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.В.Э.3.1 Защита информации в высокопроизводительных 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.В.Э.3.1 Защита информации в высокопроизводительных системах*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 8 от "25" марта 2024 г.

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

Исполнители:
Доцент — Ю.Д. Фот
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 _____

© Фот Ю.Д., 2024
© ОГУ, 2024

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: *формирование у обучающихся знаний и умений, необходимых для обеспечения защиты информации в высокопроизводительных системах.*

Задачи:

Знать:

Основные угрозы безопасности информации в высокопроизводительных системах

Методы и средства защиты информации в высокопроизводительных системах

Нормативно-правовые основы защиты информации

Особенности защиты информации в различных типах высокопроизводительных систем

Уметь:

Разрабатывать и реализовывать комплексные меры защиты информации в высокопроизводительных системах

Использовать методы и средства защиты информации в высокопроизводительных системах

Осуществлять контроль и мониторинг безопасности информации в высокопроизводительных системах

Проводить расследование инцидентов информационной безопасности

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.10 Информатика*

Постреквизиты дисциплины: *Отсутствуют*

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
ПК*-3 Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей	ПК*-3-В-1 Знает основные требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей ПК*-3-В-2 Способен осуществлять разработку и тестирование средств защиты информации компьютерных систем и сетей ПК*-3-В-3 Владеет основными методами защиты информации компьютерных систем и сетей	**Знать:** Основные угрозы безопасности информации в высокопроизводительных системах Программно-аппаратные средства защиты информации в высокопроизводительных системах Нормативно-правовые основы защиты информации Особенности защиты информации в различных типах

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		высокопроизводительных систем **Уметь:** осуществлять контроль и мониторинг безопасности информации, расследование инцидентов информационной безопасности, тестирование и анализ защищенности информационных систем, администрирование систем защиты информации; уметь работать с различными инструментами разработки и использования программно-аппаратных средств защиты информации **Владеть:** Навыками контроля и мониторинга безопасности информации в высокопроизводительных системах Навыками расследования инцидентов информационной безопасности в высокопроизводительных системах Навыками тестирования и анализа защищенности высокопроизводительных систем Навыками администрирования систем защиты информации в высокопроизводительных систем

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	10 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**74,25**	**74,25**
Лекции (Л)	30	30
Лабораторные работы (ЛР)	44	44
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- написание реферата (Р);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);* *- изучение разделов электронного курса «Защита информации в высокопроизводительных системах» в системе обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю.*	**69,75**	**69,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 10 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Сети и системы передачи информации в высокопроизводительных системах	86	16		30	40
2	Безопасная эксплуатация высокопроизводительных систем. Расследование инцидентов информационной безопасности в высокопроизводительных системах	58	14		14	30
	Итого:	144	30		44	70
	Всего:	144	30		44	70

4.2 Содержание разделов дисциплины

Раздел №1. Сети и системы передачи информации в высокопроизводительных системах

Маршрутизируемые сети. Основы коммутации. Виртуальные локальные сети, построение магистральных каналов. Маршрутизация между VLAN. Статистическая маршрутизация. Протокол динамической маршрутизации OSPF. Протокол динамической маршрутизации BGP. Безопасность маршрутизируемой инфраструктуры. Безопасность коммутируемой инфраструктуры. Виртуальные частные сети. Реализация сервисов высокой доступности. Качество обслуживания в компьютерных сетях. Мониторинг и диагностика компьютерной сети. Виртуальные частные сети. Реализация сервисов высокой доступности. Качество обслуживания в высокопроизводительных сетях. Мониторинг и диагностика высокопроизводительных сетей.

Раздел №2. Безопасная эксплуатация высокопроизводительных систем. Расследование инцидентов информационной безопасности в высокопроизводительных системах

Средства аутентификации и авторизации. Шифрование. Контроль доступа. Межсетевые экраны. Системы обнаружения вторжений. Системы предотвращения вторжений.

Управление обновлениями: установка патчей, исправление уязвимостей

Резервное копирование и восстановление: защита от сбоев, восстановление данных

Мониторинг безопасности: анализ журналов, выявление угроз

Реагирование на инциденты: расследование инцидентов, восстановление работоспособности

