

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таскаев Сергей Васильевич

Должность: Ректор

Дата подписания: 15.09.2025 11:03:21

Уникальный программный ключ:

04c19ed8bfb98f3b6cb77a486b9a8788b8522525

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)

Математический факультет

Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»

по специальности 10.05.01 Компьютерная безопасность

специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 1

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

**Фонд оценочных средств  
для промежуточной аттестации  
по дисциплине  
Защита в операционных системах**

Направление подготовки (специальность)  
10.05.01 Компьютерная безопасность

Направленность (профиль)  
специализация № 6 «Информационно-аналитическая и техническая  
экспертиза компьютерных систем»

Присваиваемая квалификация  
специалист по защите информации

Форма обучения  
очная

Челябинск 2025 г.



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 2

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

## Содержание

1. Паспорт фонда оценочных средств
2. Перечень формируемых компетенций
  - 2.1. Компетенции, закреплённые за дисциплиной
3. Содержание оценочных средств по дисциплине
  - 3.1. Виды оценочных средств
  - 3.2. Содержание оценочных средств
4. Порядок проведения и критерии оценивания промежуточной аттестации
  - 4.1. Порядок проведения промежуточной аттестации
  - 4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств
  - 4.3. Результаты промежуточной аттестации и уровни сформированности компетенций



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 3

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_

## 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.

Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».

Дисциплина: **Защита в операционных системах.**

Семестр (семестры) изучения: 8,9 семестры.

Форма (формы) промежуточной аттестации:

зачёт 8 семестр, экзамен 9 семестр.

Используется балльно-рейтинговая система для оценивания результатов.

## 2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

### 2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Защита в операционных системах» направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
1	2	3	4
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и	ОПК-9.1 Знает методы защиты и средства обеспечения безопасности в операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных. ОПК-9.2 Умеет осуществлять меры противодействия нарушениям безопасности в операционных системах, компьютерных сетях и системах управления базами данных с использованием	Знать: – основные понятия операционных систем и их защиты; – основные понятия, основные алгоритмы хранения и обработки данных ОС; – основные стандарты и алгоритмы передачи данных; – основные понятия защищенных операционных систем, баз данных и компьютерных сетей; – основные актуальные модели атак; – понятие защиты информации, системы защиты; – аппаратно-программные средства защиты информации: – средства обеспечения конфиденциальности данных; – средства аутентификации электронных данных и средства управления ключевой информацией; – цели и концептуальные основы защиты информации; – основные виды угроз безопасности информации и их классификацию. Уметь:



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 4

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

	средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	различных программных и аппаратных средств защиты.	<ul style="list-style-type: none"><li>– осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;</li><li>– оценивать угрозы безопасности клиентским ОС</li><li>осуществлять проверку защищенности клиентских ОС;</li><li>– осуществлять проверку защищенности серверных ОС;</li><li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li><li>– использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем;</li><li>– использовать алгоритмы генерации, хранения и распределения ключей;</li><li>– проектировать и использовать системы электронной цифровой подписи;</li><li>– применять на практике алгоритмы управления открытыми ключами.</li></ul> <p>Владеть:</p> <ul style="list-style-type: none"><li>– навыками настройки политики безопасности и учетных записей ОС оценки степени защищенности клиентских ОС;</li><li>– навыками оценки степени безопасности ОС;</li><li>– навыками администрирования протокольных средств обеспечения безопасности ОС;</li><li>– навыками администрирования прав пользователей и аудита доступа к ресурсам ОС;</li><li>– основными методами администрирования и настройки ОС и сетей передачи;</li><li>– алгоритмами формирования хеш-функций;</li><li>– инструментами обеспечения безопасной работы в сети интернет;</li><li>– методологией применения безопасных публичных служб;</li><li>– методами управления ключами в системах с открытым ключом;</li><li>– инструментами обеспечения безопасной работы в сети интернет.</li></ul>
ОПК-13	Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их	ОПК-13.1 Знает средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем. ОПК-13.2 Умеет формулировать и	<p>Знать:</p> <ul style="list-style-type: none"><li>– цели и концептуальные основы защиты информации;</li><li>– основные виды угроз безопасности информации и их классификацию;</li><li>– программно-аппаратные средства защиты информации:</li><li>– средства обеспечения конфиденциальности данных;</li><li>– средства аутентификации электронных данных и средства управления ключевой информацией;</li><li>– требования к криптографическим системам защиты информации;</li></ul>



