Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Борисов Дмитрий Николаевич

Кафедра информационных систем

03.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.41 Защита в операционных системах

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Анализ безопасности компьютерных систем, Математические методы защиты информации

3. Квалификация (степень) выпускника:

Специалист

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра информационных систем

6. Составители программы:

Савинков Андрей Юрьевич, д.т.н., профессор

7. Рекомендована:

рекомендована НМС ФКН 03.05.2023, протокол № 7

8. Учебный год:

2025-2026

9.Цели и задачи учебной дисциплины:

Обучение студентов принципам построения защиты информации в ОС и анализа надежности их защиты.

Основные задачи дисциплины:

- получение базовых знаний о принципах построения подсистем защиты в ОС различной архитектуры;
- знакомство со средствами и методами несанкционированного доступа к ресурсам ОС;
- выработка системного подхода к проблеме защиты информации в ОС;
- овладение механизмами защиты информации и изучение возможностей по их преодолению.

10. Место учебной дисциплины в структуре ООП:

Дисциплина обязательной части (Б1.О). Входные знания: «Операционные системы»

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
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 средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;	ОПК-9.11 знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных	Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных
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 средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;	ОПК-9.12 знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных;	Знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных
ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.6 знает средства и методы хранения и передачи аутентификационной информации	Знает средства и методы хранения и передачи аутентификационной информации
ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.7 знает основные требования к подсистеме аудита и политике аудита	Знает основные требования к подсистеме аудита и политике аудита
ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.8 знает защитные механизмы и средства обеспечения безопасности операционных систем	Знает защитные механизмы и средства обеспечения безопасности операционных систем

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.9 умеет формулировать и настраивать политику безопасности основных операционных систем	Умеет формулировать и настраивать политику безопасности основных операционных систем
ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.10 умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем	Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем
ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;	ОПК-12.2 знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей.	Знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем
ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;	ОПК-12.4 владеет навыками системного программирования	Владеет навыками системного программирования
ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;	ОПК-13.1 умеет формулировать и настраивать политику безопасности основных операционных систем	Умеет формулировать и настраивать политику безопасности основных операционных систем
ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;	ОПК-13.2 владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств	Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 6	Всего
Аудиторные занятия	72	72
Лекционные занятия	36	36
Практические занятия	0	0
Лабораторные занятия	36	36
Самостоятельная работа	36	36
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль		0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Основы защиты информации в операционных системах	Общие требования к защите информации, технические и административные методы защиты, уровни доверия, политики безопасности, профили защиты	https://edu.vsu.ru/course/view.php?id=15499
1.2	Управление доступом	Объекты, субъекты и методы доступа, модели управления доступом, изолированная программная среда	https://edu.vsu.ru/course/view.php?id=15499
1.3	Аутентификация пользователей и проверка целостности информации	Факторы аутентификации, хранение паролей, аутентификация по открытому каналу, одноразовые пароли, многофакторная аутентификация	https://edu.vsu.ru/course/view.php?id=15499

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.4	Разграничение доступа в Unix и Unix-подобных системах	Базовая модель разграничения доступа в UNIX-подобных системах, учет пользователей и хранение паролей, регистрация пользователей и вход в систему, PAM	https://edu.vsu.ru/course/view.php?id=15499
1.5	Методы защиты информации в Linux	Возможности (capabilities) потоков в Linux, управление возможностями, списки контроля доступа Linux, дополнительные атрибуты файлов, изоляция (пространства имен) в Linux, система sudo, seccomp, SELinux, AppArmor	https://edu.vsu.ru/course/view.php?id=15499
1.6	Методы защиты информации в Windows	Дескрипторы защиты и маркеры доступа, олицетворение, списки контроля доступа в Windows	https://edu.vsu.ru/course/view.php?id=15499
1.7	Основы сетевой безопасности	Межсетевой экран Linux и Windows	https://edu.vsu.ru/course/view.php?id=15499
1.8	Аудит в операционных системах	Журналы аудита Linux и Windows, фильтры аудита	https://edu.vsu.ru/course/view.php?id=15499
2. Практические занятия			
3. Лабораторные работы			
3.1	Управление пользователями в Linux	Создание учетной записи, присоединение к группе, замена программы (оболочки) пользователя, создание псевдопользователя для запуска программы	https://edu.vsu.ru/course/view.php?id=15499

