Аннотация рабочей программы дисциплины

«Сетевая безопасность»

Направление подготовки

02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) образовательной программы

Сетевые технологии

Цели и задачи освоения дисциплины

Цель изучения дисциплины «Сетевая безопасность» соотносятся с общими целями образовательной программы (далее – ОПОП ВО) по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии. Дисциплина «Сетевая безопасность» направлена на обеспечение теоретической и практической подготовки студентов в области современных методов, технологий защиты информации в процессе её получения, хранения, обработки и передачи по линиям связи. Дисциплина «Сетевая безопасность» рассматривает вопросы, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, работы без отказов, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Основные задачи изучения дисциплины заключаются в приобретении знаний, умений и владений, благодаря которым студенты, используя современные программные продукты, методы и технологии защиты информации, смогут осуществлять безопасный сбор, хранение и переработку информации, планировать организовывать и проводить научные исследования и эксперименты в области создания новых методов идентификации, аутентификации, авторизации пользователей и оборудования, методов шифрования информационных сообщений, защиты данных от сетевых атак и вирусов, разработки защищенных корпоративных сетей, аппаратного и программного обеспечения оконечного оборудования и оборудования передачи данных.

Рассматриваются физические и логические информационные ресурсы. К физическим ресурсам относятся как отдельные устройства целиком (процессор, внешние устройства, маршрутизаторы, коммутаторы, физические каналы связи и др.), так и физические разделяемые ресурсы устройств (разделы и секторы диска, процессорное время, физические соединения канала связи). Логическими ресурсами являются файлы, вычислительные процессы, сетевые сервисы, приложения, пропускная способность каналов связи и т.д.

Место дисциплины в структуре ОПОП ВО

Дисциплина «Сетевая безопасность» относится к обязательным дисциплинам вариативной части учебного плана по направлению 02.03.02

Фундаментальная информатика и информационные технологии, изучается в 7 семестре (4 курс), форма промежуточной аттестации – зачет с оценкой.

Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

После изучения данной дисциплины студенты приобретают знания, умения и владения (навыки), соответствующие результатам основной профессиональной образовательной программы.

Формируемые компетенции	**Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций**
ОПК-3. Способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию	З4 (ОПК-3) Знать основные принципы организации и функционирования современных локальных и территориальных компьютерных сетей*) З5 (ОПК-3) Знать принципы построения математических моделей для анализа показателей функционирования компьютерных сетей
ОПК-4. Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З5 (ОПК-4) Знать основы методологии защиты информации в информационных системах З7 (ОПК-4) Знать средства и методы хранения и передачи аутентификационной информации; основные протоколы идентификации и аутентификации абонентов сети З8 (ОПК-4) Знать механизмы реализации атак в сетях TCP/IP; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений У5 (ОПК-4) Уметь проводить анализ угроз информационной безопасности информационной системы (ИС) У6 (ОПК-4) Уметь проводить анализ состояния защищенности информационной системы (ИС) В1 (ОПК-4) Владеть программно-информационными средствами для решения практических задач в области профессиональной деятельности *)
ПК-4. Способность решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива	У6 (ПК-4) Уметь применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Объем дисциплины составляет 4 зачетных единицы, всего 144 часа, из которых:

- **68 часов составляет контактная работа обучающегося с преподавателем:**
  - 34 часов – лекционные занятия;
  - 34 часа – практические занятия;
- **мероприятия промежуточной аттестации (зачет с оценкой в 7 семестре);**
- **76 часов составляет самостоятельная работа обучающегося.**

Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и виды учебных занятий

Наименование и краткое содержание разделов и тем дисциплины (модуля) Форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	Контактная работа (работа во взаимодействии						Самостоятельная работа обучающегося,		
		Лекционные	Семинарские	Практические	Лабораторные	Учебные занятия, направленные на проведение текущего контроля	Всего	Выполнение	Подготовка	Всего
7 семестр										
Основные понятия, концепции и принципы информационной безопасности, идентификация, аутентификация и авторизация, модели информационной безопасности, триада «конфиденциальность, доступность, целостность», гексада Паркера и модель STRIDE, уязвимость, угроза, атака, ущерб и риск, управление рисками.	11	2		3		ПР-1	5	6		6
Типы и примеры атак, пассивные и активные атаки, отказ в обслуживании, внедрение вредоносных программ, кража личности, фишинг, иерархия средств защиты от информационных угроз, средства безопасности законодательного уровня, административный уровень, политика безопасности, средства безопасности процедурного уровня, средства безопасности технического уровня, принципы защиты информационной системы, подход сверху вниз, защита как процесс, эшелонированная защита, сбалансированная защита, компромиссы системы безопасности	11	2		2		ПР-2	4	7		7
Шифрование — базовая технология безопасности, основные понятия и определения, симметричное шифрование, проблема распределения ключей, метод	14	3		4		ПР-3, ПР-4	7	7		7

1 Перечень видов учебных занятий уточняется в соответствии с учебным планом.

