АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«Безопасность открытых информационных систем»
по направлению 10.05.03 «Информационная безопасность автоматизированных систем»
(специалитет)
специализация *«*Безопасность открытых информационных систем*»*

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- изучение основных уязвимостей открытых информационных систем;
- освоение методов и средств защиты ОИС;

Задачи освоения дисциплины:

- формирование у студентов навыков экспертизы качества и надёжности реализации открытых информационных систем;
- знакомство студентов с программно-аппаратными средствами обеспечения безопасности открытых информационных систем;
- развитие навыков обеспечения высокой степени защиты открытых информационных систем.

2. Место дисциплины в структуре ОПОП

Дисциплина относится к вариативной части дисциплин в рамках профессионального цикла Б1 образовательной программы и читается в 9-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения.

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов Профессиональная этика, Модели безопасности компьютерных систем, Безопасность операционных систем, Безопасность сетей ЭВМ, Безопасность систем баз данных, Управление информационной безопасностью, Программно-аппаратные средства обеспечения информационной безопасности, Виртуальные частные сети.

Основные положения дисциплины используются при изучении дисциплин: Защита программ и данных, Разработка и эксплуатация защищённых автоматизированных систем, Дополнительные главы криптографии», а также для прохождения практик и государственной итоговой аттестации.

3. Перечень планируемых результатов освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Знать: основные требования к профессии Уметь: адекватно оценивать собственные возможности и находит способы их качественного совершенствования Владеть: основными понятиями информационной безопасности, различными техниками этичного пентеста
ОПК-8 - способностью к освоению новых	Знать: современные программные продукты

образцов программных, технических средств и информационных технологий	Уметь: устанавливать, настраивать и актуализировать ПО Владеть: навыками мониторинга актуальности современного ПО
ПК-1 - способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	Знать: источники релятивной научно-технической информации Уметь: обрабатывать и анализировать научно-техническую информация Владеть: навыками работы с иностранными источниками, их адаптацией и актуализацией
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Знать: основные методы анализа защищенности ОИС Уметь: настраивать и устанавливать ПО, необходимое для защиты ОИС Владеть: навыками анализа текущего состояния ИС
ПК-4 - способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать: понятия модели угроз и модели нарушителя Уметь: строить модель актуальных угроз на основе имеющихся данных ФСТЭК Владеть: навыками разработки технической документации
ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать: перечень рисков ОИС и их источники Уметь: анализировать и систематизировать информацию по текущему состоянию ОИС Владеть: умением снижения и устранения рисков в реализации ОИС
ПК-8 - способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Знать: этапы разработки проектных решений по обеспечению ИБ Уметь: проводить анализ и проетирование сложных систем ИБ Владеть: нормативно-правовой базой в области ИБ
ПК-11 - способностью разрабатывать политику информационной безопасности автоматизированной системы	Знать: основные типы политик ИБ Уметь: разрабатывать ПБ согласно заданной модели Владеть: навыками обеспечения ИБ в рамках заданной ПБ
ПК-19 - способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Знать: актуальные вектора атак Уметь: проводить тестирование на проникновение Владеть: навыками составления отчетов о проделанной работе по вскрытию и реализации уязвимостей
ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Знать: основы построения защищенных ОИС Уметь: строить архитектурно-грамотные решения по реализации требований ИБ Владеть: знаниями по ИБ
ПК-27 - способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Знать: инструменты по мониторингу функционирования подопечной ИС Уметь: настраивать, актуализировать и совершенствовать инструменты обеспечения программной безопасности Владеть: навыками работы с ОИС, анализа её защищенности
ПК-28 - способностью управлять информационной безопасностью автоматизированной системы	Знать: что такое безопасность ОИС, из чего она складывается, как реализовать наиболее защищенную ОИС Уметь: защитить АС от внешнего и внутреннего нарушителя Владеть: приемами обеспечения безопасности ОИС
ПСК-4.1 - способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем	Знать: нормо-правовые аспекты ИБ Уметь: применять законодательную базу по ИБ на практике Владеть: перечнем нормативно-правовых документов в области защиты информации
ПСК-4.2 - способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	Знать: основные типы политик ИБ ОИС Уметь: разрабатывать ПБ согласно заданной модели ОИС Владеть: навыками обеспечения ИБ в рамках заданной ПБ ОИС

ПСК-4.3 - способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы	Знать: этапы проектирования системы управления ИБ Уметь: эксплуатировать и совершенствовать современные системы управления ИБ Владеть: приемами обеспечения безопасности ОИС
ПСК-4.4 - способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы	Знать: инструментарий для проведения тестирования на проникновение Уметь: применять современные программные средства для пентеста Владеть: языками программирования и навыками работы с программными средствами
ПСК-4.5 - способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем	Знать: совокупность мер по обеспечению информационной безопасности Уметь: эффективно использовать на практике принципы, методы и средства для обеспечения ИБ Владеть: навыками взаимодействия с современными сканерами безопасности

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы (**108** часов).

5. Образовательные технологии

В ходе изучения дисциплины используются традиционные методы и формы обучения, а также технологии дистанционного обучения в ЭИОС.

При организации самостоятельной работы используются следующие образовательные технологии: самостоятельная работа, сопряженная с основными аудиторными занятиями (проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины); подготовка к тестированию; самостоятельная работа под контролем преподавателя в форме плановых консультаций, при подготовке к сдаче зачета; внеаудиторная самостоятельная работа при выполнении студентом лабораторных работ.

6. Контроль успеваемости

Программой дисциплины предусмотрены виды текущего контроля: лабораторные работы, проверка тестовых заданий.

Промежуточная аттестация проводится в форме: зачет.