|  |  |  |
| --- | --- | --- |
| **Основные принципы обеспечения ИБ** | **Основные документы в области обеспечения ИБ** | **Структура государственных органов обеспечения национальной ИБ** |
| **1. Законность:** Обеспечение ИБ осуществляется в соответствии с законодательством РБ. | 1. Закон Республики Беларусь "Об информации, информатизации и защите информации" | **1. Совет Безопасности Республики Беларусь** |
| **2. Защита информации:** Информация должна быть защищена от несанкционированного доступа, использования, изменения, уничтожения, распространения. | **2. Концепция информационной безопасности Республики Беларусь** | **2. Государственный секретариат Совета Безопасности Республики Беларусь** |
| **3. Превентивность:** Принимаются меры по предупреждению угроз ИБ. | **3. Стратегия развития информационного общества в Республике Беларусь на 2021-2025 годы** | **3. Оперативно-аналитический центр при Президенте Республики Беларусь** |
| **4. Соответствие:** Системы защиты информации должны соответствовать требованиям законодательства и нормативным правовым актам. | **4. Положение о системе защиты информации в Республике Беларусь** | **4. Комитет государственной безопасности Республики Беларусь** |

**Задание 2. Заполните таблицу.**

**Задание 3. Присвойте номер определениям в порядке приоритета.**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Уровень модели** |  | **Механизмы безопасности** |
| **1** | **Аутентификация** | **2** | **Шифрование** |
| **2** | **Управление доступом** | **5** | **Электронная (цифровая) подпись** |
| **3** | **Конфиденциальность соединения** | **3** | **Механизмы управления доступом** |
| **4** | **Конфиденциальность вне соединения** | **4** | **Механизмы контроля целостности данных** |
| **9** | **Выборочная конфиденциальность** | **1** | **Механизмы аутентификации** |
| **8** | **Конфиденциальность трафика** | **7** | **Механизмы дополнения трафика** |
| **6** | **Целостность с восстановлением** | **8** | **Механизмы управления маршрутизацией** |
| **7** | **Целостность без восстановления** | **6** | **Механизмы подтверждения подлинности** |
| **10** | **Избирательная целостность** |  |  |
| **11** | **Целостность вне соединения** |  |  |
| **5** | **Безотказность** |  |  |

**Задание 4. Заполните таблицу. Укажите 1) основные функции, 2) достоинства 3) недостатки**

|  |  |  |  |
| --- | --- | --- | --- |
| **Утилита** | **Основные функции** | **Достоинства** | **Недостатки** |
| Антивирус Касперского | Защита от вирусов, шифровальщиков, фишинга, спама. | Высокий уровень защиты, регулярные обновления, множество дополнительных функций. | Платная подписка, может влиять на производительность. |
| Антивирус Dr.Web для Windows | Защита от вирусов, троянов, руткитов, шпионов. | Эффективная защита, не влияет на производительность, есть бесплатная версия. | Платная версия дороже аналогов. |
| Panda Antivirus | Защита от вирусов, фишинга, онлайн-мошенничества. | Легкий и простой в использовании, есть бесплатная версия. | Не такой эффективный, как другие антивирусы. |
| ESET NOD32 Антивирус | Защита от вирусов, троянов, руткитов, фишинга. | Не влияет на производительность, есть бесплатная версия. | Платная версия дороже аналогов. |
| Avast! Free Antivirus | Защита от вирусов, фишинга, спама. | Бесплатная, эффективная защита. | Показывает рекламу, может влиять на производительность. |
| Avirs AntiVir Personal | Защита от вирусов, троянов, руткитов. | Бесплатная, простая в использовании. | Не такая эффективная, как другие антивирусы. |
| Norton AntiVirus | Защита от вирусов, фишинга, онлайн-мошенничества. | Высокий уровень защиты, множество дополнительных функций. | Платная подписка, может влиять на производительность. |
| Trend Micro Internet Security | Защита от вирусов, фишинга, спама, родительский контроль. | Высокий уровень защиты, множество дополнительных функций. | Платная подписка, может влиять на производительность. |
| Microsoft Security Essentials | Защита от вирусов, шпионских программ, других угроз. | Бесплатная, интегрирована с Windows. | Не такая эффективная, как другие антивирусы. |

