;
Владеть	основными навыками администрирования встроенных механизмов обеспечения ИБ ОС;
Базовый уровень освоения компетенции	
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;
Высокий уровень освоения компетенции	
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

Знать	
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/Linux, 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/Linux.
Уметь	
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.
Владеть	
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»
	Раздел 1. Назначение и функции ОС. Эволюция ОС				
1.1	Функции ОС. Структура ОС /Лек/	5	2	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
	Раздел 2. Классификация ОС				
2.1	Особенности алгоритмов управления ресурсами; аппаратных платформ; областей использования; методов построения /Лек/	5	2	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
	Раздел 3. Архитектура, современные концепции и технологии проектирования ОС				
3.1	Расширяемость. Переносимость. Совместимость. Безопасность. Монолитные системы и микроядро.Многоуровневые системы/Лек/	5	2	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
	Раздел 4. Управление процессами				
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	3	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
	Раздел 5. Управление памятью				
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	4	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
	Раздел 6. Управление вводом-выводом				
6.1	Физическая организация устройств ввода-вывода. Организация программного обеспечения ввода-вывода. Обработка прерываний. Драйверы устройств/Лек/	5	3	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
	Раздел 7. Файловые системы				
7.1	Логическая организация файла. Физическая организация и адрес файла. Модели файловых систем/Лек/	5	3	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
	Раздел 8. Семейство операционных систем Windows				
8.1	Линейка ОС Windows. Концепции построения ОС Windows. Структура ОС Windows и обзор особенностей. Управление ресурсами. /Лек/	5	2	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
	Раздел 9. Семейство операционных систем UNIX/Linux				
9.1	История и общая характеристика семейства ОС UNIX/Linux/ Управление процессами и памятью/ Файловые системы Система ввода-вывода./Лек/	5	2	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 /Linux/Ср/	5	18	ПК-23, ПК-26	Л1.1, Л2.1-Л2.3, Э1, Э2
	Раздел 10. Организация защиты ресурсов ОС				

10.1	Типичные атаки на ОС. Понятие защищенной ОС. Защищенная ОС: административные меры защиты.Типовая архитектура подсистемы защиты ОС /Лек/	5	2	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/	5	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/	5	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/	5	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/	5	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/	5	14	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
	Раздел 11. Основные механизмы безопасности ОС: средства и методы аутентификации, модели разграничения доступа, организация и использование средств аудита				
11.1	Идентификация, аутентификация и авторизация субъектов доступа ОС. Модели разграничения доступа к объектам ОС. Политика аудита /Лек/	5	13	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/	5	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/	5	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/	5	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/	5	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/	5	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/	5	15	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
	Раздел 12. Администрирование в ОС Windows и Unix/Linux				
12.1	Защита в ОС Windows: права доступа и привилегии субъектов; маркер доступа; дескриптор защиты; алгоритм проверки	5	5	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1,

	прав доступа. /Лек/				Э3
12.2	Защита в ОС Windows: уровни подсистемы аутентификации; политика аудита /Лек/	5	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/	5	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/	5	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/	5	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/	5	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/	5	4	ПК-23, ПК-26	Л1.2-Л1.4, Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3Л2.3-Л2.7, Л3.1, Л4.1, Э3
12.10	Оценка защищенности данной конфигурации ОС Windows: файловая система, реестр, список пользователей, политика безопасности в области паролей, политика аудита /Ср.	5	22	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
12.11	Задачи и принципы сопровождения системного программного обеспечения/Ср/	5	15	ПК-23, ПК-26	Л1.2-Л1.4, Л2.3-Л2.7, Л3.1, Л4.1, Э3
	Раздел 13. Аттестация				
13.1	Подготовка к экзамену /Экзамен/	5	36	ПК-23, ПК-26	Л1.1-Л1.4, Л2.1-Л2.7, Л3.1, Л 4.1, Э1-Э3

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 дисциплиныи 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; http://biblioclub.ru/index.php?page=book_red&id=429091#	М.: Национальный Открытый Университет «ИНТУИТ», 2016	100 % онлайн
Л1.2	Проскурин В.Г.	Защита в операционных системах: http://e.lanbook.com/books/element.php?pl1_id=63241	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; http://e.lanbook.com/books/element.php?pl1_id=5114: для ВПО	Горячая линия-Телеком, 2012	100 % онлайн
Л1.4	Бирюков А.А.	Информационная безопасность: защита и нападение; http://e.lanbook.com/books/element.php?pl1_id=39990: 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	Столлингс 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 http://e.lanbook.com/books/element.php?pl1_id=5176	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
6.1.3 Методические разработки				
	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
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	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	
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э1	Материалы "Основы операционных систем"		http://paramax.susu.ru/study/OS.	

