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

Аннотация рабочей программы дисциплины
Б1.В.ДВ.9.2 «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.9.2). 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 2 зачетные единицы, 72 часа, в том числе лекции – 24 часа, лабораторные занятия – 24 часа, самостоятельная работа студента – 24 часа. 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	8	72	24	24	24	2	Зачет
итого		**72**	**24**	**24**	**24**	**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	экз	по неделям семестра	по семестрам
1.	Виды атак. Модель сетевой безопасности.	8	6	2	2	2		Лабораторная работа	Зачет
2.	Криптография и системы шифрования.		10	4	2	4		Лабораторная работа	
3.	Механизмы обеспечения безопасности коммутируемых локальных сетей.		12	4	6	2		Лабораторная работа	
4.	Механизмы обеспечения безопасности беспроводных локальных сетей.		14	4	6	4		Лабораторная работа	
5.	Механизмы межсетевой безопасности.		12	4	4	4		Лабораторная работа	
6.	Системы тунелирования.		10	4	2	4		Лабораторная работа	
7.	Безопасность удаленного управления.		8	2	2	4		Лабораторная работа	
	Итого		**72**	**24**	**24**	**24**			

Для заочной формы обучения общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа, в том числе лекции – 6 часов, лабораторные занятия – 10 часов, самостоятельная работа студента – 52 часа. 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**	**контроль**	**зет**	
1	10	72	6	10	52	4	2	Зачет
итого		**72**	**6**	**10**	**52**	**4**	**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.	8	7		1	6	4	Лабораторная работа	Зачет
2.	Криптография и системы шифрования.		8	1	1	6		Лабораторная работа	

3.	Механизмы обеспечения безопасности коммутируемых локальных сетей.		10	1	1	8		Лабораторная работа	
4.	Механизмы обеспечения безопасности беспроводных локальных сетей.		10	1	1	8		Лабораторная работа	
5.	Механизмы межсетевой безопасности.		11	1	2	8		Лабораторная работа	
6.	Системы тунелирования.		11	1	2	8		Лабораторная работа	
7.	Безопасность удаленного управления.		11	1	2	8		Лабораторная работа	
	Итого		**72**	**6**	**10**	**52**	**4**		

5. Учебно-методическое и информационное обеспечение дисциплины

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

а) основная литература

1. Гребенюк Е.И. Технические средства информатизации: учеб. для студентов сред. профес. образования /Е.И. Гребенюк, Н.А. Гребенюк. - 5-е изд., стер. - М.: Академия, 2009. - 267 с. - (Среднее профессиональное образование).
2. Куприянов А.И. Основы защиты информации: учебное пособие для студентов вузов /А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. - 2-е изд., стереотип. - М.: Академия, 2007. – 254 с. - (Высшее профессиональное образование).
3. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для студентов вузов /П.Б. Хорев. - 3-е изд., стереотип. - М.: Академия, 2007. – 255 с. - (Высшее профессиональное образование).

б) дополнительная литература

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2012. — 311 c. — 978-5-374-00301-7. — Режим доступа: http://www.iprbookshop.ru/10677.html
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 c. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/63800.html
3. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. — Электрон. текстовые данные. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 c. — 978-5-9585-0603-3. — Режим доступа: http://www.iprbookshop.ru/43183.html
4. Семенов Ю.А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс] / Ю.А. Семенов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 581 c. — 978-5-94774-708-9. — Режим доступа: http://www.iprbookshop.ru/62827.html
5. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В.Г. Спицын. — Электрон. текстовые данные. — Томск:

Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 148 с. — 978-5-4332-0020-3. — Режим доступа: http://www.iprbookshop.ru/13936.html

в) Программное обеспечение и Интернет-ресурсы

1. Windows 10 Pro
2. Microsoft Office Professional Plus 2013
3. Microsoft Office Professional Plus 2016
4. https://www.securitylab.ru/
5. https://xakep.ru/
6. https://securelist.ru/

Автор:	старший преподаватель		Е.Н. Козлов
Рецензент:	зав. кафедрой информатики, д.т.н., профессор		Г.С. Осипов

Рассмотрена на заседании кафедры 19 сентября 2017 г., протокол № 1.

Утверждена на совете института 10 октября 2017 года, протокол № 1.