**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Гжельский государственный университет»** (ГГУ)

Колледж ГГУ

Специальность 09.02.07. Информационные системы и программирование.

**Лабораторная работа №1**

**по предмету «Стандартизация, сертификация и техническая документация»**

**«Нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности».**

ВЫПОЛНИЛА:

Студентка группы ИСП-О-17

Пигарева Е. А.

ПРОВЕРИЛА:

Пркуронова А. Ю.

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

п. Электроизолятор

2019 г.

#### Законодательный уровень информационной безопасности.

**Цель работы:**

Изучить законодательный уровень информационной безопасности.

**Практическое задание:**

1. **Уголовный кодекс РФ не предусматривает наказания за:**

* неправомерный доступ к компьютерной информации
* создание, использование и распространение вредоносных программ
* ***массовую рассылку незапрошенной рекламной информации.***

**2. Согласно Закону "Об информации, информатизации и защите информации", персональные данные — это:**

* ***сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность***
* данные, хранящиеся в персональном компьютере
* данные, находящиеся в чьей-либо персональной собственности

**3. Согласно Закону "О лицензировании отдельных видов деятельности", лицензия — это:**

* ***специальное разрешение на осуществление конкретного вида деятельности***
* удостоверение, подтверждающее высокое качество изделия
* документ, гарантирующий безопасность программного продукта

**4. В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на:**

* системы электронной коммерции
* инфраструктуру для электронных цифровых подписей
* ***средства электронной аутентификации***

**5. Уголовный кодекс РФ не предусматривает наказания за:**

* ***увлечение компьютерными играми в рабочее время***
* неправомерный доступ к компьютерной информации
* нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

**6. Согласно Закону "Об информации, информатизации и  
защите информации", конфиденциальная информация —  
это:**

* информация с грифом "секретно"
* ***документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации***
* информация, доступ к которой ограничивается сертифицированными техническими средствами

**7. Действие Закона "О лицензировании отдельных видов  
деятельности" не распространяется на:**

* деятельность по технической защите конфиденциальной информации
* ***образовательную деятельность в области защиты информации***
* предоставление услуг в области шифрования информации

**8. В следующих странах сохранилось жесткое  
государственное регулирование разработки и  
распространения криптосредств на внутреннем рынке:**

* Китай
* ***Россия***
* Франция

**9. Уголовный кодекс РФ не предусматривает наказания за:**

* создание, использование и распространение вредоносных программ
* ***ведение личной корреспонденции на производственной технической базе***
* нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

**10. Согласно Закону "Об информации, информатизации и  
защите информации", риск, связанный с использованием  
информации, полученной из несертифицированной системы, лежит на:**

* + владельце этой системы
  + собственнике документов
  + ***потребителе информации***

**11. Действие Закона "О лицензировании отдельных видов  
деятельности" распространяется на:**

* деятельность по использованию шифровальных (криптографических) средств
* ***деятельность по рекламированию шифровальных (криптографических) средств***
* деятельность по распространению шифровальных (криптографических) средств

**12. В законопроекте "О совершенствовании информационной  
безопасности" (США, 2001 год) особое внимание  
обращено на:**

* + смягчение ограничений на экспорт криптосредств
  + ***разработку средств электронной аутентификации***
  + создание инфраструктуры с открытыми ключами

**Стандарты и спецификации в области информационной безопасности.**

**Цель:**

Изучить международные и национальные стандарты и специфи­кации в области ИБ — от "Оранжевой книги" до ISO 15408. Получить навыки определения сильных и слабых стороны этих документов.

**Практическое задание:**

**Уровень безопасности С, согласно "Оранжевой книге",  
характеризуется:**

* + ***произвольным управлением доступом***
  + принудительным управлением доступом
  + верифицируемой безопасностью

**2. Согласно рекомендациям Х.800, аутентификация может  
быть реализована на:**

* ***сетевом уровне***
* транспортном уровне
* прикладном уровне

**3. "Общие критерии" содержат следующие виды  
требований:**

* ***функциональные***
* ***доверия безопасности***
* экономической целесообразности

**4. Уровень безопасности В, согласно "Оранжевой книге",  
характеризуется:**

* произвольным управлением доступом
* ***принудительным управлением доступом***
* верифицируемой безопасностью

**5. Согласно рекомендациям Х.800, целостность с  
восстановлением может быть реализована на:**

* + сетевом уровне
  + транспортном уровне
  + ***прикладном уровне***

**6. В число классов функциональных требований "Общих  
критериев" входят:**

* + анонимность
  + ***приватность***
  + ***связь***

**7. Уровень безопасности А, согласно "Оранжевой книге",  
характеризуется:**

* + произвольным управлением доступом
  + принудительным управлением доступом
  + ***верифицируемой безопасностью***

**8. Согласно рекомендациям Х.800, неотказуемость может  
быть реализована на:**

* сетевом уровне
* ***транспортном уровне***
* прикладном уровне

**9. В число классов требований доверия безопасности  
"Общих критериев" входят:**

* ***разработка***
* ***оценка профиля защиты***
* сертификация

#### Процедурный уровень информационной безопасности.

# ***Цель:***

# Изучить основные классы мер процедурного уровня. Получить навыки использования принципов, позволяющих обеспечить надёжную защиту.

**Практические задания**

**1. В число классов мер процедурного уровня входят:**

* логическая защита
* ***физическая защита***
* ***планирование восстановительных работ***

**2. В число принципов управления персоналом входят:**

* "разделяй и властвуй"
* ***разделение обязанностей***
* инкапсуляция наследования

**3. В число этапов процесса планирования восстановительных работ входят:**

* ***выявление критически важных функций организации***
* ***определение перечня возможных аварий***
* проведение тестовых аварий

**4. В число классов мер процедурного уровня входят:**

* ***управление персоналом***
* управление персоналками
* ***реагирование на нарушения режима безопасности***

**5. В число принципов управления персоналом входят:**

* + ***минимизация привилегий***
  + минимизация зарплаты
  + максимизация зарплаты

**6. В число этапов процесса планирования восстановительных работ входят:**

* идентификация персонала
* проверка персонала
* ***идентификация ресурсов***

**7. число классов мер процедурного уровня входят:**

* + ***поддержание работоспособности***
  + поддержание физической формы
  + ***физическая защита***

**8. В число принципов физической защиты входят:**

* беспощадный отпор
* ***непрерывность защиты в пространстве и времени***
* минимизация защитных средств

**9. В число этапов процесса планирования восстановительных работ входят:**

* + ***разработка стратегии восстановительных работ***
  + сертификация стратегии
  + ***проверка стратегии***