Тема 1: **Информация как объект защиты**

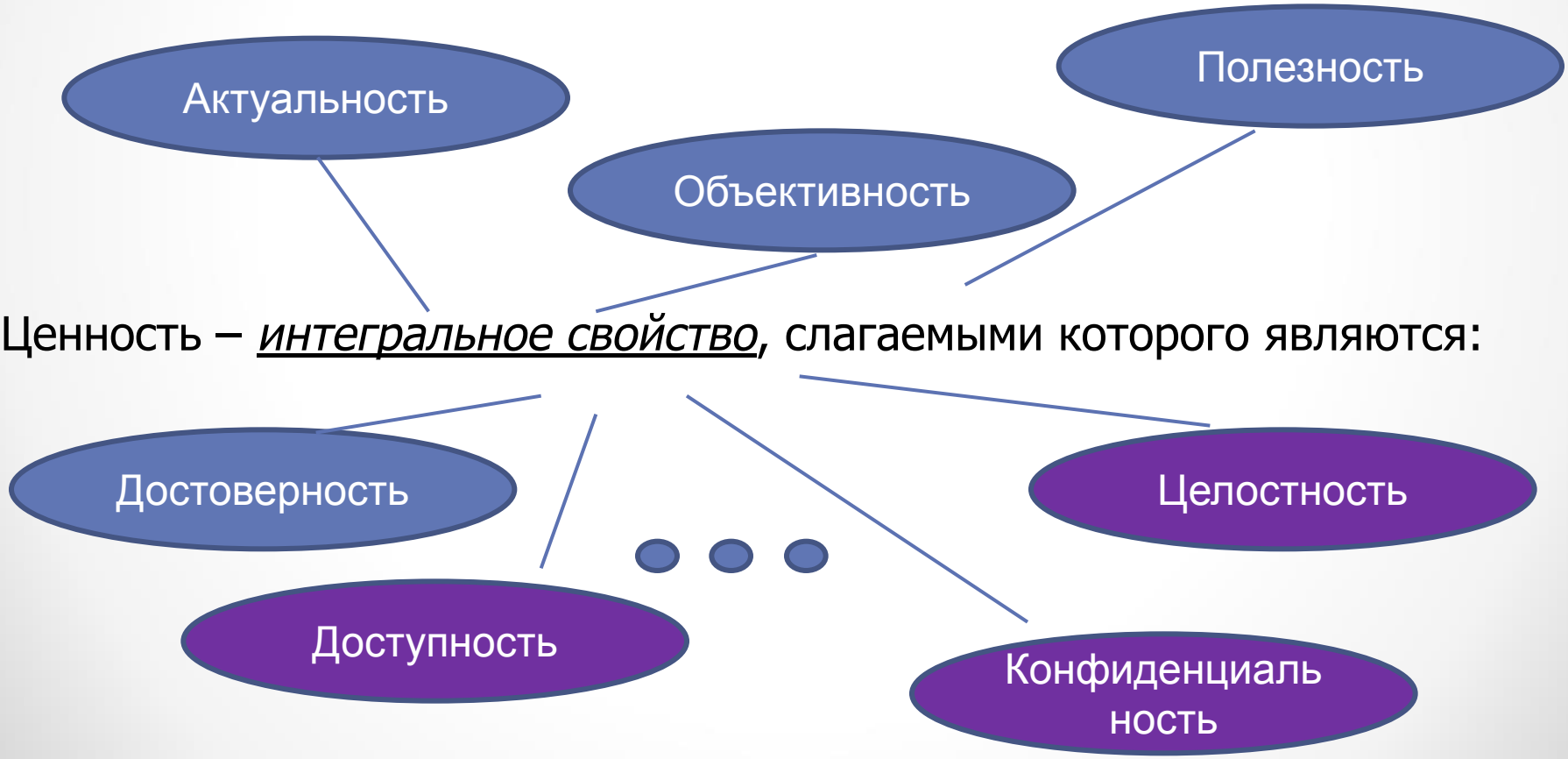
Учебные вопросы:

1. Ценность информации.
2. Тайна информации.
3. Доступ к информации

1. Ценность информации.

Обрабатываемая в информационных системах информация бывает ценной независимо от происхождения.

Ценность – свойство информации, определяемое степенью ее пригодности к практическому использованию в различных областях целенаправленной деятельности человека.



Нарушение любого свойства информации приводит к определенным потерям (**ущербу**), имеющим различный характер и различное выражение:

-денежные;
-материальные;
-репутационные (моральные);
-технические и др.

Все они в конечном счете могут быть выражены

Информационные активы требуют защиты

Для защиты информации необходимы затраты определенных сил и средств.

В денежном выражении затраты на защиту не должны превышать возможные потери.

Не всегда возможно и необходимо давать денежную оценку ценности информации (личная, политическая, военная, служебная).

В этом случае сравнивают ценность отдельных информационных элементов между собой с использованием разрабатываемых порядковых шкал ценностей (качественных).