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3.2	Контроль целостности файлов в Linux	Вычисление и проверка контрольной суммы, проверка целостности программы при запуске	https://edu.vsu.ru/course/view.php?id=15499
3.3	Изучение PAM	Реализация модуля PAM, реализующего аутентификацию по серийному номеру устройства USB	https://edu.vsu.ru/course/view.php?id=15499
3.4	Изучение возможностей (capabilities) Linux	Установка возможностей программы для выполнения привилегированных действий без использования root	https://edu.vsu.ru/course/view.php?id=15499
3.5	Изучение изоляции ресурсов Linux	Создание изолированной сетевой среды, создание сетевого туннеля для доступа к изолированной среде, утилита unshare, файловая система /sys/fs/cgroup/	https://edu.vsu.ru/course/view.php?id=15499
3.6	Изучение подсистемы sudo	Создание правила для конкретного пользователя	https://edu.vsu.ru/course/view.php?id=15499
3.7	Изучение подсистемы seccomp	Ограничение запуска программ и доступа к файлам за счет реализации фильтра системных вызовов	https://edu.vsu.ru/course/view.php?id=15499
3.8	Изучение межсетевого экрана Linux	Создание правил для netfilter, ограничивающих доступ к отдельным сетевым протоколам и портам	https://edu.vsu.ru/course/view.php?id=15499
3.9	Изучение механизмов ограничения запуска программ в Windows	Создание правил политики ограничения запуска программ	https://edu.vsu.ru/course/view.php?id=15499
3.10	Изучение межсетевого экрана Windows	Создание правил для netfilter, ограничивающих доступ к отдельным сетевым протоколам и портам	https://edu.vsu.ru/course/view.php?id=15499

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Основы защиты информации в операционных системах	4	0	0	2	6
2	Управление доступом	2	0	0	2	4
3	Аутентификация пользователей и проверка целостности информации	4	0	0	2	6
4	Разграничение доступа в Unix и Unix-подобных системах	4	0	0	2	6
5	Методы защиты информации в Linux	6	0	0	2	8
6	Методы защиты информации в Windows	6	0	0	2	8
7	Основы сетевой безопасности	6	0	0	2	8
8	Аудит в операционных системах	4	0	0	2	6
9	Управление пользователями в Linux	0	0	2	2	4
10	Контроль целостности файлов в Linux	0	0	2	2	4
11	Изучение PAM	0	0	4	2	6
12	Изучение возможностей (capabilities) Linux	0	0	4	2	6
13	Изучение изоляции ресурсов Linux	0	0	6	2	8
14	Изучение подсистемы sudo	0	0	4	2	6
15	Изучение подсистемы seccomp	0	0	4	2	6
16	Изучение механизмов ограничения запуска программ в Windows			2	2	4

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
17	Изучение межсетевого экрана Linux	0	0	4	2	6
18	Изучение межсетевого экрана Windows	0	0	4	2	6
		36	0	36	36	108

14. Методические указания для обучающихся по освоению дисциплины

Дисциплина требует работы с файлами-презентациями лекций и соответствующими главами рекомендованной основной литературы, а также, обязательного выполнения всех лабораторных заданий в компьютерном классе.

