Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.31 Защита в операционных системах»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2024

Рабочая программа дисциплины «*Б1.Д.Б.31 Защита в операционных системах*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 8 от "25" марта 2024г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем — И.В. Влацкая
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент — И.А. Щудро
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность — И.В. Влацкая
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

© Щудро И.А., 2024
© ОГУ, 2024

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование знаний, умений, навыков и компетенций у студентов по основным методам и технологиям защиты информации в операционных системах.

Задачи:

Разработка проектов систем и подсистем защищенных операционных систем в соответствии с техническим заданием;

Проведение инструментального мониторинга защищенности объекта;

Поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения;

Установка, настройка, эксплуатация и обслуживание аппаратно-программных средств защиты информации;

Обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.13 Информатика, Б1.Д.Б.19 Операционные системы, Б1.Д.Б.20 Компьютерные сети*

Постреквизиты дисциплины: *Б2.П.В.П.1 Производственная практика (по специализации), Б2.П.В.П.2 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	ОПК-12-В-1 Знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей ОПК-12-В-2 Знает основные принципы конфигурирования и администрирования операционных систем ОПК-12-В-3 Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями ОПК-12-В-4 Владеет навыками системного программирования	**Знать:** основные методы и технологии защиты в операционных системах **Уметь:** производить установку, настройку и тестирование современного общего и специального программного обеспечения **Владеть:** способностью обеспечить восстановление работо-способности систем защи-ты информации при воз-никновении нештатных ситуаций

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**61,25**	**61,25**
Лекции (Л)	30	30
Лабораторные работы (ЛР)	30	30
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса «Защита в операционных системах» в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю и т.п.)*	**82,75**	**82,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Понятие защищенной операционной системы	28	6		6	16
2	Управление доступом в операционных системах семейства Unix	28	6		6	16
3	Идентификация, аутентификация и авторизация	28	6		6	16
4	Аудит операционной системы	28	6		6	16
5	Интеграция операционных систем в защищенную сеть	32	6		6	20
	Итого:	144	30		30	84
	Всего:	144	30		30	84

4.2 Содержание разделов дисциплины

Понятие защищенной операционной системы

Угрозы безопасности операционной системы, классификация угроз, наиболее распространенные угрозы. Понятие защищенной операционной системы. Подходы к организации защиты. Этапы построения защиты. Административные меры защиты.

Управление доступом в операционных системах семейства Unix

Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Требования к правилам управления доступом. Дискреционное управление доступом. Матрица доступа. Изолированная программная среда. Мандатное управление доступом. Метки доступа. Контроль информационных потоков. Проблемы реализации мандатного управления доступом в операционных системах.

Управление доступом в операционных системах семейства UNIX. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Атрибуты защиты объектов доступа.

Средства динамического изменения полномочий субъектов: SUID/SGID. Расширения стандартной системы управления доступом в SCO UNIX, Solaris, Linux.

Контроль целостности: мандатный, дискреционный, регламентный, динамический.

Идентификация, аутентификация и авторизация

Понятия идентификации, аутентификации и авторизации пользователей. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей.

Аутентификация на основе паролей. Средства и методы защиты от компрометации и подбора паролей. Парольная аутентификация в UNIX, библиотеки PAM. Парольная аутентификация в Windows, средства управления параметрами аутентификации.

Аутентификация на основе внешних носителей ключа. Особенности проверки аутентификационной информации для различных типов носителей ключа. Проблемы генерации, рассылки и смены ключей.

Биометрическая аутентификация: общая схема, преимущества, проблемы. Достоинства и недостатки различных схем биометрической аутентификации.

Аудит

Необходимость аудита в защищенной системе. Требования к подсистеме аудита. Реализация аудита в UNIX системах. Системы обнаружения вторжений (IDS). Системы предотвращения вторжений (IPS).

Интеграция защищенных операционных систем в защищенную сеть

Преимущества доменной архитектуры локальной сети. Понятие домена, контроллер домена. Сквозная аутентификация, возникающие проблемы и способы их решения. Порядок наделения пользователей домена полномочиями на отдельных компьютерах. Централизованное управление политикой безопасности в домене.

Идентификация компьютеров в сети. Двусторонние транзитивные отношения доверия. Средства и методы синхронизации баз данных контроллеров разных доменов одного леса. Аутентификация по Kerberos. Групповая политика. Делегирование полномочий.