Пример: очень высокая – высокая – средняя – низкая - незначительная

Ценность информации определяется экспертами, и относится к раз личным уровням критичности.
В этом случае документам, отнесенным к некоторому уровню по шкале, присваиваются соответствующие **грифы** (пометки) секретности.
Грифы секретности образуют порядковую шкалу.
Более высокий класс имеет более высокую ценность, следовательно – более высокие требования по защите.

Примеры порядковых шкал ценностей:

- **Секретно – Совершенно секретно – Особой важности;**

- **Конфиденциально – Строго конфиденциально – Абсолютно конфиденциально и др.**

Автоматизированная обработка информации с использованием ИТ требует более детальной классификации ценности с позиции определения **прав доступа пользователя** в информационному активу (файл, папка, диск, массив, база данных и др.).

В РФ исторически сложился подход к классификации государственной информации по уровням требований к ее защищенности основанный на оценке и обеспечении только одного свойства информации - **конфиденциальности** (**секретности**).
Требования к обеспечению целостности и доступности информации учитываются лишь косвенно среди общих требований к системам обработки, а остальные – практически не учитываются.

Логика: если к информации доступ имеет только узкий круг доверенных лиц, то вероятность ее искажения (несанкционированного уничтожения) незначительна.

Данный подход не подходит для информации, где степень конфиденциальности и доля конфиденциальной информации незначительна.

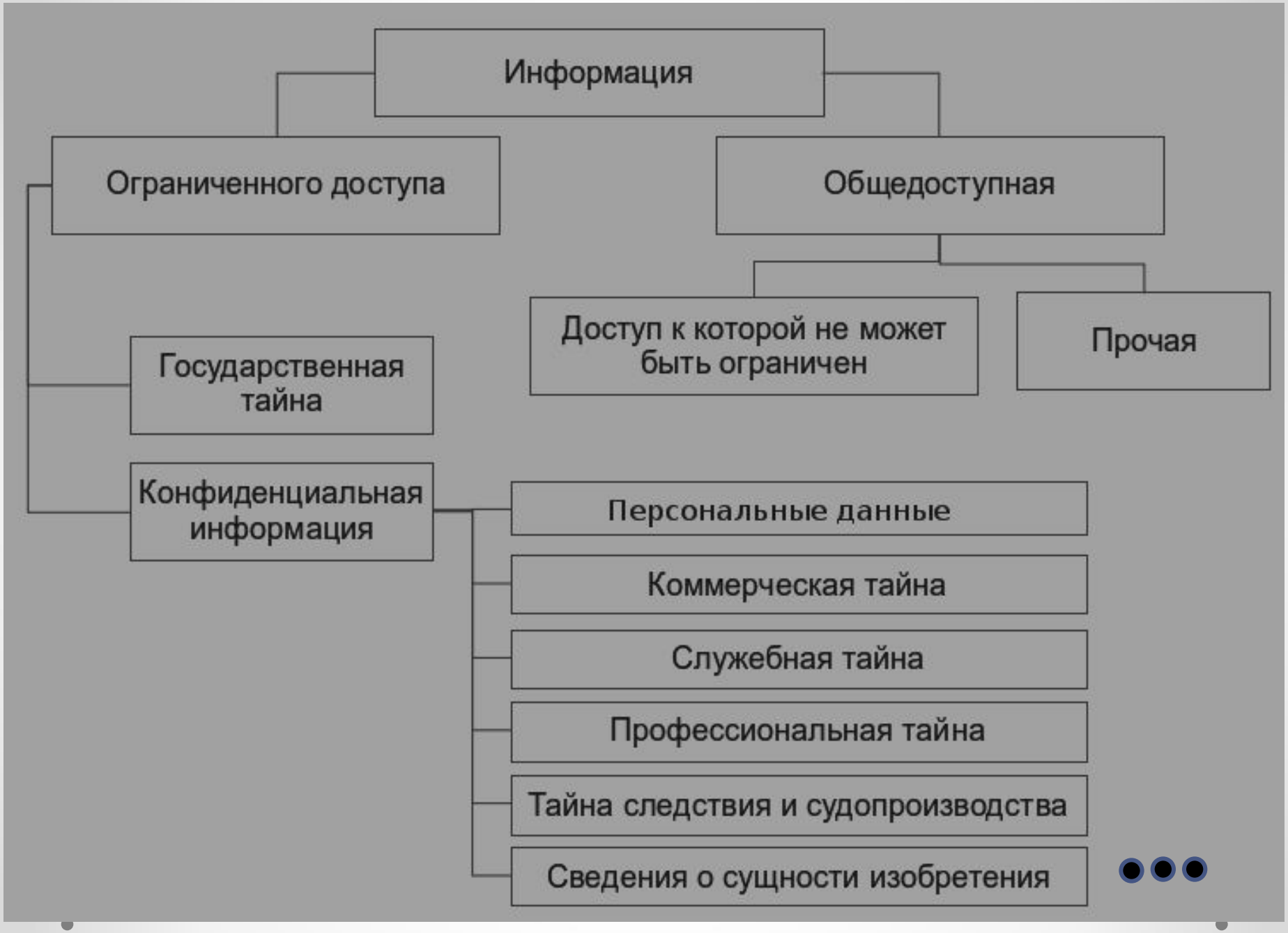
Считается, что **оценка и обеспечение других свойств ценности информации** не является задачей большинства систем ее обработки за исключением специально разработанных для оценки непротиворечивости, релевантности, достоверности и др. (например, поисковые системы Интернет, аналитические информационные системы).

