Б1.В.ДВ.3.2 «Электронная цифровая подпись»

Цели дисциплины:

1. получение студентами знаний по использованию различных средств автоматизации, в том числе и инструментария Интернет, для проведения расчетов в процессе ведения коммерческой деятельности;
2. формирование знаний и умений, которые образуют теоретический и практический фундамент, необходимый для построения и анализа безопасных информационных систем и технологий.

Задачи дисциплины:

1. приобретение студентами теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;
2. обучение проблемам защиты информации, стоящих перед современной вычислительной техникой;
3. обучение использованию полученных знания для правильного выбора решений при разработке криптографических средств защиты информации.

Место дисциплины в структуре ОПОП:

Дисциплина «Электронная цифровая подпись» вариативной части дисциплин по выбору учебного плана.

Дисциплина основывается на знании дисциплины: «Экономическая информатика».

Для успешного освоения дисциплины «Электронная цифровая подпись», студент должен:

Знать:

- системы счисления, используемые в вычислительной технике (ОПК-2);
- принцип взаимодействия частей компьютера (ОПК-2);
- назначение операционной системы (ОПК-2);
- понятие компилятора (ОПК-2);
- логическую схему ЭВМ (ПК-8).

Уметь:

- создавать файлы, папки (ПК-8);
- проверять файлы на вирусы (ПК-8);
- работать MS OFFICE (ОПК-2);
- запустить компьютер с диска (ПК-8).

Владеть:

- навыками программирования (ПК-8);
- подключением дополнительных устройств к компьютеру (ОПК-2);
- установкой операционной системы с диска (ОПК-2);
- техникой быстрой работы на клавиатуре (ОПК-2).

Требования к результатам освоения дисциплины:

В результате освоения дисциплины должны быть сформированы следующие компетенции:

ОПК-2 способность осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач

В результате освоения компетенции **ОПК -2** студент должен:

1. Знать:

- технологию сбора и обработки информации и эффективности использования этих знаний.

2. Уметь:

- осуществлять поиск и сбор информации с помощью программных средств;
- анализировать информацию и данные, необходимые для решения задач.

3. Владеть:
- современными техническими средствами обработки данных;
- современными программными средствами решения задач.

ПК-6 способность анализировать и интерпретировать данные отечественной и зарубежной статистики о социально-экономических процессах и явлениях, выявлять тенденции изменения социально-экономических показателей

1. Знать:
- структуру социально-экономических явлений и процессов.;
- основные понятия информационной безопасности.

2. Уметь:
- использовать нормативные правовые документы в своей деятельности;
- анализировать безопасность многопользовательских систем

3. Владеть:
- навыками выявлять тенденции изменения социально-экономических показателей.

Содержание дисциплины:

№ п/п	Наименование раздела дисциплины (темы)
1	**Основные понятия и классификация средств криптографической защиты информации. Аппаратно-программные средства защиты информации**
2	**Средства обеспечения конфиденциальности данных; средства идентификации и аутентификации пользователей**
3	***Электронно-цифровая подпись.*** **Основные понятия и свойства.**
4	**Основные свойства симметричных криптосистем. Классическая сеть Фейстеля. Блочные алгоритмы шифрования данных**
5	**Алгоритмы цифровой подписи RSA , Эль Гамаля. DSA**

Форма контроля - зачет