Обучение пользователей: повышение осведомленности о безопасности

Восстановление удаленных данных с образа. Сканирование корпоративной инфраструктуры. Восстановление удаленных данных с образа. Сбор информации о доменах, IP-адресах, подсетях, URL-адресах, именах хостов, веб-технологиях и т.д.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Маршрутизируемые сети. Основы коммутации.	2
2	1	Виртуальные локальные сети, построение магистральных каналов.	2
3	1	Маршрутизация между VLAN	2
4	1	Статистическая маршрутизация	2
5	1	Протокол динамической маршрутизации OSPF. Протокол динамической маршрутизации BGP	2
6	1	Безопасность маршрутизируемой инфраструктуры	2
7	1	Безопасность коммутируемой инфраструктуры	2
8	1	Виртуальные частные сети	2
9	1	Реализация сервисов высокой доступности	2
10	1	Качество обслуживания в компьютерных сетях	2
11	1	Мониторинг и диагностика компьютерной сети	2
12	1	Виртуальные частные сети	2
13	1	Реализация сервисов высокой доступности	2
14	1	Качество обслуживания в высокопроизводительных сетях	2
15	1	Мониторинг и диагностика высокопроизводительных сетей.	2
16	2	ProDiscover	2
17	2	Сбор данных Sysinternals	2
18	2	Анализ файловой системы в Sleuth Kit	2
19	2	Восстановление удалённых Файлов Autopsy	2
20	2	Работа с дампами памяти в Bulk Extractor	2
21	2	Анализ дампа памяти с использованием Volatility	2
22	2	Восстановление удаленных данных с образа. Scalpel.	2
		Итого:	44

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Киренберг, Информационная безопасность современных операционных систем : учебное пособие / Киренберг, Г. А. . — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/295736 (дата обращения: 18.03.2024). — Режим доступа: для авториз. пользователей

2. Системы хранения данных : учебное пособие / Д. В. Гадасин, Д. Д. Рахмани, В. В. Маклачкова [и др.]. — Москва : МТУСИ, 2022. — 150 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333794 (дата обращения: 18.03.2024). — Режим доступа: для авториз. пользователей.

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак : учебное пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. — Москва : РТУ МИРЭА, 2022. — 120 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/311249 (дата обращения: 18.03.2024). — Режим доступа: для авториз. пользователей.

5.2 Дополнительная литература

1. Рылов, С. А. Промышленный интернет. Современный подход и концепции : учебник / С. А. Рылов. — Москва : РТУ МИРЭА, 2023. — 124 с. — ISBN 978-5-7339-1969-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/386144 (дата обращения: 18.03.2024). — Режим доступа: для авториз. пользователей.

2. Импортозамещающие технологии обеспечения информационной безопасности и защиты данных : учебное пособие / Д. А. Короченцев, Л. В. Черкесова, Е. А. Ревякина [и др.]. — Ростов-на-Дону : Донской ГТУ, 2021. — 335 с. — ISBN 978-5-7890-1893-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237782 (дата обращения: 18.03.2024). — Режим доступа: для авториз. пользователей.

3. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев.- 4-е изд., стер. - М. : Академия, 2008. - 256 с. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 251-252. - ISBN 978-5-7695-5118-5.

4. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для вузов / П. Н. Девянин [и др.]. - М. : Радио и связь, 2000. - 192 с. : ил. - Авт. указаны на обороте тит. л.. - Библиогр. в конце гл. - ISBN 5-256-01413-7.

5. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 10.03.2022). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

5.3 Периодические издания

1. Информация и безопасность : журнал. - М. : Агентство "Роспечать".
2. Вестник информационной безопасности : журнал. - М. : Агенство "Роспечать".
3. Системы безопасности : журнал. - М. : Агентство "Роспечать".
4. Проблемы информационной безопасности. Компьютерные системы : журнал. - М. : АПР.

5.4 Интернет-ресурсы

1. Безопасность IIS: Информация. – Режим доступа: https://intuit.ru/studies/courses/1002/122/info

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

а) программно-аппаратное обеспечение:

1. Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021

2. Open Office/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.

б) базы данных, информационно-справочные и поисковые системы:

– Консультант Плюс [Электронный ресурс] : справочно-правовая система / Компания Консультант Плюс. – Электрон. дан. – Москва, [1992–2016]. – Режим доступа : в локальной сети ОГУ \\fileserver1\!CONSULT\cons.exe

– Гарант [Электронный ресурс] : справочно-правовая система / НПП Гарант-Сервис. – Электрон. дан. - Москва, [1990–2016]. – Режим доступа \\fileserver1\GarantClient\garant.exe. В локальной сети ОГУ.

– Законодательство России [Электронный ресурс] : информационно-правовая система. – Режим доступа : http://pravo.fso.gov.ru/ips/, в локальной сети ОГУ.

– Открытые поисковые системы

– OWASP https://owasp.org/www-project-top-ten//

– CVE https://cve.mitre.org//

– Common Attack Pattern Enumeration and Classification (CAPEC) https://capec.mitre.org/.

– Банк данных угроз безопасности информации https://bdu.fstec.ru/vul.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, курсового проектирования, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный персональными компьютерами с установленным программным обеспечением.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

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