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 5

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

	безопасности	настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем. ОПК-13.3 Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.	– понятие и виды криптографических атак. Уметь: – оценивать угрозы безопасности клиентским ОС; – проектировать и использовать системы электронной цифровой подписи; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем; – использовать алгоритмы генерации, хранения и распределения ключей; – осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации; – осуществлять проверку защищенности клиентских ОС; – осуществлять проверку защищенности серверных ОС. Владеть: – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет.
--	--------------	---	---



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 6

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

### 3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

#### 3.1 Виды оценочных средств

№ п/п	Код компетенции / планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	ОПК-9 ОПК-13	Раздел 1. Подсистема защиты информации в ОС UNIX.	Вопросы для устного опроса № 1-4, 11-15. Самостоятельная работа № 1. Лабораторная работа № 1, 5.	Вопросы для зачета № 1-5. Вопросы для экзамена № 11.
2.	ОПК-9 ОПК-13	Раздел 2. Подсистема Защиты информации в ОС Windows	Вопросы для устного опроса № 1-10. Самостоятельная работа № 2. Лабораторная работа № 2.	Вопросы для зачета № 8-13. Вопросы для экзамена № 5.
3.	ОПК-9 ОПК-13	Раздел 3. Защита информации при интеграции UNIX и Windows	Вопросы для устного опроса № 16. Самостоятельная работа № 3. Лабораторная работа № 4.	Вопросы для зачета № 6, 15-16. Вопросы для экзамена № 8.
4.	ОПК-9 ОПК-13	Раздел 4. Программно-аппаратные методы и средства ограничения доступа к ресурсам ПЭВМ	Вопросы для устного опроса № 27-31. Лабораторная работа № 6,7.	Вопросы для зачета № 17-21. Вопросы для экзамена № 5-14.
5.	ОПК-9 ОПК-13	Раздел 5. Подсистемы защиты информации	Вопросы для устного опроса № 1-15. Самостоятельная работа № 4. Лабораторная работа № 9.	Вопросы для зачета № 1-13. Вопросы для экзамена № 1-17.
6.	ОПК-9 ОПК-13	Раздел 6. Инфраструктура открытых ключей РКІ	Вопросы для устного опроса № 32-34. Самостоятельная работа № 5,6. Лабораторная работа № 8.	Вопросы для зачета № 22-24.
7.	ОПК-9 ОПК-13	Раздел 7. Службы сертификации в ОС Windows	Вопросы для устного опроса № 35-36. Самостоятельная работа №	Вопросы для зачета № 25.



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 7

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

			7. Лабораторная работа № 12.	
8.	ОПК-9 ОПК-13	Раздел 8. Служба управления правам ADRMS	Вопросы для устного опроса № 37.	Вопросы для зачета № 27.
9.	ОПК-9 ОПК-13	Раздел 9. Безопасность ОС Windows на серверном уровне	Вопросы для устного опроса № 38-42. Самостоятельная работа № 10. Лабораторная работа № 12.	Вопросы для зачета № 24. Вопросы для экзамена № 18-23.
10.	ОПК-9 ОПК-13	Раздел 10. Шифрование IPsec в ОС Windows	Вопросы для устного опроса № 39.	Вопросы для зачета № 28.
11.	ОПК-9 ОПК-13	Раздел 11. Сервер сетевых политик, защита и маршрутизация сетевого доступа и дистанционный доступ	Вопросы для устного опроса № 43-58. Самостоятельная работа № 9. Лабораторная работа № 13-17.	Вопросы для зачета № 32. Вопросы для экзамена № 24-33.

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

	МИНОБРНАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ») Математический факультет Кафедра компьютерной безопасности и прикладной алгебры		
	Фонд оценочных средств по дисциплине «Защита в операционных системах» по специальности 10.05.01 Компьютерная безопасность специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»		
Версия документа - 1	стр. 8	Первый экземпляр _____	КОПИЯ № _____