Самостоятельная работа проводится в компьютерных классах ФКН с использованием методических материалов расположенных на учебно-методическом сервере ФКН "\\fs.cs.vsu.ru\Library" и на сервере Moodle ВГУ moodle.vsu.ru, выполнением задач конфигурирования виртуализированной ИС. Во время самостоятельной работы студенты используют электронно-библиотечные системы, доступные на портале Зональной Библиотеки ВГУ по адресу www.lib.vsu.ru. Часть заданий может быть выполнена вне аудиторий на домашнем компьютере, после копирования методических указаний и необходимого ПО с учебно-методического сервера ФКН.

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимыхдля освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. // ЭБС Университетская библиотека. – URL: https://biblioclub.ru/index.php?page=book_red&id=598988

б) дополнительная литература:

№ п/п	Источник
1	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. // ЭБС Университетская библиотека. – URL: https://biblioclub.ru/index.php?page=book&id=438331

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Библиотека ВГУ, http://www.lib.vsu.ru
2	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
3	Образовательный портал "Электронный университет ВГУ", http://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
2	Образовательный портал "Электронный университет ВГУ", http://edu.vsu.ru

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Лекции-визуализации с демонстрацией иллюстративных и графических материалов, анимации, блок-схем алгоритмов и примеров исходного кода, демонстрацией выполнения команд операционной системой, лабораторные работы.

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1. Лекционная аудитория, оснащенная видеопроектором.
2. Компьютерный класс для проведения лабораторных занятий, оснащенный видеопроектора и компьютерами с операционной системой GNU/Linux.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Основы защиты информации в операционных системах	ОПК-9	ОПК-9.11	Собеседование
2	Основы защиты информации в операционных системах	ОПК-9	ОПК-9.12	Собеседование
3	Аутентификация пользователей и проверка целостности информации	ОПК-11	ОПК-11.6	Собеседование
4	Аудит в операционных системах	ОПК-11	ОПК-11.7	Собеседование
5	Управление доступом Разграничение доступа в Unix и Unix-подобных системах Методы защиты информации в Linux Методы защиты информации в Windows Основы сетевой безопасности	ОПК-11	ОПК-11.8	Собеседование
6	Управление пользователями в Linux Изучение подсистемы sudo Контроль целостности файлов в Linux	ОПК-11	ОПК-11.9	Лабораторные работы
7	Изучение межсетевого экрана Linux Изучение межсетевого экрана Windows	ОПК-11	ОПК-11.10	Лабораторные работы
8	Методы защиты информации в Linux Методы защиты информации в Windows	ОПК-12	ОПК-12.2	Собеседование
9	Изучение возможностей (capabilities) Linux Изучение изоляции ресурсов Linux Изучение подсистемы seccomp	ОПК-12	ОПК-12.4	Лабораторные работы

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
10	Управление пользователями в Linux Изучение подсистемы sudo Изучение механизмов ограничения запуска программ в Windows	ОПК-13	ОПК-13.1	Лабораторные работы
11	Изучение PAM	ОПК-13	ОПК-13.2	Лабораторные работы

Промежуточная аттестация

Форма контроля - Зачет с оценкой, Контрольная работа

Оценочные средства для промежуточной аттестации

1. Собеседование
2. Контрольная работа

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущий контроль успеваемости выполняется по лабораторным работам.

По каждой выполненной работе должен быть предоставлен отчет, включающий исходный код разработанных программ и описание полученных результатов. По отчету преподаватель вправе задать дополнительные вопросы для уточнения уровня понимания материала. Лабораторная работа оценивается максимум в 100 баллов.

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине

Компетенция ОПК-9

Задания закрытого типа

1) Какие из перечисленных далее методов защиты информации относятся к техническим методам защиты
   a) Разработка политики безопасности
   b) Контроль целостности информации
   c) Разграничение доступа
   d) Создание и хранение резервных копий ценной информации
   e) Криптографическая защита
   f) Аудит безопасности
2) Псевдопользователи в UNIX и UNIX-подобных системах это
   a) Зарегистрированные пользователи (есть учетная запись в системе), которые не ассоциируются с человеком
   b) Пользователи, работающие в системе удаленно
   c) Пользователи, доступ которых в систему временно ограничен
   d) Низкоквалифицированные пользователи
3) Операционная система называется защищенной, если
   a) Назначен системный администратор
   b) Она не подключена к сети Интернет
   c) В ней реализованы средства защиты информации
4) Использование модели управления доступом типа изолированная программная среда обеспечивает
   a) Существенное повышение защищенности от программных закладок по сравнению с дискреционной моделью

