**Задание 1**

1. Биометрические данные могут собираться путем считывания, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения персональных данных, используя технические средства автоматизированной обработки информации и без их использования (Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных", статья 3).
2. Биометрические данные должны храниться в течение не дольше, чем это необходимо для достижения целей их обработки, если иное не предусмотрено федеральными законами (статья 6).
3. Субъект персональных данных имеет право отозвать свое согласие на обработку персональных данных (статья 9).
4. Сбором персональных данных может заниматься только субъект персональных данных или его представитель, а также уполномоченные государственные органы и муниципальные органы в соответствии с законодательством Российской Федерации (статья 6).
5. Требования к защите персональных данных включают в себя обеспечение их конфиденциальности, целостности и доступности, а также защиту от несанкционированного доступа к ним, в том числе от утечки и утраты данных (статьи 19-25).
6. Уровни безопасности данных могут быть различными и зависят от значимости персональных данных, а также от угроз их безопасности. Федеральными законами предусмотрено четыре уровня защиты персональных данных, которые должны быть обеспечены организациями при их обработке (статья 19).
7. Организации, осуществляющие обработку персональных данных, должны уведомлять субъектов персональных данных или их представителей о сборе и обработке их персональных данных, если иное не предусмотрено федеральными законами (статья 14).
8. Семь принципов обработки персональных данных включают в себя:

* законность обработки;
* целевое ограничение;
* связь объема и характера обрабатываемых персональных данных с целью их обработки;
* правомерность сбора персональных данных;
* точность персональных данных;
* сохранение персональных данных не дольше, чем необходимо для целей их обработки;
* защита персональных данных.

Эти принципы установлены Федеральным законом "О персональных данных" и являются основой правового регулирования обработки персональных данных в России. В соответствии с этими принципами, субъекты персональных данных обязаны соблюдать требования закона при сборе, обработке и хранении персональных данных.

1. В Российской Федерации угрозы безопасности персональных данных могут включать следующие типы:

* Несанкционированный доступ к персональным данным, например, взлом системы безопасности или доступ к данным, не предоставленный соответствующим лицам или организациям.
* Утрату персональных данных, например, в результате катастрофы или иных чрезвычайных ситуаций.
* Изменение или порчу персональных данных.
* Несанкционированный сбор персональных данных, например, путем незаконного доступа к сетевой инфраструктуре.

1. Для обеспечения различных уровней безопасности персональных данных необходимо реализовать ряд мероприятий:

* Уровень "Стандартная защита". Необходимо защитить данные от случайного и намеренного удаления. Для этого нужно проводить резервное копирование данных, использовать антивирусное программное обеспечение, установить пароль на доступ к компьютеру, серверу или базе данных.
* Уровень "Улучшенная защита". Для достижения этого уровня необходимо защитить данные от несанкционированного доступа. Это можно сделать путем ограничения доступа к персональным данным, использования средств шифрования информации, установки брандмауэра и других средств защиты.
* Уровень "Защита по ГОСТ Р ИСО/МЭК 27001-2013". Для обеспечения данного уровня необходимо разработать систему управления информационной безопасностью, реализовать меры защиты информации от утечки, внедрить меры контроля и аудита доступа к персональным данным.
* Уровень "Защита по ГОСТ Р ИСО/МЭК 27002-2005". Этот уровень обеспечивает комплексную защиту информации и требует проведения анализа угроз безопасности информации, оценки рисков и разработки стратегии управления рисками.

Для обеспечения высокого уровня безопасности персональных данных, необходимо также обеспечить надежность и безопасность технических средств хранения данных, применять шифрование информации при передаче и хранении, а также проводить регулярное обучение персонала по вопросам информационной безопасности.

**Задание 3**

1. Web Developer - расширение для Chrome и Firefox, которое предоставляет различные инструменты для отладки, проверки доступности и оптимизации веб-страниц.
2. Wappalyzer - расширение для Chrome и Firefox, которое позволяет определить используемые технологии на сайте, такие как CMS, фреймворки и другие инструменты разработки.
3. ColorZilla - расширение для Chrome и Firefox, которое позволяет извлекать цвета из веб-страницы и создавать цветовые палитры.
4. Window Resizer - расширение для Chrome и Firefox, которое позволяет изменять размер окна браузера, чтобы проверить, как веб-страница будет отображаться на различных устройствах.
5. PerfectPixel - расширение для Chrome и Firefox, которое помогает при работе с макетами, позволяет накладывать макет на веб-страницу и точно настраивать ее элементы.
6. Fontface Ninja - расширение для Chrome и Firefox, которое позволяет идентифицировать используемые шрифты на веб-страницах и даже копировать текст, написанный этим шрифтом.
7. Grammarly - расширение для Chrome и Firefox, которое проверяет грамматику и орфографию при написании текста на английском языке.
8. JSONView - расширение для Chrome и Firefox, которое форматирует JSON-данные на веб-странице для более удобного чтения и отладки.
9. LiveReload - расширение для Chrome и Firefox, которое автоматически перезагружает страницу после внесения изменений в файлы проекта.
10. Octotree - расширение для Chrome и Firefox, которое упрощает навигацию по репозиториям на GitHub, предоставляя древовидное представление файлов.
11. User-Agent Switcher - расширение для Chrome и Firefox, которое позволяет изменять заголовки User-Agent, чтобы проверить, как сайты отображаются на различных устройствах.
12. CSSViewer - расширение для Chrome и Firefox, которое позволяет просматривать CSS-свойства, примененные к любому элементу на веб-странице.
13. React Developer Tools - расширение для Chrome и Firefox, которое облегчает отладку приложений на React.
14. Redux Logger - расширение для Chrome и Firefox, которое позволяет отслеживать действия и состояние Redux-приложения в консоли браузера.
15. Redux Test Recorder - расширение для Chrome, которое автоматически записывает действия пользователя в Redux-приложении, чтобы их можно было использовать в тестах.