АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Методы и системы защиты информации, информационная безопасность»

по основной профессиональной образовательной программе по направлению подготовки 2.3.6. «Методы и системы защиты информации, информационная безопасность» (научная специальность)

Направленность (профиль):
Общий объем дисциплины – 4 з.е. (144 часа)
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
Содержание дисциплины:
Дисциплина «Методы и системы защиты информации, информационная безопасность» включает в себя следующие разделы:
Форма обучения очная. Семестр 4.
Объем дисциплины в семестре – 2 з.е. (72 часов)
Форма промежуточной аттестации – Зачет
1. Тема 1: Теория и методология обеспечения информационной безопасности и защиты информации. -Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.
-Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида
-Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.
-Модели и методы оценки защищенности информации и информационной безопасности объекта.
-Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.
-Методы и модели выявления и противодействия распространению ложной и вредоносной информации..
2. Тема 2: Организационно-правовые аспекты обеспечения информационной безопасности и защиты информации. -Методы и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
-Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации
-Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования
-Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
-Модели, методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.
-Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих организационных методов защиты информации и обеспечения информационной безопасности.
-Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем..
3. Тема 3: Обеспечение безопасности в компьютерных сетях. -Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным

атакам в компьютерных сетях.

-Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях.

-Методы, модели и средства, а также комплексы средств противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет

-Модели, методы и средства противодействия отказам в обслуживании и другим видам компьютерных атак

-Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа..

Форма обучения очная. Семестр 5.

Объем дисциплины в семестре – 2 з.е. (72 часов)

Форма промежуточной аттестации – Экзамен

1. Тема 4: Программно-аппаратные средства обеспечения информационной безопасности и защиты информации. -Методы и аппаратно-программные средства для защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.

-Принципы и решения по созданию новых и совершенствованию существующих программно-аппаратных средств защиты информации и обеспечения информационной безопасности.

-Современные тенденции развития программно-аппаратных средств защиты информации и обеспечения информационной безопасности

-Тема: Инженерно-технические средства обеспечения информационной безопасности и защиты информации – 6 ч

-Новые подходы и методы, используемые при создании извещателей пожарно-охранной сигнализации

-Общие принципы построения и тенденции развития современных средств контроля и управления доступом.

2. Инженерно-технические средства обеспечения информационной безопасности и защиты информации. -Новые подходы и методы, используемые при создании извещателей пожарно-охранной сигнализации

-Общие принципы построения и тенденции развития современных средств контроля и управления доступом.

3. Информационная безопасность объектов критической информационной инфраструктуры (КИИ). -Объекты и субъекты КИИ и их категорирование

-Особенности обеспечения информационной безопасности объектов КИИ

-Общие принципы построения системы обеспечения информационной безопасности КИИ

-Правовое регулирование в области обеспечения безопасности значимых объектов КИИ.

4. Особенности обеспечения информационной безопасности киберфизических систем. - Методы выявления и прогнозирования появления нештатных ситуаций в киберфизических истемах

-Управление информационной безопасностью и управление рисками в киберфизической системе

-Особенности обеспечения информационной безопасности беспроводного сетевого взаимодействия самоорганизующихся киберфизических систем и компонентов IoT

-Принципы, решения (технические, математические, организационные и др.) и тенденции развития методов защиты информации и обеспечения информационной безопасности киберфизических систем..

Разработал:
заведующий кафедрой
кафедры ИВТиИБ А.Г. Якунин
Проверил:

Декан ФИТ А.С. Авдеев