## 3.2. Содержание оценочных средств

### 3.2.1. Вопросы для устного опроса для текущей аттестации

1. Типовые модели управления доступом.
2. Дискреционное управление доступом.
3. Изолированная программная среда.
4. Мандатное управление доступом.
5. Архитектура безопасности ОС Windows.
6. Security accounts manager.
7. LM, NTLM, NTLM2, NTLMv2.
8. Kerberos.
9. Реестр ОС Windows.
10. Microsoft Management Console.
11. Подсистема защиты информации в ОС UNIX.
12. Passwd и shadow файлы.
13. Основные компоненты подсистем защиты UNIX.
14. Права доступа к элементам файловой системы.
15. Управление процессами.
16. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах.
17. Аудит событий.
18. Бюджет пользователя в ОС Windows.
19. Список доступа в ОС Windows.
20. Аудит в Windows, UNIX.
21. Подсистема защиты информации в ОС Windows.
22. Основные компоненты подсистем защиты Windows.
23. Политики безопасности.
24. Понятие домена.
25. Основы взаимодействия элементов гетерогенных сетей.
26. Шлюзы NFS.
27. Программно-аппаратные методы и средства ограничения доступа к ресурсам ПЭВМ.
28. Методы и средства ограничения доступа к компонентам ПЭВМ.
29. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
30. Методы и средства хранения ключевой информации.
31. Программная закладка.
32. Инфраструктура открытых ключей PKI.
33. Основные компоненты PKI.
34. Функции удостоверяющего и регистрационного центров, репозитория, архива сертификатов, серверных компонентов PKI.
35. Службы сертификации в ОС Windows.
36. Основные действия необходимые для установки и базовой настройки службы сертификации ActiveDirectory® (AD CS) в тестовой среде.



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 9

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

37. Служба управления правам ADRMS.
38. Шифрование IPsec в ОС Windows.
39. NATTraversal в IPsec.
40. Компоненты NAP.
41. Протокол RADIUS.
42. Сервер сетевых политик.
43. Сетевая система обнаружения и предотвращения вторжений.
44. Выявление вторжений.
45. Методы предотвращения вторжений.
46. Способы обхода системы обнаружения вторжений.
47. Хостовая система обнаружения вторжений.
48. Мониторинг файловой системы.
49. Обнаружение rootkit.
50. Honeyrot. Виды, классификация.
51. Обнаружение Honeyrot.
52. Security Information and Event Management.
53. Log Management System
54. Security Log/Event Management
55. Security Information Management
56. Security Event Correlation
57. Security Information and Event Management.
58. Функции SIEM.

### 3.2.2. Перечень самостоятельных работ

1. Создание бюджетов пользователя в ОС Windows, UNIX.
2. Использование списков доступа в ОС Windows, UNIX.
3. Аудит в Windows, UNIX.
4. Оценка защищенности заданной конфигурации Windows.
5. Создание сертификатов в PKI.
6. Создание смарт-карт в PKI.
7. Создание репозитория сертификатов и восстановление ЦС.
8. Создание шаблонов RMS для защиты офисных документов.
9. Создание дополнительных сценариев резервного копирования.
10. Создание политик сетевого доступа.

### 3.2.3. Перечень лабораторных работ

1. Изучение систем безопасности ОС Windows, UNIX. Создание бюджетов пользователя. Использование списков доступа.
2. Аудит событий в ОС Windows, UNIX.
3. Оценка защищенности заданной конфигурации Windows: файловая система, реестр, список пользователей, политика безопасности в области паролей.
4. Интеграция сетей Microsoft и UNIX с использованием сервера Samba.
5. Изучение средств защиты сетевого взаимодействия Unix.
6. Поиск программных закладок в заданной консультации Windows.
7. Использование возможностей файловой системы ОС Windows для шифрования



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 10

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_

- файлов BitLocker, EFS.
8. Изучение инфраструктуры открытых ключей. Создание смарт-карт. Защита конфигурации ADCS.
  9. Изучение дополнительных мер безопасности (резервное копирование, работа со службой обновления).
  10. Изучение протокола RADIUS.
  11. Развертывание и внедрение виртуальной частной сети.
  12. Внедрение параметров политики с помощью сервера сетевых политик.
  13. Настройка и разработка правил для NIPS/NIDS Snort.
  14. Настройка и разработка правил для HIDS OSSEC.
  15. Настройка системы Honeypot и интеграция с SIEM.
  16. Отправка уведомлений OSSEC.
  17. SIEM Splunk.

Полные тексты лабораторных работ и задания выложены на сетевом диске кафедры компьютерной безопасности и прикладной алгебры DC1\doc\.

#### **3.2.4. Перечень вопросов к зачету (8 семестр)**

1. Подсистема защиты информации в ОС UNIX.
2. Passwd и shadow файлы.
3. Основные компоненты подсистем защиты UNIX.
4. Права доступа к элементам файловой системы.
5. Управление процессами.
6. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах.
7. Аудит событий.
8. Бюджет пользователя в ОС Windows.
9. Список доступа в ОС Windows.
10. Аудит в Windows, UNIX.
11. Подсистема защиты информации в ОС Windows.
12. Основные компоненты подсистем защиты Windows.
13. Политики безопасности.
14. Понятие домена.
15. Основы взаимодействия элементов гетерогенных сетей.
16. Шлюзы NFS.
17. Программно-аппаратные методы и средства ограничения доступа к ресурсам ПЭВМ.
18. Методы и средства ограничения доступа к компонентам ПЭВМ.
19. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
20. Методы и средства хранения ключевой информации.
21. Программная закладка.
22. Инфраструктура открытых ключей PKI.
23. Основные компоненты PKI.
24. Функции удостоверяющего и регистрационного центров, репозитория, архива



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 11

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

сертификатов, серверных компонентов PKI.

