ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САХАЛИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Аннотация рабочей программы дисциплины
Б1.В.ДВ.1.1 «Сетевая безопасность»

Направление подготовки
01.03.02 Прикладная математика и информатика

Профиль подготовки
Системное программирование и компьютерные технологии

1. Цели освоения дисциплины

Целью изучения дисциплины является предоставление обучаемым знаний об основных типах и способах защиты информации в компьютерных сетях, а также навыков по проектированию системы защиты информации и анализу защищенности вычислительных сетей. Данная дисциплина предназначена для подготовки к работе на должностях: инженера по телекоммуникациям или системного администратора.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Сетевая безопасность» относится к разделу дисциплин по выбору (Б1.В.ДВ.1.1). Для освоения данной дисциплины студент должен владеть основными понятиями дисциплины «Компьютерные сети и телекоммуникации». В тоже время освоение данной дисциплины должно подготовить студентов к дальнейшему образованию в области вычислительной техники и систем обработки информации, в частности к прохождению производственной практики.

3. Требования к результатам освоения содержания дисциплины

Дисциплина нацелена на формирование общепрофессиональных компетенций ОПК-2, ОПК-4 и профессиональных компетенций ПК-4, ПК-5 выпускника.

общепрофессиональные компетенции (ОПК):

(ОПК-2)	– способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии;
(ОПК-4)	– способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

профессиональные компетенции (ПК):

(ПК-4)	способностью работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности;
(ПК-5)	способностью осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет") и в других источниках.

В результате освоения дисциплины студент должен:

Знать:

- перспективные направления развития технологий обеспечения безопасности в сетях;
- методологические и технические основы обеспечения информационной безопасности сетевых автоматизированных систем;
- типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем;
- условия осуществимости атак, возможные последствия и способы их предотвращения.

Уметь:

- проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности;
- разрабатывать модели и политику сетевой безопасности, использую известные подходы, методы и средства;
- применять защищенные протоколы и межсетевые экраны, необходимые для реализации системы защиты информации в сетях;
- реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения.

Владеть:

- комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей;
- построения и эксплуатации вычислительных сетей;
- проектирования защищенных сетей;
- комплексного анализа и оценки сетевой безопасности.

4. Структура и содержание дисциплины Сетевая безопасность

Для очной формы обучения общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов, в том числе лекции – 38 часов, лабораторные занятия – 54 часа, самостоятельная работа студента – 88 часов. Вид промежуточной аттестации – зачет.

№ п/п	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
		всего	лк	лб	срс	зет	
1	7	108	14	30	64	3	Зачет
2	8	72	24	24	24	2	Зачет
итого		**180**	**38**	**54**	**88**	**2**	

№ п/п	Раздел Дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*	
			всего	лк	лб	срс	зач	по неделям семестра	по семестрам
1.	Виды атак. Модель сетевой безопасности.	7	8	2	2	4		Лабораторная работа	Зачет
2.	Криптография и системы шифрования.		34	4	10	20		Лабораторная работа	
3.	Механизмы обеспечения безопасности коммутируемых локальных сетей.		32	4	8	20		Лабораторная работа	
4.	Механизмы обеспечения безопасности беспроводных локальных сетей.		34	4	10	20		Лабораторная работа	
Итого за 7 семестр			**108**	**14**	**30**	**64**			
5.	Механизмы межсетевой безопасности.	8	30	10	10	10		Лабораторная работа	
6.	Системы тунелирования.		24	8	8	8		Лабораторная работа	
7.	Безопасность удаленного управления.		18	6	6	6		Лабораторная работа	
Итого за 8 семестр			**72**	**24**	**24**	**24**			
Итого			**180**	**38**	**54**	**88**			

Содержание разделов дисциплины

Раздел 1. Виды атак. Модель сетевой безопасности.
Обобщенный сценарий атаки. Пассивная разведка. Активная разведка. Взлом целевой системы. Сокрытие следов взлома. Классификация атак. Модель сетевой безопасности.

Раздел 2. Криптография и системы шифрования.
Криптография. Структура шифрования Фейстеля. Алгоритмы стандартного шифрования. Режимы работы блочных шифровальщиков. Расположение устройств шифрования. Распределение ключей. Криптография и аутентификация сообщений на основе общего ключа.

Раздел 3. Механизмы обеспечения безопасности коммутируемых локальных сетей.
Ограничение количества управляющих компьютеров. Настройка безопасности индивидуального порта. Фильтрация MAC-адресов. Технология фильтрации IP-MAC Binding. Списки контроля доступа. Сегментация трафика. Протокол IEEE 802.1x. Виртуальные сети. Аудит безопасности протокола связующего дерева STP.

Раздел 4. Механизмы обеспечения безопасности беспроводных локальных сетей.
Классификация механизмов безопасности в сетях Wi-Fi. Механизмы шифрования. Принцип аутентификации абонента. Открытая аутентификация. Аутентификация с общим ключом. Аутентификация по MAC-адресу. Дополнительные механизмы защиты.

Раздел 5. Механизмы межсетевой безопасности.
Межсетевые экраны. Фильтры пакетов. Фильтры инспекции состояний. Транслятор адресов. Транспортные шлюзы. Шлюзы приложений. Системы обнаружения атак и вторжений.

Раздел 6. Системы тунелирования.
Протокол PPPoE. Виртуальные частные сети. Протокол IPSEC. Протокол SSL/TLS.

Раздел 7. Безопасность удаленного управления.
Аудит безопасности протокола SNMP. Версии протокола SNMP. Протокол SNMPv3. Протокол SSH. Рекомендации по безопасности использования протокола SSH.