**Задание 5. Приведите характеристику (особенности) в области внедрения и распространения вирусов.**

**Среда обитания вирусов:**

|  |  |
| --- | --- |
| **Тип** | **Особенности** |
| Сетевые | Распространяются по сети, заражая компьютеры, подключенные к ней. |
| Файловые | Заражают файлы, делая их непригодными для использования. |
| Загрузочные | Заражают загрузочный сектор диска, что приводит к заражению компьютера при загрузке. |

**Способы заражения:**

|  |  |
| --- | --- |
| **Тип** | **Особенности** |
| Резидентные | Постоянно находятся в памяти компьютера, что позволяет им заражать другие файлы. |
| Нерезидентные | Загружаются в память компьютера только при выполнении зараженного файла. |

**Другие особенности:**

|  |  |
| --- | --- |
| **Тип** | **Особенности** |
| Безвредные | Не причиняют вреда компьютеру. |
| Опасные | Могут привести к потере данных, краже информации, другим серьезным последствиям. |

**Вирусы-спутники** заражают другие файлы, но не могут самостоятельно размножаться.  
**Вирусы-невидимки** используют методы стелс-технологий, чтобы скрыться от антивирусных программ.  
**Макровирусы** заражают макросы в документах, например, в Microsoft Word.

**Задание 6. Присвойте номер признакам воздействия вирусов на компьютерную систему в порядке приоритета.**

|  |  |
| --- | --- |
| **Признак** |  |
| Самопроизвольная перезагрузка | **1** |
| «Зависание» компьютера | **2** |
| Появление неожиданных графических и звуковых эффектов | **3** |
| Замедление работы процессора | **4** |
| Слишком частые обращения к диску | **5** |
| Непонятные ошибки | **6** |
| Пропажа файла | **7** |
| Изменение даты создания и длины файла | **8** |
| Сообщения антивирусных программ | **9** |

**Задание 7**

**Аутентификация:** Доступ к системе возможен только после ввода логина и пароля.  
**Изоляция:** Система не имеет доступа к Интернету, что ограничивает возможность проникновения вредоносных программ через скачанные файлы.  
**Контроль доступа к Wi-Fi:** Ограничение круга пользователей, имеющих доступ к беспроводной сети.

**Однако, для комплексной защиты информационной безопасности в учебном заведении рекомендуется:**  
**1). Расширить меры защиты системы для учащихся:  
Установить антивирусное ПО:** Защита от вредоносных программ, которые могут попасть на компьютеры учащихся через другие носители (например, USB-накопители).  
**2). Усилить безопасность университетской сети Wi-Fi:  
Использовать шифрование данных:** Защитить передаваемые по Wi-Fi данные от перехвата и несанкционированного доступа.  
**Ограничить доступ к конфиденциальным ресурсам:** Запретить доступ к веб-сайтам и другим ресурсам, содержащим конфиденциальную информацию

**Задание 8:**

**1. Дайте определение понятию информационная безопасность.  
Информационная безопасность – это состояние защищенности информации от несанкционированного доступа, использования, раскрытия, изменения, уничтожения, а также от случайных или непреднамеренных действий, которые могут привести к ущербу.**

**2. Охарактеризуйте основные составляющие национальных интересов Беларуси в информационной сфере.  
Основные составляющие:  
Защита суверенитета и территориальной целостности Беларуси в информационной сфере.  
Обеспечение информационной безопасности государственных органов, организаций и граждан.  
Развитие информационного общества и обеспечение доступа к информации.  
Противодействие информационным угрозам.  
Сотрудничество с другими государствами в области информационной безопасности.**

**3. Охарактеризуйте угрозы информационной безопасности Беларуси.  
Основные угрозы:  
Кибератаки: хакерские атаки, DDoS-атаки, распространение вредоносных программ.  
Информационные войны: распространение дезинформации, пропаганды, фейковых новостей.  
Кибершпионаж: кража конфиденциальной информации.  
Киберпреступность: использование информационных технологий для совершения преступлений.  
Технические угрозы: сбои в работе информационных систем, стихийные бедствия.**

**4. Охарактеризуйте комплекс мер по совершенствованию информационной безопасности Беларуси.  
Основные меры:  
Совершенствование законодательства в области информационной безопасности.  
Развитие системы защиты информации государственных органов, организаций и граждан.  
Повышение осведомленности населения о вопросах информационной безопасности.  
Подготовка кадров в области информационной безопасности.  
Развитие международного сотрудничества в области информационной безопасности.**

**Задание 9**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
| **c** | **c** | **d** | **a** | **b** | **c** | **a** | **c** | **a** | **b** | **d** |