АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

(название дисциплины)

10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

2,3

(семестр)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- «Защищенные информационные системы» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность». Целью освоения дисциплины является ознакомление магистров с современным теоретическим аппаратом информационной безопасности, представление сведений о базовых моделях и алгоритмах, используемых в управлении информационной безопасностью в информационных системах, а также о процессе теоретико-методологического анализа различных механизмов и сервисов защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

- Данная дисциплина относится к базовой части блока Б1 (код Б1.Б.1). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.
- Дисциплина изучается на 2 курсе, в 3 семестре требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.04.01 «Информационная безопасность» по курсам «Анализ и моделирование информационно-телекоммуникационных сетей», «Методы и средства защиты объектов информатизации», «Методология информационной безопасности». Кроме того, требования к «входным» знаниям, умениям и готовностям обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Защита информации в корпоративных информационных системах» или аналогичных, в соответствии с программой подготовки бакалавров в следующих или смежных областях знаний: -информационная безопасность; -энергетика, энергетическое машиностроение и электротехника; -авиационная и ракетно-космическая техника; -фотоника, приборостроение, -оптические и биотехнические системы и технологии; -электронная техника, радиотехника и связь; -автоматика и управление; -информатика и вычислительная техника; -физико-технические науки и технологии; -управление в технических системах.
- Курс тесно взаимосвязан с другими дисциплинами. Он может быть полезен для изучения таких дисциплин как «Управление информационной безопасностью», «Информационно-аналитические системы безопасности» и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими общекультурными и профессиональными компетенциями:

- ПК-2 – способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;
- ПК-7 – способностью проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;
- ПК-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

- Информационные технологии и информационные системы. Примеры информационных технологий и информационных систем
- Проектирование и разработка защищенных информационных технологий
- Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
- Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC.
- Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.

- Классы в системе общих критериев. Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.
- Гарантии безопасности компьютерных систем в системе общих критериев. Понятие гарантии безопасности. Уровни гарантий.
- Каналы утечки и их анализ в системе общих критериев. Виды каналов утечки информации.
- Безопасное функционирование в системе общих критериев. Управление конфигурацией.
- Основные угрозы безопасности информации в компьютерных системах.
- Модель угроз. Анализ критичных технологий. Требования, предъявляемые к разработке модели угроз.
- Государственная политика в области безопасности компьютерных систем. Система лицензирования и сертификации средств защиты.
- Разработка политик безопасности для защищенных компьютерных систем. Требования, предъявляемые к разработке политик безопасности. Дискреционная и многоуровневая политика безопасности.
- Порядок аттестации защищенных компьютерных систем. Понятие аттестации защищенных компьютерных систем.
- Концепция управления ИТ-подразделением (IT Service Management. ITIL) — основа концепции управления ИТ-службами.
- Порядок внедрения SLM-системы. Service Desk — цели, возможности, реализации. Microsoft Operations Framework (MOF).
- Стадии создания ЗИС: формирование требований к ЗИС, разработка концепции ЗИС, техническое задание, эскизный проект, технический проект, рабочая документация
- Методы и методики оценки качества ЗИС. Требования к эксплуатационной документации ЗИС. Порядок приемки защищенных ЗИС

Составитель: зав. кафедрой ИЗИ д.т.н., Монахов М.Ю.

должность, ФИО, подпись

Заведующий кафедрой ИЗИ М.Ю. Монахов

ФИО, подпись

Директор института ИТР А.А. Галкин

ФИО, подпись

Дата, Печать института (факультета)