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.32 Основы построения защищенных компьютерных сетей»

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.32 Основы построения защищенных компьютерных сетей*» 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 — Н.П. Мошуров
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 факультета
И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

© Мошуров Н.П., 2024
© ОГУ, 2024

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Задачи:

- изучение базовых понятий защиты информации в компьютерных сетях;
- изучение принципов межсетевого экранирования;
- изучение принципов построения виртуальных частных сетей;
- изучение основ шифрования данных в компьютерных сетях;
- изучение основ работы систем обнаружения вторжения;
- изучение встроенных средств обеспечения безопасности современных сетевых операционных систем;
- изучение принципов безопасного подключения локальных сетей к Интернету;
- изучение методов обеспечения безопасности беспроводных сетей.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.10 Информатика, Б1.Д.Б.25 Операционные системы, Б1.Д.Б.26 Компьютерные сети, Б1.Д.Б.28 Основы информационной безопасности, Б1.Д.Б.29 Модели безопасности компьютерных систем, Б1.Д.Б.35 Электроника и схемотехника*

Постреквизиты дисциплины: *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-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-В-1 Знает основные виды политик управления доступом и информационными потоками в компьютерных системах ОПК-11-В-2 Знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков ОПК-11-В-3 Умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками ОПК-11-В-4 Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и	**Знать:** - основные нормативно-правовые документы по защите информации в компьютерных сетях в Российской Федерации и за рубежом; - основные требования к подсистеме аудита и политике аудита; - защитные механизмы и средства обеспечения безопасности операционных систем. **Уметь:** - формулировать и настраивать политику

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	информационными потоками в компьютерных системах	безопасности основных операционных систем; - формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем. **Владеть:** - навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	ОПК-16-В-1 Способен применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях ОПК-16-В-2 Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты ОПК-16-В-3 Владеет навыками настройки межсетевых экранов и методиками анализа сетевого трафика ОПК-16-В-4 Владеет методиками анализа сетевого трафика	**Знать:** - руководящие и нормативно-правовые документы по оценке уровня защищенности информации в компьютерных системах. **Уметь:** - оценивать уровень защищенности информации в компьютерных системах в части используемых компьютерных сетей; - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях **Владеть:** - навыками составления отчетов по результатам проводимых оценок; - навыками настройки межсетевых экранов и методиками анализа сетевого трафика; - методиками анализа сетевого трафика.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**69,25**	**69,25**
Лекции (Л)	34	34
Лабораторные работы (ЛР)	34	34
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 «Основы построения защищенных компьютерных сетей» в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю и т.п.)*	**74,75**	**74,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1.	Введение в предмет	8	2			6
2.	Межсетевые экраны	20	6		6	8
3.	Виртуальные частные сети	18	6		6	6
4.	Шифрование в компьютерных сетях	16	4		6	6
5.	Системы обнаружения вторжений	24	2		4	18
6.	Безопасность сетевых операционных систем	18	6		4	8
7.	Безопасное подключение к сети Интернет	16	4		4	8
8.	Безопасность беспроводных сетей	24	4		4	16
	Итого:	144	34		34	76
	Всего:	144	34		34	76

4.2 Содержание разделов дисциплины

№ 1 Введение в предмет. Понятие информационной безопасности. История развития информационной безопасности. Современные стандарты обеспечения информационной безопасности. Основные компоненты защиты информации.

Понятие атаки. Категории атак. Механизмы проведения атак.

Службы информационной безопасности. Проблема конфиденциальности, целостности и доступности информации в компьютерных сетях.

Политики информационной безопасности. Методика разработки политик, создания, развертывания и эффективного использования.

Выявление и оценка возможных рисков в компьютерных сетях.

Обеспечение информационной безопасности. Оценка стоимости проведения мероприятий по безопасности. Разработка и реализации политики безопасности, аудита систем.

Рекомендации по обеспечению сетевой безопасности. Стандарт ISO 17799.

№ 2 Межсетевые экраны. Понятие межсетевого экрана. Классификация межсетевых экранов. Типы окружений межсетевых экранов. Принципы настройки межсетевых экранов. Примеры атак, предотвращаемых межсетевыми экранами. Атаки на сетевые экраны.

№ 3 Виртуальные частные сети. Понятие VPN. Типы VPN. Стандартные технологии функционирования VPN. Программное обеспечение для организации VPN.

№ 4 Шифрование в компьютерных сетях. Понятие шифрования. Виды шифрования. Принципы шифрования информации, хранимой или передаваемой в компьютерной сети. Протокол Kerberos.