b) Высокую надежность защиты от утечки информации

5) Перечислите пункты, определяющие общие требования к защите информации
   a) Сохранение количества информации
   b) Сохранение целостности информации
   c) Сохранение формата представления информации
   d) Сохранение доступности информации
   e) Сохранение конфиденциальности информации

Ответы на вопросы

Номер вопроса	Ответ (буква)
1	b, c, e, f
2	a
3	c
4	a
5	b, d, e

Задания открытого типа

1) Сколько методов доступа различается в традиционной модели разграничения доступа UNIX
2) Напишите команду, чтобы назначить пользователя ivan владельцем файла с именем file в текущем каталоге

Ответы на вопросы

Номер вопроса	Ответ
1	3
2	chown ivan file или chown ivan ./file

Задания с развёрнутым ответом

1) Дайте определение политики безопасности
2) Дайте определение права доступа

Ответы на вопросы

Номер вопроса	Критерии оценивания
1	[Политика безопасности – это набор правил, регламентирующих порядок хранения и обработки информации] Обучающийся дал правильное определение политики безопасности – 3 балла Обучающийся дал правильное определение политики безопасности. Ответ содержит незначительные неточности – 2 балла Обучающийся дал не точное определение политики безопасности. Ответ не содержит грубых ошибок или неточностей – 1 балл Обучающийся дал не точное определение политики безопасности. Ответ содержит грубые ошибки и неточности – 0 баллов
2	[Право доступа – это возможность субъекта доступа выполнять доступ к объекту доступа по некоторому методу доступа]

	Обучающийся дал правильное определение права доступа – 3 балла Обучающийся дал правильное определение права доступа. Ответ содержит незначительные неточности – 2 балла Обучающийся дал не точное определение права доступа. Ответ не содержит грубых ошибок и неточностей – 1 балл Обучающийся дал не точное определение права доступа. Ответ содержит грубые ошибки или неточности – 0 баллов

Компетенция ОПК-11

Задания закрытого типа

1) Политика безопасности это
   a) Скрипт для проверки целостности информации
   b) Набор правил, регламентирующих порядок хранения и обработки информации
   c) Метод аутентификации пользователя
   d) Набор правил для анализа данных аудита безопасности
2) Адекватная политика безопасности
   a) Политика безопасности, обеспечивающая достаточный уровень защиты без излишних ограничений и неудобств в работе пользователей
   b) Политика безопасности, обеспечивающая гарантированную защиту информации
3) Аудит системных событий позволяет
   a) Ввести дополнительный уровень разграничения доступа к объектам доступа
   b) Своевременно обнаружить попытки нарушений политики безопасности
   c) Своевременно обнаружить изменения важных для безопасности системных настроек
   d) Предотвратить нарушение целостности данных
4) Оценочный уровень доверия 1 предполагает
   a) Минимальный уровень доверия, основанный на наличие в составе ОС некоторых средств защиты
   b) Уровень доверия от умеренного до высокого в отношении уже существующей ОС общего назначения
   c) Высокий уровень доверия для разрабатываемой ОС
   d) Уверенность в безопасности ОС при работе в условиях чрезвычайно высокого риска
5) Оценочный уровень доверия 4 предполагает
   a) Минимальный уровень доверия, основанный на наличие в составе ОС некоторых средств защиты
   b) Уровень доверия от умеренного до высокого в отношении уже существующей ОС общего назначения
   c) Высокий уровень доверия для разрабатываемой ОС
   d) Уверенность в безопасности ОС при работе в условиях чрезвычайно высокого риска

