



АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Технология программной защиты в интернете»

по направлению/специальности 09.03.02 Информационные системы и технологии

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

изучение теоретических основ программной защиты в интернет

Задачи освоения дисциплины:

Знать:

-место и роль информационной безопасности в системе национальной безопасности РФ, общие характеристики процессов сбора, передачи, обработки, накопления и хранения информации; основные принципы передачи и обработки информации в инфокоммуникационных системах; основы защиты информации и сведений, составляющих государственную тайну; методы защиты информации;

-принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

-операционные системы ПЭВМ, системы управления базами данных, принципы построения информационных систем, структуру систем документационного обеспечения, перечень и характеристики угроз информационным ресурсам;

-эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы, сигналы электросвязи, принципы построения систем и средств связи, методы анализа электрических цепей, базовые принципы контроля, диагностики, технического обслуживания и ремонта средств связи;

-принципы организации и проектирования сложных информационных систем в соответствии с требованиями по защите информации, основы технико-экономического обоснования проектов;

-современные средства разработки и анализа программного обеспечения на языках высокого уровня, методы программирования и разработки эффективных алгоритмов решения прикладных задач;

-перечень, назначение, принципы работы инструментальных средств и систем программирования;

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

- типовые задачи обеспечения информационной безопасности;

Уметь:

- применять достижения информатики и вычислительной техники, перерабатывать большие объёмы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

- организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

- анализировать и оценивать угрозы информационной безопасности объекта;

- устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации, осуществлять контроль технического состояния, диагностику неисправностей и ремонт базовых стандартных блоков средств и систем связи;

- проектировать средства и сети связи с учётом требований по защите информации на базе серийно выпускаемых узлов и блоков, а также синтезировать нестандартные решения и проекты невысокой сложности; проводить технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности;

- составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;

- выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;

- разрабатывать алгоритмы решения типовых задач;

Владеть:

-- навыками переработки больших объёмов информации, целенаправленного поиска информации в различных источниках по профилю деятельности, в том числе в глобальных компьютерных системах, анализа инфокоммуникационных сетей и систем, их информационной безопасности и разработки мероприятий по её обеспечению;

-- навыками выполнения комплекса мер по информационной безопасности, управления процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

-- методами и средствами выявления угроз безопасности автоматизированным системам;

-- профессиональной терминологией, навыками чтения электронных схем, безопасного

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

использования технических средств в профессиональной деятельности, базовыми практическими навыками тестирования, поиска неисправностей, технического обслуживания и ремонта средств и систем связи, в том числе сетевого оборудования;

-методами анализа и формализации информационных процессов объекта и связей между ними, базовыми навыками проектирования средств и сетей связи; использования стандартных и разработки нестандартных программных средств автоматизации проектирования; технико-экономического анализа и обоснования проектов;

-навыками работы с программным обеспечением, использования программ;

-методами расчёта и инструментального контроля показателей технической защиты информации;

-- навыками и методиками разработки алгоритмов для решения задач информационной безопасности

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Технология программной защиты в интернете» относится к числу дисциплин блока Б1.В.1.ДВ.12, предназначенного для студентов, обучающихся по направлению: 09.03.02 Информационные системы и технологии.

Для успешного изучения дисциплины необходимы знания и умения, приобретённые в результате освоения курсов и полностью или частично сформированные компетенции ПК-9, ПК-11, ПК-13.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Операционные системы, Преддипломная практика, Надежность информационных систем, Научно-исследовательская работа, Выполнение и защита выпускной квалификационной работы.


3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- Способен поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества (ПК-9)
- Способен проводить расчет экономической эффективности информационных систем и технологий (ПК-13)
- Способен оценивать надежность и качество функционирования информационных систем и технологий (ПК-11)

В результате изучения дисциплины студент должен:

знать:

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

место и роль информационной безопасности в системе национальной безопасности РФ, общие характеристики процессов сбора, передачи, обработки, накопления и хранения информации; основные принципы передачи и обработки информации в инфокоммуникационных системах; основы защиты информации и сведений, составляющих государственную тайну; методы защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации

принципы организации и проектирования сложных информационных систем в соответствии с требованиями по защите информации, основы технико-экономического обоснования проектов; современные средства разработки и анализа программного обеспечения на языках высокого уровня, методы программирования и разработки эффективных алгоритмов решения прикладных задач

операционные системы ПЭВМ, системы управления базами данных, принципы построения информационных систем, структуру систем документационного обеспечения, перечень и характеристики угроз информационным ресурсам; эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы, сигналы электросвязи, принципы построения систем и средств связи, методы анализа электрических цепей, базовые принципы контроля, диагностики, технического обслуживания и ремонта средств связи

уметь:


применять достижения информатики и вычислительной техники, перерабатывать большие объёмы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах; организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации

проектировать средства и сети связи с учётом требований по защите информации на базе серийно выпускаемых узлов и блоков, а также синтезировать нестандартные решения и проекты невысокой сложности; проводить технико-экономический анализ и обоснование проектных решений по обеспечению информационной безопасности; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;

анализировать и оценивать угрозы информационной безопасности объекта; устанавливать, настраивать и обслуживать технические и программно-аппаратные средства защиты информации, осуществлять контроль технического состояния, диагностику неисправностей и ремонт базовых стандартных блоков средств и систем связи

владеть:

- навыками переработки больших объёмов информации, целенаправленного поиска информации в различных источниках по профилю деятельности, в том числе в глобальных

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

компьютерных системах, анализа инфокоммуникационных сетей и систем, их информационной безопасности и разработки мероприятий по её обеспечению; - навыками выполнения комплекса мер по информационной безопасности, управления процессом их реализации с учётом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации методами анализа и формализации информационных процессов объекта и связей между ними, базовыми навыками проектирования средств и сетей связи; использования стандартных и разработки нестандартных программных средств автоматизации проектирования; технико- экономического анализа и обоснования проектов; навыками работы с программным обеспечением, использования программ;

- методами и средствами выявления угроз безопасности автоматизированным системам; - профессиональной терминологией, навыками чтения электронных схем, безопасного использования технических средств в профессиональной деятельности, базовыми практическими навыками тестирования, поиска неисправностей, технического обслуживания и ремонта средств и систем связи, в том числе сетевого оборудования

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 5 ЗЕТ зачетных единиц (180 часов).

5. Образовательные технологии

При реализации учебного процесса по курсу применяются классические и современные образовательные технологии: лекции для изложения теоретического материала и практические лабораторные занятия для изучения методов разработки, тестирования и оценивания программного обеспечения.

Самостоятельная работа студентов осуществляется в виде изучения теоретического материала, основной и дополнительной литературы, рекомендованной по дисциплине, выполнения лабораторных работ по практической части дисциплины.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: Тесты . Промежуточная аттестация проводится в форме: Экзамен, Защита курсовой работы (проекта).