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 2022

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 № 9 от "31" 03 2022 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации Т.З. Аралбаев
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент кафедры ВТ и ЗИ А.Л. Коннов
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность Т.З. Аралбаев
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
И.В. Крюкова
личная подпись *расшифровка подписи*

№ регистрации 4.19528

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: является изучение современных способов защиты информационных систем и сетей, формирование знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств

Задачи:

- изучение методов и средств защиты информации в компьютерных сетях;
- изучение технологии межсетевого экранирования;
- исследование методов и средств построения защищенных виртуальных частных сетей;
- исследование методов и средств проведения аудита уровня защищенности в сетях и телекоммуникациях.

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-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1-В-1 Применяет философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач УК-1-В-2 Осуществляет критический анализ и синтез информации, полученной из разных источников УК-1-В-3 Понимает основные закономерности и главные особенности социально-исторического развития различных культур в этическом и философском контексте УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с применением философского понятийного аппарата	**Знать:** Теоретические основы и методы поиска, критического анализа и синтеза информации, применения системного подхода для решения поставленных задач **Уметь:** осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач **Владеть:** навыками поиска, критического анализа и синтеза информации, применения системного подхода для решения поставленных задач

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	УК-1-В-6 Формулирует собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий	
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 при постановке целей и выборе оптимальных способов их достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов	**Знать:** теоретические основы и методы определения круга задач в рамках поставленной цели и выбора оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Уметь:** определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеть:** навыками определения круга задач в рамках поставленной цели и выбора оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ПК*-1 Способен диагностировать системы защиты автоматизированных систем	ПК*-1-В-1 Применяет современные методы и средства диагностирования автоматизированных систем	**Знать:** теоретические основы и методы диагностирования системы защиты автоматизированных систем **Уметь:** диагностировать системы защиты автоматизированных систем **Владеть:** навыками диагностирования системы защиты

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		автоматизированных систем
ПК*-2 Способен администрировать системы защиты автоматизированных систем	ПК*-2-В-1 Решает задачи администрирования автоматизированных систем	**Знать:** теоретические основы и методы администрирования системы защиты автоматизированных систем **Уметь:** администрировать системы защиты автоматизированных систем **Владеть:** навыками администрирования системы защиты автоматизированных систем
ПК*-8 Способен проводить анализ уязвимостей внедряемой системы защиты информации	ПК*-8-В-1 Составляет отчеты по аудиту уязвимостей внедряемой системы защиты информации	**Знать:** теоретические основы и методы анализа уязвимостей внедряемой системы защиты информации **Уметь:** проводить анализ уязвимостей внедряемой системы защиты информации **Владеть:** навыками анализа уязвимостей внедряемой системы защиты информации

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
Лабораторные работы (ЛР)	6	6

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Практические занятия (ПЗ)	18	18
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- подготовка к практическим занятиям;* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным 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 и сертификация средств защиты в компьютерных сетях	5	1			6
2	Концепция информационной безопасности	7	1			6
3	Направления обеспечения информационной безопасности	8	2			6
4	Основные понятия и положения защиты информации в компьютерных сетях и телекоммуникациях	8	2			6
5	Обнаружение компьютерных атак	8	2			6
6	Методы защиты от несанкционированного изменения структур КС	10	2		2	6
7	Защита информации в КС от несанкционированного доступа	12	2		4	6
8	Защита информации в распределенных КС	16	2	2	4	8
9	Технология межсетевого экранирования	16	2	2	4	8
10	Организация защиты виртуальных частных сетей	16	2	2	4	8
	Итого:	108	18	6	18	66
	Всего:	108	18	6	18	66

4.2 Содержание разделов дисциплины

Раздел 1 Правовые основы информационной безопасности и сертификация средств защиты в компьютерных сетях

1. Политика информационной безопасности.
2. Органы обеспечения информационной безопасности.
3. Лицензирование деятельности в области информационной безопасности компьютерных сетей.
4. Сертификация средств защиты информации компьютерных сетей.

Раздел 2 Концепция информационной безопасности

1. Положения системы защиты информации.
2. Модель информационной безопасности.
3. Источники утечки информации.

4. Классификация каналов утечки акустической информации.

Раздел 3 Направления обеспечения информационной безопасности

1. Организация защиты.
2. Классификация аппаратно-технических средств защиты.
3. Аппаратные средства защиты.
4. Криптографические средства защиты.

Раздел 4 Основные понятия и положения защиты информации в компьютерных сетях и телекоммуникациях

1. Случайные угрозы.
2. Дублирование информации.
3. Повышение надежности КС.
4. Блокировка ошибочных операций.
5. Преднамеренные угрозы.

Раздел 5 Обнаружение компьютерных атак

1. Классификация атак на компьютерные сети.
2. Основные типы сетевых атак.
3. Атаки на сетевые службы.
4. Атаки с использованием промежуточных узлов и территорий.
5. Прямые и косвенные признаки атак.
6. Методы обнаружения атак.
7. Классификация систем обнаружения атак (СОА).
8. Сетевые и узловые СОА.

Раздел 6 Методы защиты от несанкционированного изменения структур КС

1. Требования к защищенности КС от несанкционированного изменения структур.
2. Защита от внедрения аппаратных средств на этапе разработки.
3. Защита от внедрения аппаратных средств на этапе производства.
4. Защита от несанкционированного изменения структур КС в процессе эксплуатации.

Раздел 7 Защита информации в КС от несанкционированного доступа

1. Разграничения доступа к информации в КС.
2. Система защиты программных средств от копирования и исследования.
3. Управление доступом.
4. Проверка полномочий субъектов на доступ к ресурсам.
5. Реагирование на несанкционированные действия.