Ответы на вопросы

Номер вопроса	Ответ (буква)
1	b
2	a
3	b, c
4	a
5	b

Задания открытого типа

1) Сколько оценочных уровней доверия определено в ГОСТ Р ИСО/МЭК 15408-3-2013

Ответы на вопросы

Номер вопроса	Ответ
1	7

Задания с развёрнутым ответом

1) Опишите процедуру взаимной аутентификации сервера и клиента на основе алгоритма OCRA (Open-Authentication Challenge-Response Algorithm)

Ответы на вопросы

Номер вопроса	Критерии оценивания
1	[Секретный ключ *K* должен быть априорно известен серверу и клиенту, секретный ключ не передается по каналу связи. Клиент посылает запрос на взаимную аутентификацию со случайными данными D_c. Сервер вычисляет OCRA(K, D_c) и отправляет полученный хэш клиенту, также сервер отправляет свои случайные данные D_s для аутентификации клиента. Клиент сравнивает полученный от сервера хэш с ожидаемым. Если хэш совпадает, то клиент теперь доверяет серверу. Клиент вычисляет OCRA(K, D_s) и отправляет полученный хэш на сервер. Сервер сравнивает полученный хэш с ожидаемым. Если хэш совпадает, то сервер теперь доверяет клиенту. Взаимная аутентификация выполнена] Обучающийся правильно описал процедуру взаимной аутентификации сервера и клиента на основе алгоритма OCRA – 3 балла Обучающийся правильно описал процедуру взаимной аутентификации сервера и клиента на основе алгоритма OCRA. Ответ содержит незначительные неточности – 2 балла Обучающийся не достаточно точно описал процедуру взаимной аутентификации сервера и клиента на основе алгоритма OCRA. Ответ не содержит грубых ошибок или неточностей – 1 балл Обучающийся не достаточно точно описал процедуру взаимной аутентификации сервера и клиента на основе алгоритма OCRA. Ответ содержит грубые ошибки и неточности – 0 баллов

Компетенция ОПК-12

Задания закрытого типа

1) В UNIX и UNIX-подобных операционных системах
   a) Пользовательские пароли хранятся в открытом виде
   b) Пользовательские пароли хранятся в зашифрованном виде
   c) Хранятся результаты необратимого преобразования пользовательских паролей (hash)
   d) Информация о паролях пользователей не хранится в системе
2) Что может использоваться в качестве фактора аутентификации
   a) Некоторая секретная информация, известная только авторизованному пользователю (пароль)
   b) Некоторый уникальный объект, который есть только у авторизованного пользователя (ключ)
   c) Некоторая характеристика, присущая только авторизованному пользователю (биометрические данные)
3) Что такое имитовставка в передаваемом сообщении
   a) Специальный проверочный код, передаваемый вместе с данными для проверки целостности данных при их передаче по ненадежному каналу

b) Фрагмент ложной информации, вставляемый в передаваемое сообщение для дезинформации злоумышленника

c) Имитация передачи данных для проверки надежности канала передачи

d) Идентификатор отправителя сообщения

Ответы на вопросы

Номер вопроса	Ответ (буква)
1	c
2	a, b, c
3	a

Задания открытого типа

2) Размер хэша (в битах), формируемого алгоритмом MD5

Ответы на вопросы

Номер вопроса	Ответ
1	128

Задания с развёрнутым ответом

1) Уровень доверия, оценочные уровни доверия

Ответы на вопросы

Номер вопроса	Критерии оценивания
1	[Доверие – степень уверенности в том, что операционная система отвечает требованиям безопасности, оценочные уровни доверия определены в ГОСТ и дают возможность сравнения различных систем и политик безопасности] Обучающийся дал правильное определение уровня доверия, перечислил и сравнил между собой оценочные уровни доверия – 3 балла Обучающийся дал правильное определение уровня доверия, перечислил и сравнил между собой оценочные уровни доверия. Ответ содержит незначительные неточности – 2 балла Обучающийся не дал точное определение уровня доверия, не перечислил или не сравнил между собой оценочные уровни доверия. Ответ не содержит грубых ошибок или неточностей – 1 балл Обучающийся не дал точное определение уровня доверия, не перечислил или не сравнил между собой оценочные уровни доверия. Ответ содержит грубые ошибки и неточности – 0 баллов

