Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Борисов Дмитрий Николаевич

Кафедра информационных систем

21.04.2021

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:**

Специалитет

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:**

8. **Учебный год:**

2023-2024

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:**

Обязательная

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-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
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-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
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-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 с использованием их недокументированных возможностей
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

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой, Контрольная работа

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 6	Всего
Аудиторные занятия	72	72
Лекционные занятия	36	36
Практические занятия		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	
1.2	Управление доступом	Объекты, субъекты и методы доступа, модели управления доступом, изолированная программная среда	
1.3	Аутентификация пользователей и проверка целостности информации	Факторы аутентификации, хранение паролей, аутентификация по открытому каналу, одноразовые пароли, многофакторная аутентификация	
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	

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	
1.6	Методы защиты информации в Windows	Дескрипторы защиты и маркеры доступа, олицетворение, списки контроля доступа в Windows	
1.7	Основы сетевой безопасности	Межсетевой экран (брандмауэр) Linux и Windows	
1.8	Аудит в операционных системах	Журналы аудита Linux и Windows, фильтры аудита	
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	
3.2	Контроль целостности файлов в Linux	Вычисление и проверка контрольной суммы, проверка целостности программы при запуске	

3.3	Изучение PAM	Реализация модуля PAM, реализующего аутентификацию по серийному номеру устройства USB	
3.4	Изучение возможностей (capabilities) Linux	Установка возможностей программы для выполнения привилегированных действий без использования root	
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/	
3.6	Изучение подсистемы sudo	Создание правила для конкретного пользователя	
3.7	Изучение подсистемы seccomp	Ограничение запуска программ и доступа к файлам за счет реализации фильтра системных вызовов	
3.8	Изучение межсетевого экрана Linux	Создание правил для netfilter, ограничивающих доступ к отдельным сетевым протоколам и портам	
3.9	Изучение механизмов ограничения запуска программ в Windows	Создание правил политики ограничения запуска программ	
3.10	Изучение межсетевого экрана Windows	Создание правил для netfilter, ограничивающих доступ к отдельным сетевым протоколам и портам	

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
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, необходимых для освоения дисциплины

№ 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 видеопроектором, компьютерами с ОС Windows с установленными средой разработки MS Visual Studio и виртуальной машиной VirtualBox с образом операционной системы GNU/Linux. Объем свободной после загрузки ОС оперативной памяти на рабочее место не менее 4 ГБ (требуется для виртуальных машин).

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	Аутентификация пользователей и проверка целостности информации	ОПК-11	ОПК-11.6	Собеседование
2	Аудит в операционных системах	ОПК-11	ОПК-11.7	Собеседование
3	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
4	Управление пользователями в Linux Изучение подсистемы sudo Контроль целостности файлов в Linux	ОПК-11	ОПК-11.9	Контрольная работа
5	Изучение межсетевого экрана Linux Изучение межсетевого экрана Windows	ОПК-11	ОПК-11.10	Контрольная работа

6	Управление пользователями в Linux Изучение подсистемы sudo Изучение механизмов ограничения запуска программ в Windows	ОПК-13	ОПК-13.1	Контрольная работа
7	Изучение PAM	ОПК-13	ОПК-13.2	Контрольная работа
8	Основы защиты информации в операционных системах	ОПК-9	ОПК-9.11	Собеседование
9	Основы защиты информации в операционных системах	ОПК-9	ОПК-9.12	Собеседование
10	Методы защиты информации в Linux Методы защиты информации в Windows	ОПК-12	ОПК-12.2	Собеседование
11	Изучение возможностей (capabilities) Linux Изучение изоляции ресурсов Linux Изучение подсистемы seccomp	ОПК-12	ОПК-12.4	Контрольная работа

Промежуточная аттестация

Форма контроля - Зачет с оценкой, Контрольная работа

Оценочные средства для промежуточной аттестации

Собеседование

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

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 равило 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 блокимровки входящих эхо-запросов в публичных сетях
7. В операционной системе GNU/Linux создайте учетную запись пользователя и ограничьте срок действия его пароля пользователя до 10 дней после установки
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.

20.2 Промежуточная аттестация

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. Многофакторная аутентификация. Хранение паролей.
10. Алгоритм проверки целостности HMAC.
11. Аутентификация HOTP на основе одноразовых паролей.
12. Аутентификация TOTP на основе одноразовых паролей.
13. Алгоритм OCRA - алгоритм взаимной аутентификации на основе взаимодействия запросответ.
14. Базовая модель разграничения доступа в UNIX-подобный системах. Маска доступа для файлов и каталогов.
15. Учет пользователей в UNIX-подобный системах. Файл /etc/passwd. Учет групп. Хранение паролей в UNIX-подобный системах.
16. Псевдопользователи. Стандартные пользователи и группы в UNIX-подобный системах. Создание нового пользователя.
17. Файлы конфигурации системы учета пользователей в Linux. Инициализация домашнего каталога нового пользователя. Стандартные утилиты управления учетными записями в Linux.
18. Linux: Вход пользователя в систему.
19. PAM. Модули PAM. Конфигурация PAM. Критерии успешной аутентификации. Расширенный стиль конфигурации в Linux.
20. Списки контроля доступа и дополнительные атрибуты файлов в файловых системах Linux.
21. Система sudo. Правила sudo. Файл sudoers. Журнал sudo.
22. Обязательный контроль целостности и контроль учетных записей в Windows
23. Ограничение использования приложений в Windows
24. Межсетевой экран Linux

25. Межсетевой экран Windows
26. Аудит безопасности в Linux
27. 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. Оценка за контрольную работу складываются с оценкой, полученной на собеседовании, и 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