Минобрнауки России

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

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.Э.6.1 Информационная безопасность в сетях и телекоммуникациях»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2024

Рабочая программа дисциплины «*Б1.Д.В.Э.6.1 Информационная безопасность в сетях и телекоммуникациях*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 10 от "18" 03 2024 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации — В.В. Тугов
наименование кафедры *подпись* *расшифровка подписи*

Исполнитель:
Доцент кафедры ВТиЗИ — М.В. Ушакова
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность — В.В. Тугов
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 _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

изучение современных способов защиты информационных систем и сетей, формирование знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи:

– ознакомление со стандартами и современными тенденциями развития сетевой безопасности;

– получение знаний об анализируемых показателях безопасности сетей передачи данных и автоматизированных систем

– ознакомление с политикой безопасности предприятий и компаний в области защиты информации;

– формирование знаний и практических навыков, необходимых для обеспечения безопасного функционирования сетевой инфраструктуры;

– формирование навыков установки и настройки средств защиты информации в автоматизированных системах и СПД

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.6 Основы информационной безопасности, Б1.Д.Б.9 Сети и системы передачи информации, Б1.Д.Б.10 Программно-аппаратные средства защиты информации, Б1.Д.Б.19 Методы и средства криптографической защиты информации, Б1.Д.В.7 Защита и обработка конфиденциальных документов*

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
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2-В-1 Понимает классическую структуру проекта с учетом оптимизации ресурсного обеспечения, способы представления проекта УК-2-В-2 Формулирует цели и задачи проекта, структурирует этапы процесса организации проектной деятельности УК-2-В-3 Применяет элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта УК-2-В-4 В рамках цели проекта опирается на правовые нормы основных отраслей российского законодательства	**Знать:** сущность и принципы проектирования; основы правового обеспечения при организации проектной деятельности; классическую структуру проекта с учетом оптимизации ресурсного обеспечения; **Уметь:** определять круг задач для организации деятельности по созданию и

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	при постановке целей и выборе оптимальных способов их достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов	продвижению проекта; формулировать цели и задачи проекта; уметь структурировать этапы процесса организации проектной деятельности. **Владеть:** навыками стратегического развития идеи в проект в рамках поставленной цели с учетом действующих правовых норм, имеющихся ресурсов и ограничений; навыками применения элементов анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта
ПК*-4 Способен осуществлять мониторинг защищенности информации в автоматизированных системах	ПК*-4-В-1 Выбирает оптимальные методы наблюдения, контроля и принятия решения по принятию мер обеспечения требуемой защищенности информации в автоматизированных системах ПК*-4-В-2 Знает основные методы оценки требуемой защищенности информации в автоматизированных системах	**Знать:** характеристики оборудования и протоколов, стандартов СКС, элементов защиты сети **Уметь:** устанавливать и настраивать средства защиты информации в автоматизированных системах и СПД, применять современные методы и средства для диагностики уровня защищенности автоматизированных систем **Владеть:** навыками мониторинга безопасности сетей и автоматизированных систем
ПК*-7 Способен разрабатывать организационно-распорядительные документы в автоматизированных системах	ПК*-7-В-1 Опираясь на правовые нормы готовит организационно-распорядительные документы в автоматизированных системах ПК*-7-В-2 Знает основные виды организационно-распорядительных документов в области защиты	**Знать:** Организационно-правовые нормы информационной в сетях и автоматизированных системах **Уметь:**

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	информации автоматизированных систем	администрировать подсистему информационной безопасности в сетях и автоматизированных системах **Владеть:** навыками решения оперативных задач обеспечения информационной безопасности в сетях и автоматизированных системах, навыками применения организационно-распорядительных документов в области защиты информации автоматизированных систем

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**43,25**	**43,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	6	6
Лабораторные работы (ЛР)	18	18
Консультации	1	1
Промежуточная аттестация (экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**64,75**	**64,75**
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	Правовые основы информационной безопасности в компьютерных сетях	16	2	2		12
2	Общие принципы обеспечения безопасности сети	24	6		2	16
3	Основы тестирования сети на проникновение	44	8	2	12	22
4	Методы социальной инженерии	24	2	2	4	16
	Итого:	108	18	6	18	66
	Всего:	108	18	6	18	66

4.2 Содержание разделов дисциплины

№ 1 Правовые основы информационной безопасности в компьютерных сетях

Политика информационной безопасности. Органы обеспечения информационной безопасности. Лицензирование деятельности в области информационной безопасности компьютерных сетей. Сертификация средств защиты информации компьютерных сетей. Нормативно-правовые основы информационной безопасности в РФ.

№ 2 Общие принципы обеспечения безопасности сети

Безопасность оконечных устройств. Контроль доступа. Угрозы безопасности на уровне 2. Атаки на локальную сеть. Текущий уровень кибербезопасности. Инструменты злоумышленников. Уязвимости протоколов IP, TCP, UDP. Практические рекомендации по обеспечению сетевой безопасности. Классификация удаленных угроз в вычислительных сетях.

