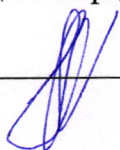


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«19 » марта 2024 г., протокол № 8
Исполняющий обязанности
заведующего кафедрой



Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1. О.20 Безопасность операционных систем

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

профиль

*Безопасность автоматизированных систем (по отрасли или в сфере
профессиональной деятельности)*

Квалификация

бакалавр

Форма обучения

очная

Южно-Сахалинск
2024 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.1 - Знает принципы поиска, обработки, обобщения и представления информации для решения задач профессиональной деятельности; ОПК-8.2 - Умеет работать с источниками информации, базами данных и нормативной документацией при решении профессиональных задач; ОПК-8.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности
ОПК-4.3	ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы; ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Тема 1. Основные механизмы обеспечения безопасности ОС	ОПК-8, ОПК-4.3	Устный опрос по теме
2.	Тема 2. Средства и методы аутентификации в ОС	ОПК-8, ОПК-4.3	Выполнение практического задания

3.	Тема 3 Разграничение доступа к ресурсам ОС	ОПК-8, ОПК-4.3	Выполнение практического задания
4.	Тема 4. Контроль работы подсистемы защиты	ОПК-8, ОПК-4.3	Выполнение практического задания

3. Оценочные средства

Форма контроля для очной формы обучения – **зачет**

Примеры заданий для текущего контроля и промежуточных заданий по различным темам:

Задание 1 (ОПК-8, ОПК-4.3)

1. Создайте пользователя.
2. Установите требования к качеству PIN-кода eToken в соответствии с Вашим вариантом (табл. 1).
3. Отформатируйте eToken, присвоив ему имя созданного пользователя и установив пароль, соответствующий требованиям п. 2.
4. Создайте профиль для входа в ОС созданного пользователя.

Задание 2 (ОПК-8, ОПК-4.3)

1. Создайте шаблон для окна приложения.
2. При создании шаблона задайте для него настройки.
3. На основе сформированного шаблона создайте и сохраните на eToken соответствующий профиль.

Задание 3 (ОПК-8, ОПК-4.3)

5. Создайте каталоги «Общедоступно» и «Конфиденциально».
6. В каждом из этих каталогов скопируйте исполняемый и текстовый файлы.
7. Разграничьте доступ к принтеру, а также созданным каталогам и файлам.

Задание 4 (ОПК-8, ОПК-4.3)

1. От имени администратора присвойте каталогам (находящимся в корне диска D:\) категории конфиденциальности.
2. В каждом каталоге создайте 2-4 документа от имени пользователя, допуск которого соответствует категории конфиденциальности каталога.
3. Проверьте возможность доступа к созданным документам.

Задание 5 (ОПК-8, ОПК-4.3)

Создайте следующую политику ограничения использования программ, которая будет удовлетворять следующим требованиям:

1. разрешает запуск ПО, подписанного сертификатом от «Microsoft»;
2. применяется ко всем пользователям, включая локальных администраторов;
3. не ограничивает использование программных библиотек, таких как «DLL»;
4. право выбора доверенных издателей разрешено только локальным администраторам;
5. запрещает запуск любых программ в качестве уровня безопасности по умолчанию;
6. разрешает запуск любых программ из папок: «C:\WINDOWS», «C:\Program Files», «C:\Documents and Settings\LocalService», «C:\Documents and Settings\All Users»;

Задание 6 (ОПК-8, ОПК-4.3)

Администратор безопасности Анатолий предоставил полный доступ к материалам по безопасности отдела только стажеру Дмитрий. Эти материалы были размещены на сетевом ресурсе «Ресурсы предприятия\Обмен\Дмитрию», к которому был заранее выставлен аудит чтения, записи, удаления, а также смены владельца. При утилизации документации Анатолий обнаружил распечатанные копии этих материалов. Стажер утверждает свою непричастность к распечатанным копиям важных документов. Докажите или опровергните причастность Дмитрия к распечатанным документам.

Задание 7 (ОПК-8, ОПК-4.3)

Создайте шаблон безопасности в соответствии и настройте операционную систему, используя созданный шаблон:

1. Локальные политики: Включите аудит доступа к объектам (успех и отказ)
2. Журнал событий: Сохранение событий в журнале безопасности – 30 дней
3. Файловая система : Аудит создания файлов и записи данных (успех и отказ) на каталог C:\Windows и дочерние для учётной записи «user»

Примерные вопросы к зачету

1. Основные группы механизмов защиты операционных систем; основные функции этих механизмов.
2. Процедуры идентификации, аутентификации, авторизации. Определение, принцип действия.
3. Функции аутентификации по контролю доступа при работе с ОС и при настройке ОС. Факторы аутентификации – определение, типы, примеры. Многофакторная аутентификация – определение, примеры.
4. Аутентификация с использованием паролей. Принцип действия, варианты реализации, недостатки.
5. Угрозы преодоления парольной защиты. Требования к паролям для увеличения их стойкости.
6. Аутентификация при помощи физического объекта. Принцип действия, варианты реализации, недостатки.
7. Технология однократного входа (SSO – Single Sign-on). Принцип действия, преимущества и недостатки. Применение физического объекта в технологии SSO.
8. Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.
9. Методы биометрической аутентификации.
10. Принципы дискреционного управления доступом. Преимущества и недостатки дискреционной модели.
11. Реализация дискреционного механизма управления доступом в Windows и UNIX системах.
12. Принципы мандатного управления доступом. Преимущества и недостатки мандатной модели.
13. Основные права доступа к файловым объектам в ОС Windows.
14. Владелец файла и его возможности. Подходы к назначению владельца файла.
15. Классификация субъектов и объектов доступа.
16. Правила наследования прав доступа к иерархическим объектам в ОС Windows. Приоритеты правил наследования.
17. Способы обеспечения замкнутости программной среды. Достоинства и недостатки этих методов.
18. Уровни безопасности и правила политики ограниченного использования программ в ОС Windows. Приоритеты использования правил.
19. Способы разграничения доступа к устройствам. Типы прав доступа к устройствам.
20. Белый список устройств и способы его применения.
21. Аудит в операционных системах. Задачи аудита.
22. События, подвергаемые аудиту в ОС Windows. Данные, фиксируемые при аудите.
23. Задачи, решаемые с использованием оснастки «Анализ и настройка безопасности» в Windows

Форма контроля	За одну работу	Всего
----------------	----------------	-------

	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,5	1	8	16
Подготовка к занятию, выполнение домашнего задания	0,5	1	8	16
выполнение практических заданий по темам	3	5	27	45
Промежуточная аттестация (зачет)	10	23	10	23
Итого за семестр			53	100

Система оценивания планируемых результатов обучения

Оценка «зачтено» выставляется,

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.
- студенту твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания

Составитель


(подпись)

Филиппова
преподаватель
информатики

Г.В., старший
кафедры

«12 » марта 2024 г