Доброго антивирусного здоровья!

Тема лекции на 15.05: **Электронная цифровая подпись**

Изучить вопросы:

• назначение, типы и функционал электронной цифровой подписи:

* схожесть и отличия между собственноручной и цифровой подписями,
* ЭЦП на основе симметричной криптографии (обычное шифрование/расшифрование сообщения на основе общего ключа, который должен гарантировать целостность документа и подлинность, т.е. авторство подписи),
* ЭЦП на основе асимметричной криптографии (обычное шифрование/расшифрование сообщения на основе тайного ключа отправителя, который (ключ) должен гарантировать целостность документа и подлинность, т.е. авторство подписи),
* ЭЦП на основе симметричной криптографии и ПОСРЕДНИКА, в качестве которого в реальной жизни выступают УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ), похожая технология реализована в протоколе Kerberos,

• математические основы технологий ЭЦП на основе асимметричной криптографии и хеширования подписываемых сообщений – классическая технология ЭЦП;

• ЭЦП на основе RSA,

• ЭЦП DSA,

• ЭЦП на основе алгоритма Эль-Гамаля,

• ЭЦП на основе алгоритма Шнорра – является основой государственного стандарта ЭЦП в нашей стране;

• криптостойкость алгоритмов на основе асимметричной криптографии и хеширования подписываемых сообщений.

Методические материалы:

- Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие для студ. спец. 1-98 01 03 «Программное обеспечение информационной безопасности мобильных систем», направления спец. 1-40 05 01-03 «Информационные системы и технологии (издательско-полиграфический комплекс)», спец. 1-40 01 01 «Программное обеспечение информационных технологий» спец. 1-40 01 01 10 «Программмирование Интернет-приложений». - Минск : БГТУ, 2016. - 220 с. – главы 9-11. (файл книга криптография .pdf в папке ЗИНИС на diskstation),

- Теоретическая часть к Лабораторной работе 10 (одноименный .pdf-файл в папке ЗИНИС на diskstation),

- Книга Б. Шнайера. Прикладная криптография. (файл SHnaier\_Brus\_Prikladnaya\_kriptografiya.\_Protokoly\_algoritmy\_i\_ishodnye\_teksty\_na\_yazyke\_S\_Litmir.net\_266719\_original\_ad9f9 в папке ЗИНИС на diskstation) – глава 20.

Завтра жду посланий от старост.

С наилучшими пожеланиями,

П. Урбанович

БЕРЕГИТЕ СЕБЯ!