№ 5 Системы обнаружения вторжений. Понятие Intrusion Detection Systems (IDS). Причины использования IDS. Классификация IDS. Возможные ответные действия IDS на вторжения. Развертывание IDS. Создание Honey Pot и Padded Cell. Развертывание и комбинирование IDS различного типа. Способы обработки выходной информации IDS. Типы атак, выявляемых IDS.

№ 6 Безопасность сетевых операционных систем. Безопасность операционной системы Unix/Linux. Управление пользователями и группами. Аутентификация пользователей. Безопасные сетевые настройки. Поиск вторжений.

Безопасность операционной системы Windows. Управление пользователями и группами. Аутентификация пользователей. Безопасные сетевые настройки. Поиск вторжений.

№ 7 Безопасное подключение к сети Интернет. Архитектура интернета. Организация безопасного доступа к Интернет сотрудников компании. Защита от случайных или преднамеренных утечек конфиденциальной информации. Организация подключения к Интернет, проектирование DMZ.

№ 8 Безопасность беспроводных сетей. Принципы организации беспроводных сетей. Протоколы WEP, WPA. Перехват и защита беспроводного траффика. Обеспечение безопасности домашней и корпоративной беспроводной сети.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1.	2	Встроенный межсетевой экран Windows. Межсетевой экран Comodo Personal Firewall	2
2.	2	Настройка межсетевых экранов в сетевом оборудовании	4
3.	3	Организация виртуальных частных сетей в Windows и Linux	6
4.	4	Встроенные средства Windows и Linux для шифрования данных в компьютерной сети	6
5.	5	Узловые и сетевые системы обнаружения вторжений	4
6.	6	Управления пользователями в Windows и Linux. Реализация политик безопасности	4
7.	7	Безопасное подключение к сети интернет	4
8.	8	Безопасность беспроводных сетей	4
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 284 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110336
2. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст] : учеб. пособие для вузов / В. В. Платонов. - М. : Академия, 2006. - 240 с. - (Высшее профессиональное образование). - Библиогр.: с. 235-236. - ISBN 5-7695-2706-4.
3. Галатенко, В. А. Основы информационной безопасности [Текст] : курс лекций: учеб. пособие / В. А. Галатенко; под ред. В. Б. Бетелина.- 2-е изд., испр. - М. : Интернет-Ун-т Информ. Технологий, 2004. - 264 с. - (Основы информационных технологий) - ISBN 5-9556-0015-9.

5.2 Дополнительная литература

1. Защита компьютерной информации : учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 146 с. — ISBN 978-5-907054-82-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157086

2. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837

3. Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176657

4. Панфилов, И. В. Проблемы защиты информации в компьютерных сетях и системах : учебное пособие / И. В. Панфилов, А. М. Заяц, Е. И. Панфилова. — Санкт-Петербург : СПбГЛТУ, 2008. — 148 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/45554

5.3 Периодические издания

1. Вестник информационной безопасности : журнал. - М. : Агенство "Роспечать".
2. Системы безопасности : журнал. - М. : Агентство "Роспечать".
3. Проблемы информационной безопасности. Компьютерные системы : журнал. - М. : АПР.
4. Вестник УрФО Безопасность в информационной сфере : журнал. - Челябинск :ЮУрГУ, 2011.

5.4 Интернет-ресурсы

1. Сети для самых маленьких. Часть нулевая. Планирование. – Режим доступа: https://habrahabr.ru/post/134892/
2. Мэйволд, Э. Безопасность сетей //Учебные курсы национального открытого университета "Intuit". – Режим доступа: http://www.intuit.ru/department/security/netsec/.
3. Лапонина, О.Р. Межсетевое экранирование //Учебные курсы национального открытого университета "Intuit". – Режим доступа: http://www.intuit.ru/department/network/firewalls/.

4. https://www.intuit.ru/studies/courses/102/102/info – «Интуит. Национальный открытый университет». Курсы, МООК: **Безопасность сетей**

5. https://www.intuit.ru/studies/courses/59/59/info– «Интуит. Национальный открытый университет». Курсы, МООК: **Протоколы безопасного сетевого взаимодействия**

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

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 организации виртуальных частных сетей OpenVPN текущей версии. Доступна бесплатно по свободной лицензии GNUGPL. Разработчик: OpenVPN Technologies. Режим доступа: https://openvpn.net

6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерным и мультимедийным оборудованием. Рабочие станции студентов и преподавателя объединены в локальную сеть с подключением к Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным проектором и экраном.

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

- системные блоки с процессором IntelCore 2 Duo;
- мониторы модели Samsung 793 DF.

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

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерным и мультимедийным оборудованием. Рабочие станции студентов и преподавателя объединены в локальную сеть с подключением к Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным проектором и экраном.

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

- системные блоки с процессором IntelCore 2 Duo;
- мониторы модели Samsung 793 DF.

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.