АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Основной целью освоения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» является формирование у студентов знаний о спектре программно-аппаратных средств обеспечения информационной безопасности, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач по настройке, выбору и эксплуатации программно-аппаратных средств защиты информации.

Задачи освоения дисциплины:

Основные задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных системах;
- о защитных механизмах, реализованных в средствах защиты информационных систем;
- о современных программно-аппаратных средствах защиты информации;
- о применении средств криптографической защиты информации и средств защиты информации от НСД для решения задач обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» изучается в 8 семестре и относится к базовой части дисциплин блока Б1.Б специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно увязан с другими учебными дисциплинами, в первую очередь с курсами «Физика», «Электроника и схемотехника», «Безопасность операционных систем», «Основы информационной безопасности», «Техническая защита информации», «Системы и сети передачи информации», позволяющими понять физическую сущность возникновения технических каналов утечки информации, возможности современных средств технической разведки, методы и способы защиты от утечки по техническим каналам.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области физики, вычислительной техники, электроники и схемотехники;

способность использовать нормативные правовые документы;

способность анализировать проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Безопасность сетей ЭВМ»; «Разработка и эксплуатация защищённых автоматизированных систем»; «Безопасность открытых информационных систем»;

«Инструментальные средства контроля защищенности информации»; «Сертификация средств защиты информации».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Способность корректно применять при решении профессиональных задач соответствующий математический аппарат, в том числе с использованием вычислительной техники (ОПК-2);

Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

Способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-5);

Способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

Способность применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций (ОПК-7);

Способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);

Способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

Способность создавать и исследовать модели автоматизированных систем (ПК-2);

Способность проводить анализ защищенности автоматизированных систем (ПК-3);

Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

Способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

Способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

Способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-26).

В результате изучения дисциплины студент должен:

знать:

математический аппарат, используемый для при решения профессиональных задач в том числе с использованием вычислительной техники;

основные языки, системы и инструментальные средства программирования, используемые в профессиональной деятельности;

основные методы научных исследований, используемых в профессиональной деятельности;

основные нормативные правовые акты в профессиональной деятельности;

основные приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций;

основные характеристики новых образцов технических средств и информационных

технологий;

основные методы поиска, изучения, обобщения и систематизации научно-технической информации;

методы создания и исследования моделей автоматизированных систем;

основы анализа защищенности автоматизированных систем;

сущность модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

основные процессы и процедуры совершенствования системы управления информационной безопасностью автоматизированной системы**;**

основные требования к информационной безопасности автоматизированных систем;

основы эффективного применения средств защиты ин-формационно-технологических ресурсов автоматизированной системы и восстановления их работоспособности при возникновении нештатных ситуаций;

основы инструментального мониторинга защищенности информации в автоматизированной системе;

типовые каналы утечки информации в автоматизированной системе;

уметь:

анализировать явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач;

применять языки, системы и инструментальные средства программирования в профессиональной деятельности;

применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

применять нормативные правовые акты в профессиональной деятельности;

применять приемы оказания первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций;

осваивать новые образцы технических средств и информационных технологий;

осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;

создавать и исследовать модели автоматизированных систем;

проводить анализ защищенности автоматизированных систем;

разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;

обеспечивать эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;

проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;

владеть:

соответствующим математическим аппаратом для решения профессиональных задач;

навыками применения языков, систем и инструментальных средств программирования для решения профессиональных задач;

навыками применения методов научных исследований в профессиональной деятельности;

навыками применения нормативных и правовых актов;

навыками применения приемов оказания первой помощи, методов защиты производственного персонала и населения в условиях чрезвычайных ситуаций;

навыками освоения новых образцов технических средств и информационных технологий;

навыками поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;

навыками создания и исследования моделей автоматизированных систем;

навыками проведения анализа защищенности автоматизированных систем;

навыками разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

навыками разработки предложений по совершенствованию системы управления информационной безопасностью автоматизированных систем;

навыками организации, разработки, внедрения, эксплуатации и сопровождения автоматизированной системы с учетом требований информационной безопасности;

навыками обеспечения эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы и восстановления их работоспособности при возникновении нештатных ситуаций;

навыками проведения инструментального мониторинга за-щищенности информации в автоматизированной системе; навыками выявления каналов утечки информации в автоматизированной системе.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зачетных единицы (180 часов).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: лекционные занятия, интерактивный опрос в ходе лекций, эвристическая беседа, диалог, ознакомительные беседы с представителями потенциальных работодателей.

При организации самостоятельной работы занятий используются образовательные технологии развивающего, проблемного и проектного обучения.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

Программой дисциплины предусмотрены следующие виды текущего контроля: письменные и устные опросы на лекциях, семинарах, лабораторных работах, в ходе написания рефератов.

Промежуточная аттестация проводится в форме экзамена.