25. Службы сертификации в ОС Windows.
26. Основные действия необходимые для установки и базовой настройки службы сертификации ActiveDirectory® (AD CS) в тестовой среде.
27. Служба управления правам ADRMS.
28. Шифрование IPsec в ОС Windows.
29. NATTraversal в IPsec.
30. Компоненты NAP.
31. Протокол RADIUS.
32. Сервер сетевых политик.

### **3.2.5. Перечень вопросов к экзамену (9 семестр)**

1. Типовые модели управления доступом.
2. Дискреционное управление доступом.
3. Изолированная программная среда.
4. Мандатное управление доступом.
5. Архитектура безопасности ОС Windows.
6. Security accounts manager.
7. LM, NTLM, NTLM2, NTLMv2.
8. Kerberos.
9. Реестр ОС Windows.
10. Microsoft Management Console.
11. Архитектура безопасности ОС Unix.
12. Базовая файловая структура.
13. Права доступа к файлам и директориям.
14. Passwd и shadow файлы.
15. Аудит событий.
16. Аудит в ОС Windows.
17. Аудит в ОС Unix.
18. Сетевая система обнаружения и предотвращения вторжений.
19. Выявление вторжений.
20. Методы предотвращения вторжений.
21. Способы обхода системы обнаружения вторжений.
22. Хостовая система обнаружения вторжений.
23. Мониторинг файловой системы.
24. Обнаружение rootkit.
25. Honeypot. Виды, классификация.
26. Обнаружение Honeypot.
27. Security Information and Event Management.
28. Log Management System
29. Security Log/Event Management
30. Security Information Management
31. Security Event Correlation
32. Security Information and Event Management.
33. Функции SIEM.



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 12

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

## 4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 4.1. Порядок проведения промежуточной аттестации

#### Часть 1 (8 семестр)

В течение семестра студент должен выполнить двенадцать лабораторных работ, каждая из которых оценивается в 5 баллов.

Максимальный балл за лабораторную работу – 5 баллов.

Максимальный балл за лабораторные работы в 8 семестре 60 баллов.

В течение семестра студент должен выполнить четыре самостоятельных работы, каждая из которых оценивается в 5 баллов.

Допуском до проведения зачета являются сданные студентом лабораторные и самостоятельные работы в течение семестра.

Зачет проводится в один этап, на котором студент отвечает один теоретический вопрос и выполняет одно практическое задание из списка лабораторных и самостоятельных работ. Продолжительность – 30 минут.

Максимальный балл за ответ на теоретический вопрос – 10 баллов.

Максимальный балл за практическую часть зачета – 10 баллов.

#### Сводная таблица рейтинга успеваемости (8 семестр)

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа №1-12	12x5=60
2	Самостоятельная работа № 1-4	4x5=20
3	Зачет (теоретический вопрос)	10
4	Зачет (практическая часть)	10
	Итого	100

#### Часть 2 (9 семестр)

В течение семестра студент должен выполнить пять лабораторных работ, каждая из которых оценивается в 5 баллов.

Максимальный балл за лабораторную работу – 5 баллов.

Максимальный балл за лабораторные работы в 9 семестре – 25 баллов.

В течение семестра студент должен выполнить шесть самостоятельных работы, каждая из которых оценивается в 5 баллов.

Допуском до проведения экзамена являются сданные студентом лабораторные и самостоятельные работы в течение семестра.

Экзамен проводится в один этап, на котором студент отвечает на два теоретических вопроса и выполняет одно практическое задание из списка лабораторных и самостоятельных работ. Продолжительность – 30 минут.

Максимальный балл за ответ на теоретический вопрос – 10 баллов.

Максимальный балл за практическую часть экзамена – 20 баллов.