Компетенция ОПК-13

Задания закрытого типа

1) В UNIX и UNIX-подобных операционных системах информация о пользователях, включая логин, идентификатор пользователя и его первичной группы, домашний каталог и имя программы для запуска при интерактивном входе пользователя хранится в файле

a) /etc/login

b) /etc/passwd

c) /etc/group

d) /etc/shadow

2) Пространство имен IPC в Linux

a) Создает изолированную сетевую среду для группы процессов, включая сетевые интерфейсы, фильтры и таблицы маршрутизации

b) Виртуализирует системные идентификаторы hostname и domainname

c) Изолирует объекты межпроцессного взаимодействия (семафоры, разделяемую память, очереди сообщений)

d) Изолирует процессы относительно операций mount/umount

3) Пространство имен Network в Linux

a) Создает изолированную сетевую среду для группы процессов, включая сетевые интерфейсы, фильтры и таблицы маршрутизации

b) Виртуализирует системные идентификаторы hostname и domainname

c) Изолирует объекты межпроцессного взаимодействия (семафоры, разделяемую память, очереди сообщений)

d) Изолирует процессы относительно операций mount/umount

Ответы на вопросы

Номер вопроса	Ответ (буква)
1	b
2	c
3	a

Задания открытого типа

1) Напишите команду для получения списка сетевых и интерфейсов в пространстве имен сети home

Ответы на вопросы

Номер вопроса	Ответ
1	ip netns exec home ip link show или ip netns exec home ip link list

Задания с развёрнутым ответом

1) Какое действие имеет флаг эффективных возможностей (effective) файла программы

Ответы на вопросы

Номер вопроса	Критерии оценивания
1	[Если этот флаг установлен у файла программы, то все новые возможности, которые появились в списке разрешенных возможностей потока в результате исполнения execve, будут автоматически добавлены в набор эффективных возможностей потока] Обучающийся правильно описал действие флага эффективных возможностей (effective) файла программы – 3 балла Обучающийся правильно описал действие флага эффективных возможностей (effective) файла программы. Ответ содержит незначительные неточности – 2 балла Обучающийся не достаточно точно описал действие флага эффективных возможностей (effective) файла программы. Ответ не содержит грубых ошибок или неточностей – 1 балл Обучающийся не достаточно точно описал действие флага эффективных возможностей (effective) файла программы. Ответ содержит грубые ошибки и неточности – 0 баллов

20.2 Промежуточная аттестация

Задания к контрольной работе

1. В операционной системе GNU/Linux создайте учетную запись псевдопользователя для запуска программы date
2. В операционной системе GNU/Linux определите правило sudo, которое позволяет пользователю user1 выполнять от имени user2 команды mkdir и rmdir
3. В операционной системе MS Windows создайте учетную запись пользователя Windows и разрешите ему вход в систему только с понедельника по пятницу с 8 до 17 часов
4. В операционной системе GNU/Linux определите правило sudo, которое позволяет членам группы operaror выполнять команды /mount и /umount без ввода пароля
5. В операционной системе GNU/Linux создайте правило межсетевого экрана для запрета доступа с локального компьютера к сайту www.anekdot.ru
6. В операционной системе MS Windows с использованием командной строки создайте правило брэндмауэра для блокировки входящих эхо-запросов в публичных сетях
7. В операционной системе GNU/Linux создайте учетную запись пользователя с созданием пароля при первом входе пользователя в систему и ограничьте срок действия пароля до 10 дней
8. В операционной системе MS Windows создайте учетную запись нового пользователя Windows и ограничьте срок ее действия до 10 дней
9. В операционной системе MS Windows запретите запуск редактора реестра
10. В операционной системе GNU/Linux создайте сообщение, которое будет отображаться в консоли при каждом входе пользователя в систему

