Лабораторная работа по дисциплине «Методы и средства защиты компьютерной информации»

Тема: «Изучение технологии асимметричного шифрования информации и применения электронно-цифровой подписи» • <u>Шифр</u> - это совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования



<u>PGP (Pretty Good Privacy)</u> – это программа, предназначенная для шифрования конфиденциальной информации и применения электронно-цифровой подписи

🚨 PGP Desktop - All Keys						
File Edit View Tools Keys Help						
PGP Keys	All Keys		R			
PIV PIVALE NEVS	vampolsm ∃ yampolsm ∡ yampolsm <1@1.ru>	Verified O O	d			
🐕 Email this Key		PGP Options				×
PGP Messaging		General Keys	Master Keys Messaging	NetShare Disk	Notifier	Advanced
		822	Master Keys are keys that create a disk, or share files any Additional Decryption H	s. You may want to	e each time y list your ow	you encrypt, In private key and
			yampolsm <1@1.r	ru>		0
<u>Главный ключ пр</u>	<u>ограммы</u>					

Add....

Remove

File	Edit	View	Tools	Keys	Help
New PGP Key			Ctrl+N		
Ne	w				
Open			Ctrl+O		
Im	port				
Im	port Pe	rsonal C	ertificate	(s)	
Ex	port				

• Создание пары сеансовых ключей для организации сеанса связи



• Экспорт и импорт открытых ключей



• Подпись открытых ключей



PGP Desktop - All Keys

File	Edit	View	Tools	Keys	Help		
Ne	ew PGP I	Ctrl+N					
Ne	ew				•		
O	pen			Ctrl+O			
In	nport						
Im	nport Pe	rsonal C	ertificate	(s)			
E>	ort			ALCONTRACT.	E.		
E>	dit						

• Выбор файла (папки) для шифрования информации



• Выполнение шифрования информации и электронно-цифровой подписи



Выбор ключа для шифрования информации







Выбор ключа для электронно-цифровой подписи информации



• Результат шифрования информации и электронно-цифровой подписи



PGP Zip Assistant

Автоматизированное планирование.docx PGP Zip

• Результат шифрования информации парольной фразой и электронно-цифровой подписи



• Результат создания архива информации



PGP Zip Assistant

• Результат электронно-цифровой подписи



• Дешифрирование информации



• Проверка электронно-цифровой подписи







- 1. Создать главный ключ программы
- 2. Создать пару сеансовых ключей для организации сеанса связи
- 3. Экспортировать открытую часть сеансового ключа
- 4. Импортировать открытую часть сеансового ключа преподавателя
- 5. Зашифровать и подписать любой текстовый файл
- 6. Передать преподавателю зашифрованный файл и открытую часть своего сеансового ключа. Проверить с преподавателем правильность использования ключей.
- 7. Проверить целостность подписи преподавателя.
- 8. Внести изменения в файл преподавателя и убедится в нарушении целостности подписи

Спасибо за внимание !