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 13

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

### Сводная таблица рейтинга успеваемости (9 семестр)

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа №1-5	5x5=25
2	Самостоятельная работа № 1-6	6x5=30
3	Посещаемость (все занятия)	5
4	Экзамен (теоретический вопрос)	2x10=20
5	Экзамен (практическая часть)	20
	Итого	100

## 4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

### 4.2.1. Критерии оценивания теоретического вопроса зачета и экзамена Максимальный балл за ответ на теоретический вопрос – 10 баллов.

Отлично/зачтено/ 9-10 баллов	Хорошо/зачтено/ 7-8 баллов	Удовлетворительно/зачтено/ 5-6 баллов	Неудовлетворительно/не зачтено/ 0-4 балла
Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.	Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

	МИНОБРНАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ») Математический факультет Кафедра компьютерной безопасности и прикладной алгебры		
	Фонд оценочных средств по дисциплине «Защита в операционных системах» по специальности 10.05.01 Компьютерная безопасность специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»		
Версия документа - 1	стр. 14	Первый экземпляр _____	КОПИЯ № ____

#### 4.2.2. Критерии оценивания практической части (практического задания) зачета

Максимальный балл за ответ на теоретический вопрос – 10 баллов.

Отлично/зачтено/ 9-10 баллов	Хорошо/зачтено/ 7-8 баллов	Удовлетворительно/зачтено/ 5-6 баллов	Неудовлетворительно/не зачтено/ 0-4 балла
Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.	Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

#### 4.2.3. Критерии оценивания практической части (практического задания) экзамена

Максимальный балл за практическую часть экзамена – 20 баллов.

Отлично/зачтено/ 17-20 баллов	Хорошо/зачтено/ 13-16 баллов	Удовлетворительно/зачтено/ 8-12 баллов	Неудовлетворительно/не зачтено/ 0-8 баллов
Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов и названий. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов и названий. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом, но допускает фактические ошибки.	Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1

стр. 15

Первый экземпляр \_\_\_\_\_

КОПИЯ № \_\_\_\_\_

#### **4.2.4. Критерии оценки лабораторной работы**

5 баллов - лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

4 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

3 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

2 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

1 балл – при выполнении лабораторной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.

0 баллов – не выполнена лабораторная работа.

#### **4.2.5. Критерии оценки самостоятельной работы**

5 баллов – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

4 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

3 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

2 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

1 балл – при выполнении самостоятельной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.

	МИНОБРНАУКИ РОССИИ Федеральное государственное бюджетное образовательное учреждение высшего образования «Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ») Математический факультет Кафедра компьютерной безопасности и прикладной алгебры		
	Фонд оценочных средств по дисциплине «Защита в операционных системах» по специальности 10.05.01 Компьютерная безопасность специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»		
Версия документа - 1	стр. 16	Первый экземпляр _____	КОПИЯ № ____

0 баллов – не выполнена самостоятельная работа.

### 4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации.

В течении семестра проводится лабораторные работы, проверяются самостоятельные работы по одному из рассматриваемых разделов, которые осуществляют срез знаний по основным понятиям, определениям и задачам.

Для зачета:

0 – 60 баллов – выставляется «не зачтено»

от 61 баллов и выше – выставляется «зачтено»

Для экзамена:

0-60 баллов – неудовлетворительно (2);

61-74 баллов – удовлетворительно (3);

75-90 баллов – хорошо (4);

91-100 баллов – отлично (5).

Особенности проведения процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

Уровни сформированности компетенций определяется следующим образом:

Оценка	Отлично/ зачтено	Хорошо/ зачтено	Удовлетворитель но/ зачтено	Неудовлетворите льно/ не зачтено
Баллы	91-100 баллов	75-90 баллов	60-74 баллов	0-59 баллов
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

- Высокий уровень сформированности компетенций соответствует оценке «Отлично»:
  - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности,
  - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, формулировать собственные выводы.
- Средний уровень соответствует оценке «Хорошо»:



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)  
Математический факультет  
Кафедра компьютерной безопасности и прикладной алгебры

Фонд оценочных средств по дисциплине «Защита в операционных системах»  
по специальности 10.05.01 Компьютерная безопасность  
специализации № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Версия документа - 1	стр. 17	Первый экземпляр _____	КОПИЯ № _____
----------------------	---------	------------------------	---------------

- предполагает формирование компетенций на достаточном уровне,
  - студент способен давать развернутые ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Хорошо».
3. Базовый уровень соответствует оценке «Удовлетворительно»:
- предполагает формирование компетенций на начальном уровне,
  - студент способен давать ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Удовлетворительно»,
  - студент способен отвечать на вопросы в закрытой форме. Количество правильных ответов – не менее 50%.
4. Низкий уровень соответствует оценке «Неудовлетворительно».

