Список заданий для контрольной работы

I. Реферативная часть задания, объем не более 15 страниц.

1. Системы управления доступом в Интернет и контроля корпоративной электронной почты
2. Утечки информации: источники, правовые и технологические аспекты
3. Утилизация данных: проблемы повторного использования.
4. Методы защиты от нелегального использования ПО (и др. IT-ресурсов).
5. Аспекты защиты информации в системах автоматизированного управления технологическими процессами.
6. Понятие политики безопасности
7. Эволюция вредоносного ПО (malware) и средств борьбы с ним.
8. Проблемы противодействия фишингу и фармингу.
9. P2P-приложения: тенденции развития и аспекты безопасности.
10. Безопасность Web-браузеров.
11. Безопасность беспроводных технологий.
12. Виртуальные частные сети (VPN) – технологии и средства организации.
13. СПАМ: способы распространения, принципы и средства противодействия
14. Защита персональных данных, типовые решения.
15. Биометрические системы аутентификации: принципы, технологии и перспективы.
16. Средства взлома парольных систем и противодействие им.

II. Практическая часть задания.

При разработке приложения выделить 3 основных модуля – генерация ключей/сертификата, шифрование сообщения, расшифровка сообщения. Использовать любой язык программирования, математический пакет или табличный процессор.

1. Реализация программы шифрования/дешифрования методом RSA.

2. Реализация программы шифрования/дешифрования методом Эль Гамаля.

3. Реализация программы шифрования/дешифрования методом упаковки рюкзака.

4. Реализация программы генерации и использования ЭЦП методом RSA.

5. Реализация программы генерации и использования ЭЦП методом Эль Гамаля.

6. Реализация программы распространения секрета Деффи-Хелмана.

7. Реализация программы распределения секрета между участниками с помощью Китайской теоремы об остатках.

8. Реализация программы распределения секрета между участниками с помощью интерполяционного полинома Лагранжа.