**Методы защиты информации**

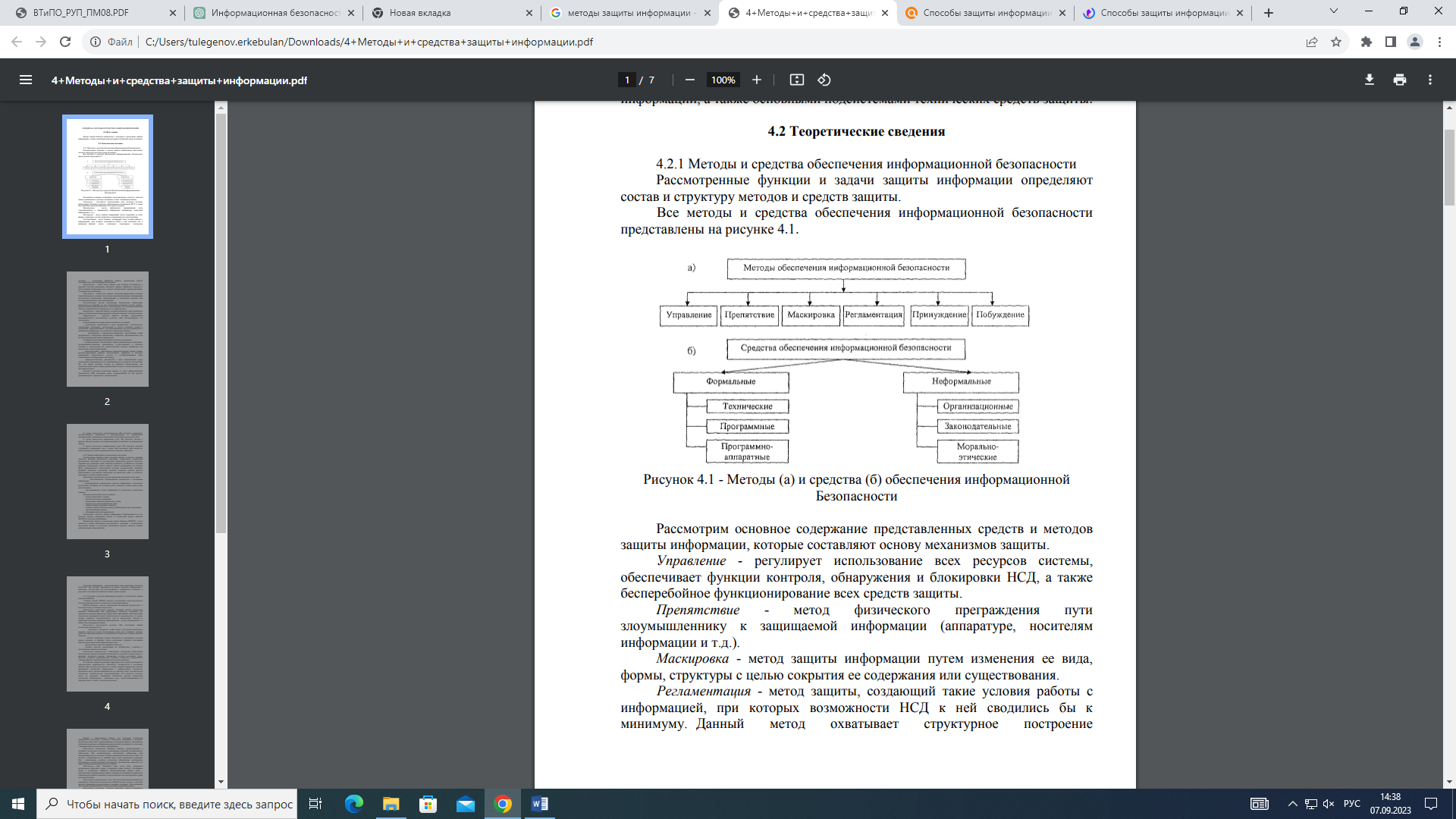
Данные в компьютерных системах подвержены риску утраты из-за неисправности или уничтожения оборудования, а также риску хищения. Способы защиты информации включают использование аппаратных средств и устройств, а также внедрение специализированных технических средств и программного обеспечения.

**Методы защиты**

На практике используют несколько групп методов защиты, в том числе:

* **препятствие на пути предполагаемого похитителя**, которое создают физическими и программными средствами;
* **управление**, или оказание воздействия на элементы защищаемой системы;
* **маскировка**, или преобразование данных, обычно – криптографическими способами;
* **регламентация**, или разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;
* **принуждение**, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;
* **побуждение**, или создание условий, которые мотивируют пользователей к должному поведению.

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – формальные и неформальные



|  |  |
| --- | --- |
| **Формальные средства защиты информации**  Разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности.  Чаще всего специалисты по безопасности:   * **разрабатывают внутреннюю документацию**, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией; * **проводят инструктаж** и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе; * **разграничивают зоны ответственности**, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков; * **внедряют программные продукты**, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации; * **составляют планы восстановления системы** на случай выхода из строя по любым причинам.   Если в компании нет выделенной ИБ-службы, выходом станет приглашение специалиста по безопасности на аутсорсинг. Удаленный сотрудник сможет провести аудит ИТ-инфраструктуры компании и дать рекомендации по ее защите от внешних и внутренних угроз. Также аутсорсинг в ИБ предполагает использование специальных программ для защиты корпоративной информации. | **Неформальные средства защиты информации**  Группа технических средств защиты информации совмещает аппаратные и программные средства. Основные:   * резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе; * дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных; * создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов; * обеспечение возможности использовать резервные системы электропитания; * обеспечение безопасности от пожара или повреждения оборудования водой; * установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.   В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией.  **Аутентификация и идентификация**  Чтобы исключить неправомерный доступ к информации применяют такие способы, как идентификация и аутентификация.  **Идентификация** – это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией.  **Аутентификация** – это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск.  Эти средства направлены на то, чтобы предоставить или, наоборот, запретить допуск к данным. Подлинность, как правила, определяется тремя способами: программой, аппаратом, человеком. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители) или данные. Простейший способ защиты – пароль. |

**Задание: Анализ и Разработка Мер Безопасности для Организации**

**Цель задания:** Студенты будут исследовать методы защиты информации и разработают план мер безопасности для вымышленной организации.

**Инструкции:**

1. Разделитесь на группы.
2. Каждая группа должна выбрать или создать вымышленную организацию (компанию, государственное учреждение, образовательное учреждение и т. д.), которая имеет чувствительную информацию (важная информация: секрет, пароли, ключи, технология).
3. Задача каждой группы - провести анализ рисков безопасности и определить потенциальные угрозы информационной безопасности для выбранной организации.
4. Вы должны предложить набор мер безопасности, которые помогли бы защитить организацию от выявленных рисков и угроз.
5. Меры безопасности могут включать в себя следующие аспекты (можно нарисовать схему, проекцию, расписать ПО какое будет, программы для фильтра, ОС какие, какие курсы):
   * **Физическая безопасность (защита серверных помещений, доступ к зданию и т. д.).**
   * **Сетевая безопасность (фаерволы, VPN, сегментация сети и т. д.).**
   * **Кибербезопасность (антивирусное ПО, системы обнаружения вторжений и т. д.).**
   * **Политики безопасности (пароли, правила доступа и т. д.).**
   * **Обучение сотрудников (курсы обучения, обучающие материалы и т. д.).**
6. Каждая группа должна представить свой план мер безопасности в виде презентации.
7. После презентации обсуждение в классе, где Вы можете задавать вопросы и давать обратную связь по планам мер безопасности других групп.