Э2	Материалы "Операционные системы"	http://hi-news.ru/tag/operacionnye-sistemy
Э3	Материалы «Комплексная защита информации в компьютерных системах»	http://padaread.com/

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)	
6.3.1 Перечень базового программного обеспечения	
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)
6.3.2 Перечень специализированных средств и программного обеспечения	
6.3.2.1	Сканер MBSA (бесплатное ПО);
6.3.2.2	«Сканер-ВС» (бесплатное ПО для вузов);
6.3.2.3	Персональные идентификаторы ruToken;
6.3.2.4	VirtualBox (бесплатное ПО)
6.3.3 Перечень информационных справочных систем	
6.3.3.1	Информационно-справочная система КонсультантПлюсhttp://www.consultant.ru

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	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать 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 удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторной работе.
Практические (семинарские) занятия	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. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в дискуссиях. Контроль качества усвоения пройденного материала.
Лабораторная	Один из видов практической работы, проводимой с целью углубления и закрепления

работа	теоретических знаний, развития навыков самостоятельной деятельности. Включает подготовку необходимых программно-аппаратных средств, составление плана работы, ее проведение и написание отчета.
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.	

Приложение 1 к рабочей программе по дисциплине
Б1.В.04 Безопасность операционных систем

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине
Б1.В.04 «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-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
ПСК4-2: способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей.

Таблица траекторий формирования у обучающихся компетенций ПК-1, ПК4-2 при освоении образовательной программы

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин/ практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Б1.Б.12 Аппаратные средства вычислительной техники	1	1
		Б1.Б.17 Сети и системы передачи информации	4	2
		Б1.Б.23 Электроника и схемотехника	4	2
		Б1.Б.16 Техническая защита информации	5	2
		Б1.В.04 Безопасность операционных систем	5	2
		Б1.Б.14 Криптографические методы защиты информации	6	3
		Б2.В.03(П) Производственная практика - эксплуатационная	6	3
		Б1.Б.13 Программно-аппаратные средства защиты информации	7	4
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	4
ПК4-2	способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Б1.Б.17 Сети и системы передачи информации	4	1
		Б1.В.04 Безопасность операционных систем	5	2
		Б1.В.ДВ.05.01 Системы управления базами данных	5	2
		Б1.В.ДВ.05.02 Средства сетевых систем управления базами данных	5	2
		Б1.В.ДВ.09.02 Администрирование систем баз данных	5	2
		Б1.В.03 Безопасность вычислительных сетей	7	3
		Б1.В.06 Безопасность систем баз данных	8	4
		Б1.В.ДВ.06.01 Информационная безопасность открытых систем	8	4
		Б1.В.ДВ.06.02 Сетевое администрирование	8	4
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	4

Таблица соответствия уровней освоения компетенций ПК-1, ПСК4-2 планируемым результатам обучения

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	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 безопасности ОС: средства и методы аутентификации, модели разграничения доступа, организация и использование средств аудита. Раздел 12. Администрирование в ОС Windows и Unix.	Минимальный уровень	Знать возможности основных встроенных механизмов защиты ресурсов типовых ОС;
				Уметь выполнять работы по установке ОС, имеющей в своем составе подсистему защиты ресурсов;
				Владеть навыками эксплуатации подсистемы управления механизмов защиты ОС на уровне системного администратора.
			Базовый уровень	Знать методы настройки параметров подсистемы защиты информации ОС;
				Уметь выполнять работы по настройке ОС, имеющей в своем составе подсистему защиты ресурсов;
				Владеть навыками эксплуатации подсистемы управления механизмов защиты ОС в составе группы сопровождения.
			Высокий уровень	Знать методики технического сопровождения функционирования подсистемы защиты ОС,
				Уметь выполнять работы по эксплуатации ОС, имеющей в своем составе подсистему защиты ресурсов;
				Владеть навыками самостоятельной эксплуатации подсистемы управления механизмов защиты ОС на уровне администратора безопасности.
ПК4-2	способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Раздел 1. Назначение и функции ОС. Эволюция ОС. Раздел 2. Классификация ОС. Раздел 3. Архитектура, современные концепции и технологии проектирования ОС. Раздел 4. Управле-	Минимальный уровень	Знать основные штатные сервисы безопасности типовых ОС;
				Уметь администрировать штатные сервисы безопасности типовых ОС;
				Владеть основными навыками администрирования встроенных механизмов обеспечения ИБ ОС;
			Базовый уровень	Знать возможности подсистем администрирования штатных сервисов безопасности типовых