4.3 Лабораторные работы

№ ЛР	Наименование лабораторных работ	Кол-во часов
1	Настройка и интеграция ОС семейства Unix	4
2	Управление доступом в Astra Linux	4
3	Настройка фильтрации и маршрутизации в Astra Linux	4
4	Аудит обнаружения вторжений в Astra Linux	4
5	Идентификация, аутентификация и авторизация в Astra Linux	4
6	Исследование методов контроля целостности и мандатного управления доступом в Astra Linux. Графический и системный киоски в Astra Linux.	4
7	Сертификация Astra Linux в ООО «КРИПТО-ПРО»	4
8	Установка обновлений безопасности в Astra Linux	2
	Итого:	30

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Проскурин, В. Г. Защита программ и данных [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 "Информационная безопасность" (бакалавр) и специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем" / В. Г. Проскурин.- 2-е изд., стер. - Москва: Академия, 2012. - 208 с. : ил. - (Высшее профессиональное образование. Бакалавриат). - Библиогр.: с. 195-196. - ISBN 978-5-7695-9288-1.

5.2 Дополнительная литература

1. Вицентий, А.В. Основы практической работы с UNIX-подобной операционной системой : учебное пособие / А.В. Вицентий, Е.С. Рудина, М.Г. Шишаев. – Мурманск : МАГУ, 2019. – 96 с. – ISBN 978-5-4222-0388-8. – Текст : электронно-библиотечная система. – URL: https://e.lanbook.com/book/140984 (дата обращения: 04.04.2024). – Режим доступа: для авториз. Пользователей.

5.3 Периодические издания

1. Вестник компьютерных и информационных технологий: журнал. - М.: Агентство "Роспечать", 2018.
2. Информационные технологии: журнал. - М. : Агентство "Роспечать", 2018.

5.4 Интернет-ресурсы

1. https://wiki.astralinux.ru - Справочный центр Astra Linux.
2. https://studylib.ru/doc/6530125/1.7.4-ruk-ksz-1 - Операционная система специального назначения «Astra Linux SE». Руководство по КСЗ часть 1. РУСБ.10015-01 97 01-1.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021.
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Антивирусное ПО: Kaspersky Endpoint Security для бизнеса, имеется лицензия на 2 года использования, входит в Реестр отечественного ПО
4. Система программирования Python, свободно распространяемая по лицензии PSFL.
5. Интегрированная среда разработки ПО NetBeans, свободно распространяемая по лицензии Apache.
6. Система управления базами данных MySQL, свободно распространяемая по лицензии GPL.
7. Система программирования Oracle Java SE JDK, бесплатно распространяемая по лицензии Oracle Technology Network License.
8. Веб-сервер Apache. Разработчик: сообщество Linux foundation. Свободно распространяемое ПО. Режим доступа: https://httpd.apache.org/download.cgi
9. СУБД MySql Community Server. Разработчик: Oracle. Доступен для скачивания бесплатный вариант Community Server (свободно-распространяемое ПО). Режим доступа: https://dev.mysql.com/downloads/mysql

10. Операционная система Linux Ubuntu Server. Разработчик: Canonical. Свободно распространяемое ПО. Режим доступа: https://www.ubuntu.com/download/server
11. Math-Net.ru [Электронный ресурс]: общероссийский математический портал, включающий информационно-справочную систему по публикациям в отечественных математических журналах. – Режим доступа http://www.mathnet.ru/.
12. Wolfram|Alpha [Электронный ресурс]: база знаний и справочная система, включающая множество вычислительных алгоритмов. – Режим доступа https://www.wolframalpha.com/
13. CITforum.ru Аналитическая информация по всем областям компьютерной сферы (http://www.citforum.ru/).

Базы данных, информационно-справочные и поисковые системы:

- Консультант Плюс, Режим доступа: https://www.consultant.ru/cons/cgi/online.cgi
- Открытые поисковые системы: Yandex, Mail и др.

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерами и мультимедийными средствами. Рабочие станции студентов и преподавателей объединены в локальную компьютерную сеть с возможностью выхода в Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием.

Лабораторные занятия проводятся в компьютерных классах, в которых установлено оборудование:

- системные блоки на базе процессора Intel Core i5;
- системные блоки на базе процессора Intel Pentium Core 2 Duo;
- мониторы моделей Samsung, ViewSonic.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.