Аннотация рабочей программы дисциплины

«Основы построения защищенных инфокоммуникационных систем»

Направление подготовки: 11.03.02 – «Инфокоммуникационные технологии и системы связи»

Профиль подготовки: «Инфокоммуникационные технологии в сервисах и услугах связи»

Квалификация (степень) выпускника: Бакалавр

Форма обучения: Очная

Общая трудоемкость дисциплины, изучаемой в 8 семестре составляет 4 зачетных единицы. По дисциплине предусмотрен экзамен.

Цели и задачи освоения дисциплины

Целями преподавания дисциплины «Основы построения защищенных инфокоммуникационных систем» является подготовка бакалавров, готовых к самостоятельной работе в области защиты информации в инфокоммуникационных сетях и системах.

Задачи освоения дисциплины:

4. Изучение нормативно-правовых актов в области информационной безопасности и защиты информации;
5. Изучение особенностей построения и эксплуатации информационно-коммуникационных систем;
6. Изучение основ защиты информации в технологических и бизнес-процессах современных информационно-коммуникационных (инфокоммуникационных) систем.

Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

а) общекультурных (ОК):

- Способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);
- Способность к самоорганизации и самообразованию (ОК-7);

б) общепрофессиональных (ОПК):

- Способностью владеть основными методами, способами и средствами получения, хранения, переработки информации (ОПК-3);
- Способностью использовать нормативную и правовую документацию, характерную для области инфокоммуникационных технологий и систем связи (нормативные правовые акты Российской Федерации, технические регламенты, международные и национальные стандарты, рекомендации Международного союза электросвязи) (ОПК-5);

в) профессиональных (ПК):

- Готовность содействовать внедрению перспективных технологий и стандартов (ПК-1);
- Умение собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов (ПК-8).

В результате освоения дисциплины обучающийся должен:

Знать:

- основные принципы построения и архитектура современных информационно-коммуникационных систем и сетей;

- действующие нормативно-правовые акты в части информационной безопасности;
- основные принципы построения защищенных инфокоммуникационных систем;
- модели безопасности инфокоммуникационных систем;
- методы и методики оценки безопасности инфокоммуникационных систем.

Уметь:

- составлять политики безопасности инфокоммуникационных систем;
- анализировать инфокоммуникационную систему с целью определения необходимого уровня защищенности и доверия;
- оформлять проектно-сметную документацию и готовить бизнес-план по развитию инфокоммуникационных систем;
- разрабатывать профили защиты и формулировать задания по безопасности, формировать политики безопасности инфокоммуникационных систем;
- изучать научно-техническую информацию, отечественный и зарубежный опыт в области информационной безопасности и защиты информации в сетях электросвязи.

Владеть:

- способами защиты информации в информационно-коммуникационных системах, сетевыми технологиями, принципами работы протоколов маршрутизации и управления, способностью использовать нормативную и правовую документацию, стандарты связи, терминологию, документацию по защите сетевой инфраструктуры;
- основами применения современных теоретических и экспериментальных методов исследования с целью создания новых перспективных средств защиты информации и информатики, готовностью к организации работ по практическому использованию и внедрению результатов исследований;
- способностью понимать особенности современных методов и способов защиты информации;
- готовностью к обеспечению эффективной и добросовестной конкуренции на рынке средств защиты информации.

Основные разделы дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела

1.	Введение. Базовые принципы информационной безопасности.	Структура мировой системы телекоммуникаций и единой сети электросвязи Российской Федерации. Концепция информационной безопасности.
2.	Роль и место информации и информационных технологий в современной жизни.	Основные формы проявления информации и их свойства. Информационная безопасность и ее обеспечение.
3.	Анализ угроз объекту информационной безопасности.	Понятие угрозы и ее основные свойства. Классификация угроз. Ущерб информационной безопасности предприятия.
4.	Каналы утечки информации.	Основы теории информации. Коммуникационный процесс. Источники конфиденциальной информации и каналы ее утечки.
5.	Организационные основы защиты информации на предприятии.	Основные направления, принципы и условия организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Основные методы, силы и средства, используемые для организации защиты информации.
6.	Инвентаризация информационных систем.	Инвентаризация информационных систем. Классификация информационных систем. Роли и ответственность субъектов. Принципы распределения прав и ответственности. Модель информационных потоков.
7.	Классификация информационных систем.	Терминология и постановка задачи. Основные регламенты классификации. Классификация информационных объектов. Классификация средств обработки информации: стандарт CCITSE. Контроль классификации.
8.	Роли и ответственность субъектов.	Субъекты информационного пространства. Принципы распределения прав и ответственности. Упрощенная модель классификации субъектов. Полная модель классификации субъектов. Сопоставление ролей классам обрабатываемой информации. Результаты классификации информационных систем.
9.	Модель информационных потоков.	Направления защиты процессов обмена информацией. Защита сетевых процессов обмена данными. Защита экспорта файлов. Вопросы построения полной и

		функциональной схемы информационных потоков. Средства создания схем информационных потоков. Контроль построения модели информационных потоков.
10.	Защита информации в компьютерных сетях.	Сети ЭВМ — построение и использование. Топология сетей. Цели, функции и задачи защиты информации в сетях ЭВМ. Понятие сервисов безопасности. Международные стандарты X. 800 и X. 509. Архитектура механизмов защиты информации в сетях ЭВМ. Прокси (Proxy) серверы.
11.	Защита информации в персональных компьютерах.	Особенности защиты информации в персональных ЭВМ. Угрозы информации в персональных ЭВМ. Обеспечение целостности информации в ПК. Защита ПК от несанкционированного доступа. Защита информации от копирования. Защита от несанкционированного доступа к компьютеру без завершения сеанса работы. Защита ПК от вредоносных закладок. Защита от несанкционированного доступа к компьютеру.

Разработчики программы:
д.т.н., профессор В.А. Докучаев

Заведующий кафедрой МСиУС,
д.т.н., профессор В.А. Докучаев

М.П.

Центр документационного обеспечения