№ 3 Основы тестирования сети на проникновение

Методы тестирования на проникновение. Типовые факторы возникновения угроз безопасности. Этапы тестирования на проникновение. Методы сбора информации. Сканирование сети, портов, уязвимостей. Определение активных сервисов в сети. Уязвимости: понятие, номенклатура, типы. Поиск и эксплуатация уязвимостей. Парольные атаки на различные сервисы. Использование фреймворка Metasploit для поиска и эксплуатации уязвимостей. Тестирование веб-приложений

№4 Методы социальной инженерии.

Принципы, формирующие цели и видение социального инженера. Моделирование психологии человека. Методы атаки социальной инженерии. Процесс и типы атак методами социальной инженерии. Инструменты социальной инженерии.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2,3	Установка и настройка элементов инфраструктуры сетевой лаборатории	2
2	3	Применение инструментов Kali Linux для сканирования сети	2
3	3	Применение инструментов Kali Linux для сканирования портов и определения активных сервисов элементов инфраструктуры сетевой лаборатории	2
4	3	Изучение принципов парольных атак на различные сервисы	2
5	3	Использование фреймворка Metasploit для поиска и эксплуатации уязвимостей	2
6	3,4	Изучение открытой системы оценки уязвимостей OpenVAS	4
7	3,4	Поиск уязвимостей веб-приложения с помощью фреймворка	4

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
		Metasploit	
		Итого:	18

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Нормативно-правовые основы информационной безопасности в РФ	2
2	3	Использование поисковых систем для проведения этапа «разведки» при тестировании на проникновение	2
3	4	Исследование инструментов социальной инженерии	2
		Итого:	6

5 Учебно-методическое обеспечение дисциплины

1. Организационно-правовое обеспечение информационной безопасности [Текст] : учеб. пособие для студентов вузов, обучающихся по специальностям 090102 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммукационных систем" / [А. А. Стрельцов и др.]; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с. - (Высшее профессиональное образование). - Авт. указаны на обороте тит. л. - Библиогр.: с. 242-245. - ISBN 978-5-7695-4240-4

5.2 Дополнительная литература

1. Васильков, А. В. Безопасность и управление доступом в информационных системах [Текст] : учебное пособие для студентов образовательных учреждений среднего профессионального образования / А. В. Васильков, И. А. Васильков. - Москва : Форум : ИНФРА-М, 2014. - 368 с. : ил. - (Профессиональное образование). - Библиогр.: с. 356-358. - Предм. указ.: с. 359-363. - ISBN 978-5-91134-360-6. - ISBN 978-5-16-006736-0.

2. Правовое обеспечение информационной безопасности [Текст] : учеб. пособие для вузов / под ред. С. Я. Казанцева.- 2-е изд., испр. и доп. - М. : Академия, 2007. - 240 с. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 234. - ISBN 978-5-7695-3635-9.

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] : учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. - Москва : Форум : ИНФРА-М, 2014. - 416 с. : ил. - Библиогр.: с. 401-408. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3.

5.4 Интернет-ресурсы

www.citforum.ru/ - портал аналитических и научных статей в области информационных технологий;

https://openedu.ru/course/ITMOUniversity/INFSEC/?session=self_2024 - «Открытое образование», Каталог курсов, МООК: «Информационная безопасность»;

https://www.cybrary.it/course/ethical-hacking - «Cybrary.it», МООК: «Penetration Testing and Ethical Hacking»;

https://www.edx.org/learn/information-security/ec-council-ethical-hacking-essentials-ehe?irclickid=x3kTxqXNdxyPRiU0Fm3oG3FEUkHUrD0YPT-4wE0&utm_source=affiliate&utm_medium=guru99&utm_c

ampaign=Online%20Tracking%20Link_&utm_content=ONLINE_TRACKING_LINK&irgwc=1 - «EDX», МООК: «EC-Council: Ethical Hacking Essentials (EHE)»;

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС для рабочих станций, имеется лицензия, входит в реестр отечественного ПО.
2. LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Система управления учебным процессом Moodle, свободно распространяемая.
4. Программная система для организации видео-конференц-связи Webinar.ru, имеется лицензия, входит в реестр отечественного ПО.
5. Программа для просмотра сайтов Яндекс.Браузер, свободно распространяемая, входит в реестр отечественного ПО.
6. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2023]. – Режим доступа в сети ОГУ для установки системы: \\fileserver1\GarantClient\garant.exe
7. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2023]. – Режим доступа к системе в сети ОГУ для установки системы: \\fileserver1\!CONSULT\cons.exe

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, 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 компьютерами с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду ОГУ и лаборатория периферийных средств и сетевых технологий. Используется оборудование: Стойка 19"; коммутатор D-Link DES-1100-26; коммутатор D-Link DES-3526; коммутатор D-Link DFL-260E; коммутатор Cisco <SRW208MP-K9-EU>SF302-8MP; экран межсетевой Cisco ASA5505-K8; "Глонасс-GPS"- модуль типа "SIM908"; модуль беспроводной связи Xbee; антенна РЭМО ВОЛНА-digital; антенна АШ-433(М).

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