Федеральное агентство
морского и речного транспорта
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Государственный университет морского и речного флота
имени адмирала С.О. Макарова»
Воронежский филиал ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»

Кафедра математики, информационных систем и технологий

АННОТАЦИЯ

дисциплины «*Основы информационной безопасности*»

Направление подготовки 09.03.02 Информационные системы и технологи

Направленность (профиль) Информационные системы на транспорте

Уровень высшего образования бакалавриат

Форма обучения очная, заочная

Промежуточная аттестация зачет

1. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к обязательной части Блока 1 учебного плана по направлению подготовки 09.03.02 «Информационные системы и технологии» (профиль «Информационные системы на транспорте») и изучается на 4 курсе в VIII семестре по очной форме обучения и на 5 курсе по заочной форме обучения.

Изучение дисциплины базируется на знаниях, полученных обучающимися при освоении курсов: «Экономическое обоснование проектов», «Технологии программирования», «Информационно-коммуникационные системы и сети», «Методы и средства проектирования информационных систем и технологий», «Администрирование информационных систем», «Анализ больших данных».

Для изучения дисциплины студент должен владеть методами работы пользователя на персональном компьютере, знать основные парадигмы языков программирования.

Дисциплина «Основы информационной безопасности» необходима в качестве предшествующей для дисциплин подготовки и защиты ВКР.

2. Планируемые результаты обучения по дисциплине

Код и наименование компетенции	Код индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИД-1ОПК-3	**Знать:** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности."
	ИД-2ОПК-3	**Уметь:** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ИД-3ОПК-3	**Иметь навыки:** подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

3. Объем дисциплины по видам учебных занятий

Объем дисциплины составляет 2 зачетных единиц, всего 72 часа, из которых по очной форме 36 часов составляет контактная работа обучающегося с преподавателем (18 час. – занятия лекционного типа, 18 час. – лабораторные работы), по заочной форме 12 часов составляет контактная работа обучающегося с преподавателем (6 час. – занятия лекционного типа, 6 час. – лабораторные работы).

4. Основное содержание дисциплины

Понятие "информационная безопасность". Проблема информационной безопасности общества. Определение понятия "информационная безопасность". Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации. Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных

актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности. Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Механизмы безопасности. Администрирование средств безопасности. Стандарты информационной безопасности в РФ. Административный уровень обеспечения информационной безопасности. Разработка политики информационной безопасности. Классификация угроз "информационной безопасности". Классы угроз информационной безопасности.

Вирусы как угроза информационной безопасности. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивные возможностям. Характеристика "вирусоподобных" программ. Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов. Обнаружение неизвестного вируса. Обнаружение загрузочного вируса. Обнаружение резидентного вируса. Обнаружение макровируса. Общий алгоритм обнаружения вируса. Ссылки на дополнительные материалы (печатные и электронные ресурсы).

Особенности обеспечения информационной безопасности в компьютерных сетях. Особенности информационной безопасности в компьютерных сетях. Специфика средств защиты в компьютерных сетях. Сетевые модели передачи данных. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Транспортный протокол TCP и модель TCP/IP. Модель взаимодействия открытых систем OSI/ISO. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Характеристика уровней модели OSI/ISO. Адресация в глобальных сетях. Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен. Классификация удаленных угроз в вычислительных сетях. Классы удаленных угроз и их характеристика. Типовые удаленные атаки и их характеристика. Удаленная атака "анализ сетевого трафика". Удаленная атака "подмена доверенного объекта". Удаленная атака "ложный объект". Удаленная атака "отказ в обслуживании". Причины успешной реализации удаленных угроз в вычислительных сетях. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей. Принципы построения защищенных вычислительных сетей.

Информационная безопасность при использовании Internet. Идентификация и аутентификация. Определение понятий "идентификация" и "аутентификация". Механизм идентификация и аутентификация пользователей. Криптография и шифрование. Структура криптосистемы.

Классификация систем шифрования данных. Симметричные и асимметричные методы шифрования. Механизм электронной цифровой подписи. Методы разграничение доступа. Методы разграничения доступа. Мандатное и дискретное управление доступом. Регистрация и аудит. Определение и содержание регистрации и аудита информационных систем. Этапы регистрации и методы аудита событий информационной системы. Межсетевое экранирование. Классификация межсетевых экранов. Характеристика межсетевых экранов. Технология виртуальных частных сетей (VPN). Сущность и содержание технологии виртуальных частных сетей. Понятие "туннеля" при передаче данных в сетях.

Безопасность операционных систем. Безопасность ОС Windows 10.

Составитель: д.ф.-м.н., профессор Кузьменко Р.В.

Зав. кафедрой: д.т.н., профессор Лапшина М. Л.