Описание технологии проведения

Контрольные работы выполняются на компьютере и на проверку сдается исходный код или листинг команды интерфейса командной строки

Требования к выполнению заданий (или шкалы и критерии оценивания)

В контрольной работе все задания оцениваются в 5 баллов (максимально возможная сумма при выполнении всех заданий – 50 баллов). При ошибках в выполнении задания или не полном выполнении оценка за задание снижается. Оценка за контрольную работу определяется как сумма баллов, набранных за все задания.

Перечень вопросов к собеседованию

1. Общие требования к защите информации. Технические и административные методы защиты.
2. Политика безопасности.
3. Уровень доверия. Оценочные уровни доверия. Профиль защиты.
4. Управление доступом. Объекты, субъекты, методы доступа. Право доступа. Привилегия. Полномочия. Роль. Суперпользователь.
5. Типовые модели управления доступом (дать общее определение дискреционного управления доступом, мандатного управление доступом и изолированной программной среды)
6. Дискреционное управление доступом. Матрица доступа. Мандат возможностей. Список контроля доступа.
7. Мандатное управление доступом. Модель Белла-Лападулы.
8. Изолированная программная среда.
9. Аутентификация пользователей. Факторы аутентификации. Одноразовый пароль.
10. Многофакторная аутентификация. Хранение паролей.
11. Алгоритм проверки целостности HMAC.
12. Аутентификация HOTP на основе одноразовых паролей.
13. Аутентификация TOTP на основе одноразовых паролей.
14. Алгоритм OCRA - алгоритм взаимной аутентификации на основе взаимодействия запросответ.
15. Базовая модель разграничения доступа в UNIX-подобный системах. Маска доступа для файлов и каталогов.

16. Учет пользователей в UNIX-подобный системах. Файл /etc/passwd. Учет групп. Хранение паролей в UNIX-подобный системах.
17. Псевдопользователи. Стандартные пользователи и группы в UNIX-подобный системах. Создание нового пользователя.
18. Файлы конфигурации системы учета пользователей в Linux. Инициализация домашнего каталога нового пользователя. Стандартные утилиты управления учетными записями в Linux.
19. Linux: Вход пользователя в систему.
20. PAM. Модули PAM. Конфигурация PAM. Критерии успешной аутентификации. Расширенный стиль конфигурации в Linux.
21. Списки контроля доступа и дополнительные атрибуты файлов в файловых системах Linux.
22. Система sudo. Правила sudo. Файл sudoers. Журнал sudo.
23. Обязательный контроль целостности и контроль учетных записей в Windows
24. Ограничение использования приложений в Windows
25. Межсетевой экран Linux
26. Межсетевой экран Windows
27. Аудит безопасности в Linux
28. Аудит безопасности в Windows

Описание технологии проведения

Собеседование производится в форме устного ответа на заданный вопрос. При необходимости преподаватель может задавать уточняющие вопросы.

Требования к выполнению заданий, шкалы и критерии оценивания

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины, осуществляется в ходе текущей и промежуточной аттестаций. При оценивании результатов промежуточной аттестации используется количественная шкала оценок. Оценки за контрольную работу и лабораторные работы складываются с оценкой, полученной на собеседовании, результат нормируется к 100 бальной шкале. Полученное значение определяет уровень сформированности компетенций и итоговую оценку (достаточный – удовлетворительно, хорошо, отлично или недостаточный – неудовлетворительно) согласно следующей шкале:

- оценка «отлично» – 90…100 баллов
- оценка «хорошо» – 70…89 баллов
- оценка «удовлетворительно» – 50...69 баллов
- оценка «неудовлетворительно» – 0...49 баллов