2. Тайна информации.

Тайна - это охраняемые законом конфиденциальные и секретные сведения в области **частной жизни граждан, предпринимательской, финансовой, политической, экономической, военной и иных сферах**, известные или доверенные определенному кругу лиц в силу их профессиональных, служебных и иных обязанностей, незаконное получение, использование, разглашение которых причиняет вред или создает угрозу причинения вреда правам и законным интересам граждан, общества, государства и влечет за собой ответственность виновных лиц в соответствии с действующим законодательством.

В российском законодательстве насчитывается несколько десятков **(более 60!!!!!!)** видов тайн. Некоторые дублируют, пересекаются друг с другом и обозначают одно и тоже и не имеют особого значения:

-врачебная, медицинская;
-банковская, кредитных организаций
-врачебная, медицинская, личная, персональные данные;
-тайна следствия, тайна следствия и судопроизводства;
- тайна исповеди.

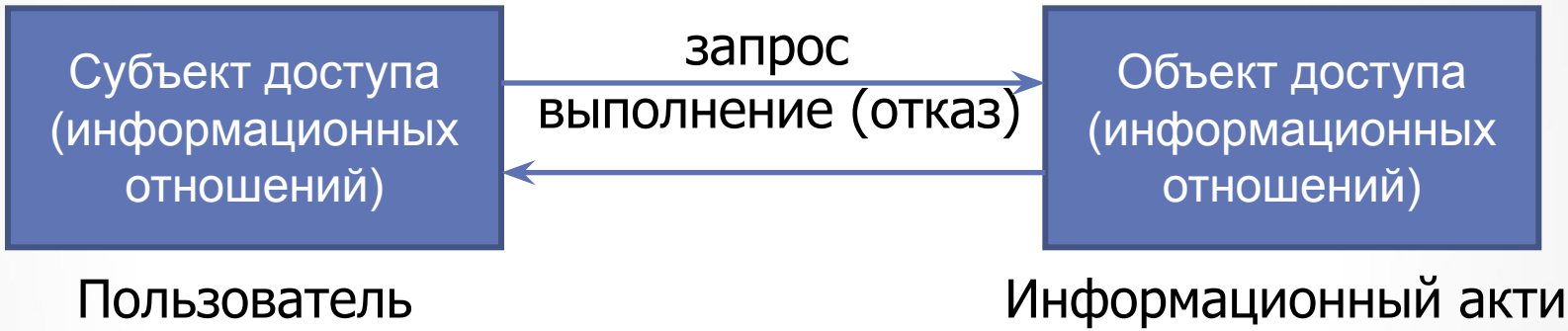

Информация
Ограниченного доступа
Общедоступная
Доступ к которой не может быть ограничен
Прочая
Государственная тайна
Конфиденциальная информация
Персональные данные
Коммерческая тайна
Служебная тайна
Профессиональная тайна
Тайна следствия и судопроизводства
Сведения о сущности изобретения

Информация, к которой нельзя ограничивать доступ:
(установлено законодательно)

- нормативным правовым актам, **затрагивающим права, свободы и обязанности** человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации **о состоянии окружающей среды**;
- информации **о деятельности государственных органов и органов местного самоуправления**, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информации, **накапливаемой в открытых фондах** библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- ***иной*** информации, недопустимость ограничения доступа к которой установлена федеральными законами.

3. Доступ к информации.

Это определенный тип взаимодействия объекта и субъекта информационных отношений, в результате которого создается (возникает) направленный поток информации.



Субъект доступа - активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы (пользователь, процесс, прикладная программа и др.)

Объект доступа - пассивный компонент системы, хранящий, принимающий или передающий информацию (файл, каталог и др.).

В автоматических (автоматизированных) информационных системах один и тот же компонент может являться **и субъектом, и объектом доступа.**

Например:

- приложение, запускаемое пользователем системы, является **объектом доступа** для данного пользователя;
- если же само приложение (объект) инициирует считывание файла, то при этом приложение выступает в роли **субъекта**.

Виды доступа:

Санкционированный - это вид доступа, не нарушающий установленные *правила ограничения (разграничения) доступа*, предназначенные для регламентации прав доступа субъектов к объектам доступа.

Несанкционированный (НСД) - это вид доступа, нарушающий установленные *правила ограничения (разграничения) доступа.* Субъект, осуществляющий НСД, является нарушителем правил разграничения доступа.

НСД – наиболее распространенный вид нарушений безопасности информации (преступлений в информационной сфере).