Наименование и краткое содержание разделов и тем дисциплины (модуля) Форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	Контактная работа (работа во взаимодействии						Самостоятельная работа обучающегося,		
		иЛекционные	иСеминарские	иПрактические	Лабораторные	Учебные занятия, направленные на проведение текущего контроля	Всего	Выполнение	Подготовка	Всего
7 семестр										
Диффи—Хелмана передачи секретного ключа по незащищенному каналу, концепция асимметричного шифрования, алгоритм асимметричного шифрования RSA, хеш-функции, односторонние функции шифрования, проверка целостности.										
Технологии аутентификации, факторы аутентификации человека, аутентификация на основе паролей, аутентификация на основе аппаратных аутентификаторов, аутентификация информации. Электронная подпись, аутентификация на основе цифровых сертификатов, аутентификация программных кодов, технологии управления доступом и авторизации, формы представления ограничений доступа, дискреционный метод управления доступом, мандатный метод управления доступом, ролевое управление доступом.	12	2		3		ПР-5	5	7		7
Фильтрация, виды фильтрации, стандартные и дополнительные правила фильтрации маршрутизаторов Cisco, файерволы, функциональное назначение файервола, типы файерволов	14	3		4		ПР-6, ПР-7	7	7		7
Прокси-серверы, функции прокси-сервера, «Проксификация» приложений, файерволы с функцией NAT, традиционная технология NAT, базовая трансляция сетевых адресов, трансляция сетевых адресов и портов, программные файерволы хоста, типовые архитектуры сетей, защищаемых	14	4		3		ПР-8	7	7		7

Наименование и краткое содержание разделов и тем дисциплины (модуля) Форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	Контактная работа (работа во взаимодействии						Самостоятельная работа обучающегося,		
		иЛекционные	иСеминарские	иПрактические	Лабораторные	Учебные занятия, направленные на проведение текущего контроля	Всего	иВыполнение	Подготовка	Всего
7 семестр										
файерволами.										
Мониторинг трафика. Анализаторы протоколов, анализаторы протоколов, система мониторинга NetFlow, системы обнаружения вторжений, архитектура сети с защитой периметра и разделением внутренних зон, аудит событий безопасности.	12	3		2		ПР-9	5	7		7
TCP-атаки, затопление SYN-пакетами, подделка TCP-сегмента, сброс TCP-соединения, ICMP-атаки, перенаправление трафика, ICMP-атака Smurf, пинг смерти и ping-затопление, UDP-атаки, UDP-затопление, ICMP/UDP-затопление, UDP/echo/chargen-затопление, IP-атаки, атака на IP-опции, IP-атака на фрагментацию.	14	4		3		ПР-10, ПР-11	7	7		7
Сетевая разведка, задачи и разновидности сетевой разведки, сканирование сети, сканирование портов, атаки на DNS, DNS-спуффинг, отравление кэша DNS, атаки на корневые DNS-серверы, DDoS-атаки отражением от DNS-серверов, методы защиты службы DNS.	13	3		3		ПР-12	6	7		7
Иерархия технологий защищенного канала, распределение функций между протоколами IPSec, безопасная ассоциация, транспортный и туннельный режимы, протокол AH, протокол ESP, базы данных SAD И SPD, VPN на основе шифрования.	15	4		4		ПР-13, ПР-14	8	7		7
Безопасность программного кода и сетевых служб,	14	4		3		ПР-15,ПР-16	7	7		7

Наименование и краткое содержание разделов и тем дисциплины (модуля) Форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	Контактная работа (работа во взаимодействии						Самостоятельная работа обучающегося,		
		иЛекционные	иСеминарские	иПрактические	Лабораторные	Учебные занятия, направленные на проведение текущего контроля	Всего	иВыполнение	Подготовка	Всего
7 семестр										
уязвимости программного кода и вредоносные программы, уязвимости, связанные с нарушением защиты оперативной памяти, уязвимости контроля вводимых данных, внедрение в компьютеры вредоносных программ, троянские программы, сетевые черви, вирусы, программные закладки , антивирусные программы, ботнет..										
Мероприятия промежуточной аттестации (зачет с оценкой в 7 семестре)										
Итого	144	34		34			68	76		76

*Опрос (ПР-1), Практические работы (ПР-2), Реферат (ПР-3), *Экзамен (УО-4). Текущий контроль проводится за счет времени, отведенного на аудиторные занятия