		ние 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.		ОС;
				Уметь выявлять уязвимости в настройках подсистем ОС, влияющие на уровень защищенности ОС;
				Владеть навыками анализа работы ОС и выявления наличия нештатных ситуаций;
			Высокий уровень	Знать методики технического сопровождения функционирования подсистемы защиты ОС,
				Уметь выполнять работы по эксплуатации ОС, имеющей в своем составе подсистему защиты ресурсов;
				Владеть навыками самостоятельной эксплуатации подсистемы управления механизмов защиты ОС на уровне администратора безопасности.

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)
5 семестр					
1	1	Текущий контроль	Внутренние команды ОС MS-DOS. Утилиты. Пакетные файлы. Команды пакетного файла /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
2	2	Текущий контроль	Внутренние команды ОС MS-DOS. Утилиты. Пакетные файлы. Команды пакетного файла /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
3	3	Текущий контроль	Создание пакетных файлов ОС MS-DOS /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
4	4	Текущий контроль	Создание пакетных файлов ОС MS-DOS /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
5	5	Текущий контроль	ОС Windows 7. Установка с компакт-диска, обновление, выявление ошибок установки /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
6	6	Текущий контроль	ОС Windows 7. Настройка среды: системных параметров, среды рабочего стола. /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
7	7	Текущий контроль	ОС Windows 7. Настройка среды: системных параметров, среды рабочего стола. /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
8	8	Текущий контроль	Установка ОС Linux /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы

9	9	Текущий контроль	Базовый набор команд ОС UNIX (Linux). Основные команды работы с файлами /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
10	10	Текущий контроль	Сканирование уязвимостей ОС Windows с помощью сканера безопасности. Способы устранения уязвимостей /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
11	11	Текущий контроль	Сканирование уязвимостей ОС Windows с помощью сканера безопасности. Способы устранения уязвимостей /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
12	12	Текущий контроль	Назначение прав пользователей в ОС Windows /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
13	13	Текущий контроль	Регистрация и аудит в ОС Windows /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
14	14	Текущий контроль	Шаблоны безопасности в ОС Windows /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
15	15	Текущий контроль	Настройка системы безопасности ОС Windows /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
16	16	Текущий контроль	Настройка системы безопасности ОС Windows /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
17	17	Текущий контроль	Настройка системы безопасности ОС Linux /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
18	18	Текущий контроль	Настройка системы безопасности ОС Linux /Лаб/	ПК-1, ПСК4-2	Защита лабораторной работы
19	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ПК-1, ПСК4-2	Сообщение, доклад (устно); наличие презентации
20	18	Текущий контроль	Защита курсовой работы	ПК-1, ПСК4-2	Курсовая работа
21	18	Промежуточная аттестация – экзамен	Разделы 1 – 12 РПД	ПК-1, ПСК4-2	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	Краткая характеристика оценочного средства	Представление оценочного

	средства		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
5	Курсовая работа	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Темы типовых групповых и / или индивидуальных проектов и типовое задание на курсовую работу
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 неточностя-	Минимальный

	ми 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	
«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

Курсовая работа

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество

	грамматических и/или стилистических ошибок. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсового проекта (работы) обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсовой работы в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. Программа не разработана и/или находится в нерабочем состоянии. При защите курсовой работыобучающийся демонстрирует слабое понимание программного материала. Курсовой работы не представлена преподавателю. Обучающийся не явился на защиту курсовой работы.

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 (структура теста по компетенциям)

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенции

«отлично»	«зачтено»	Обучающийся при тестировании набрал 86-93 баллов	Высокий
«хорошо»		Обучающийся при тестировании набрал 69-85 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 53-68 баллов	Минимальный
«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.

3.4. Перечень тем курсовых работ

1-25. Организация защищенных рабочих мест сотрудников подразделений производственного предприятия.

Количество различных подразделений равняется количеству обучающихся (см. методические указания).

3.5. 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.
Курсовая работа	Обучаемый самостоятельно, под руководством преподавателя выполняет курсовую работу на заданную тему. Тема предлагается в общем виде. Конкретные методы и инструменты для ее разработки обучаемый выбирает самостоятельно. Обучаемый подбирает литературу по теме, не менее 3-4 источников, включая самостоятельный поиск в интернет (обязательно), разрабатывает ее, готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования. 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 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 экзамену); 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

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **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.