Раздел 8 Защита информации в распределенных КС

1. Архитектура распределенных КС.
2. Особенности защиты информации в РКС.
3. Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных КС.
4. Защита информации в каналах связи.
5. Анализ возможностей маршрутизации.
6. Типы межсетевых экранов.

Раздел 9 Технология межсетевого экранирования

1. Средства межсетевого экранирования.
2. Типы межсетевых экранов.
3. Схемы межсетевого экранирования.
4. Фильтрация пакетов.
5. Шлюзы прикладного уровня.

Раздел 10 Организация защиты виртуальных частных сетей

1. Уровни защищенных каналов.
2. Защита данных на канальном уровне.
3. Защита данных на сетевом уровне.
4. Протокол SKIP.
5. Настройка политики межсетевого экранирования с использо-ванием протокола IPSec.

Защита на транспортном уровне.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	6	Настройка базовых параметров безопасности маршрутизатора	2
2	7	Настройка стандартных списков контроля доступа	4
3	8	Настройка стандартных именованных списков контроля доступа	4
4	9	Настройка расширенных списков контроля доступа №1	4
5	10	Настройка расширенных именованных списков контроля доступа	2
6	10	Настройка расширенных списков контроля доступа №2	2
		Итого:	18

4.4 Практические занятия

№ ПЗ	№ раздела	Наименование лабораторных работ	Кол-во часов
1	8	Анализ стандартных именованных списков контроля доступа	2
2	9	Анализ расширенных списков контроля доступа №1	2
3	10	Анализ расширенных именованных списков контроля доступа	2
		Итого:	6

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. **Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства** [Текст] : учеб. пособие / В. Ф. Шаньгин . - М. : ДМК Пресс, 2008. - 544 с. : ил. - Библиогр.: с. 524-542. - ISBN 5-94074-383-8.

2. **Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей** [Текст] : учебное пособие для вузов / В. В. Платонов . - М. : Академия, 2006. - 240 с. - (Высшее профессиональное образование). - Библиогр.:с. 235-236. - ISBN 5-7695-2706-4.

5.2 Дополнительная литература

1. **Черняков, М. В. Основы информационных технологий** [Текст] : учебник / М. В. Черняков, А. С. Петрушин . - Москва : Академкнига, 2007. - 406 с. : ил.. - Библиогр.: с. 406-407. - ISBN 978-5-94628-273-4.

2. **Домарев, В. В. Безопасность информационных технологий. Методология создания систем защиты** [Текст] / В. В. Домарев . - М. : DiaSoft, 2002. - 688 с - ISBN 966-7992-02-0.

3. **Соколов, А. В. Методы информационной защиты объектов и компьютерных сетей** [Текст] / А. В. Соколов, О. М. Степанюк . - М. : АСТ ; СПб. : Полигон, 2000. - 272 с. : ил.. - (Шпионские штучки ; Вып. 5). - Библиогр.: с. 267-269. - ISBN 5-89173-079-0.

4. **Джонс, К. Дж. Анти-хакер. Средства защиты компьютерных сетей** [Текст] : [справ. профессионала]: [пер. с англ.] / Кейт Дж. Джонс, Майк Шема, Бредли С. Джонсон. - М. : СП ЭКОМ, 2003. - 688 с. : ил + 1 электрон. опт. диск (CD-ROM) - ISBN 5-9570-0014-0.

5. **Данжани, Н. Средства сетевой безопасности** = Network Security Tools [Текст] : пер. с англ. / Н. Данжани, Д. Кларк. - М. : Кудиц-Пресс, 2007. - 368 с. - Парал. тит. л. на англ. яз - ISBN 978-5-91136-022-1.

5.3 Периодические издания

Открытые системы. СУБД : журнал. - М. : Агентство "Роспечать", 2016.

Программные продукты и системы : журнал. - М. : Агентство "Роспечать", 2017.

Информационные технологии в проектировании и производстве : журнал. - Москва: Агентство "Роспечать", 2019, № 1-4;

Информационные технологии в проектировании и производстве : журнал. - Москва: Агентство "Роспечать", 2020, № 1;

Вестник компьютерных и информационных технологий : журнал. - Москва: Агентство "Роспечать", 2019, № 1-12;

Вестник компьютерных и информационных технологий : журнал. - Москва: Агентство "Роспечать", 2020, № 1.

5.4 Интернет-ресурсы

1. Единое окно доступа к образовательным ресурсам: информационная система. – Электрон. дан. – ФГУ ГНИИ ИТТ «Информика», 2005 – 2011; Министерство образования и науки РФ, 2005 – 2016. – Режим доступа: http://window.edu.ru/ . – Загл. с экрана.

2. Национальный Открытый Университет «ИНТУИТ». – Электрон. дан. - НОУ «ИНТУИТ», ИДО «ИНТУИТ», ООО «ИНТУИТ», 2003-2016. – Режим доступа: www.intuit.ru. – Загл. с экрана.

3. https://openedu.ru/course/ - «Открытое образование», Каталог курсов, МООК: «Базы данных»;

4. Сайт компании «ИНФОРМЗАЩИТА» – Электрон. дан. Компания «Информзащита» 1995-2016. – Режим доступа: http://www.infosec.ru/ . – Загл. с экрана

5. Сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/

6. Система управления данными Линтер https://linter.ru/ru/

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система Microsoft Windows.
2. Пакет настольных приложений Microsoft Office (Word, Excel, PowerPoint, Access).
3. Microsoft SQL Server.
4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2016]. – Режим доступа в сети ОГУ для установки системы: \\fileserver1\GarantClient\garant.exe.
5. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2016]. – 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-

08MP; 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.