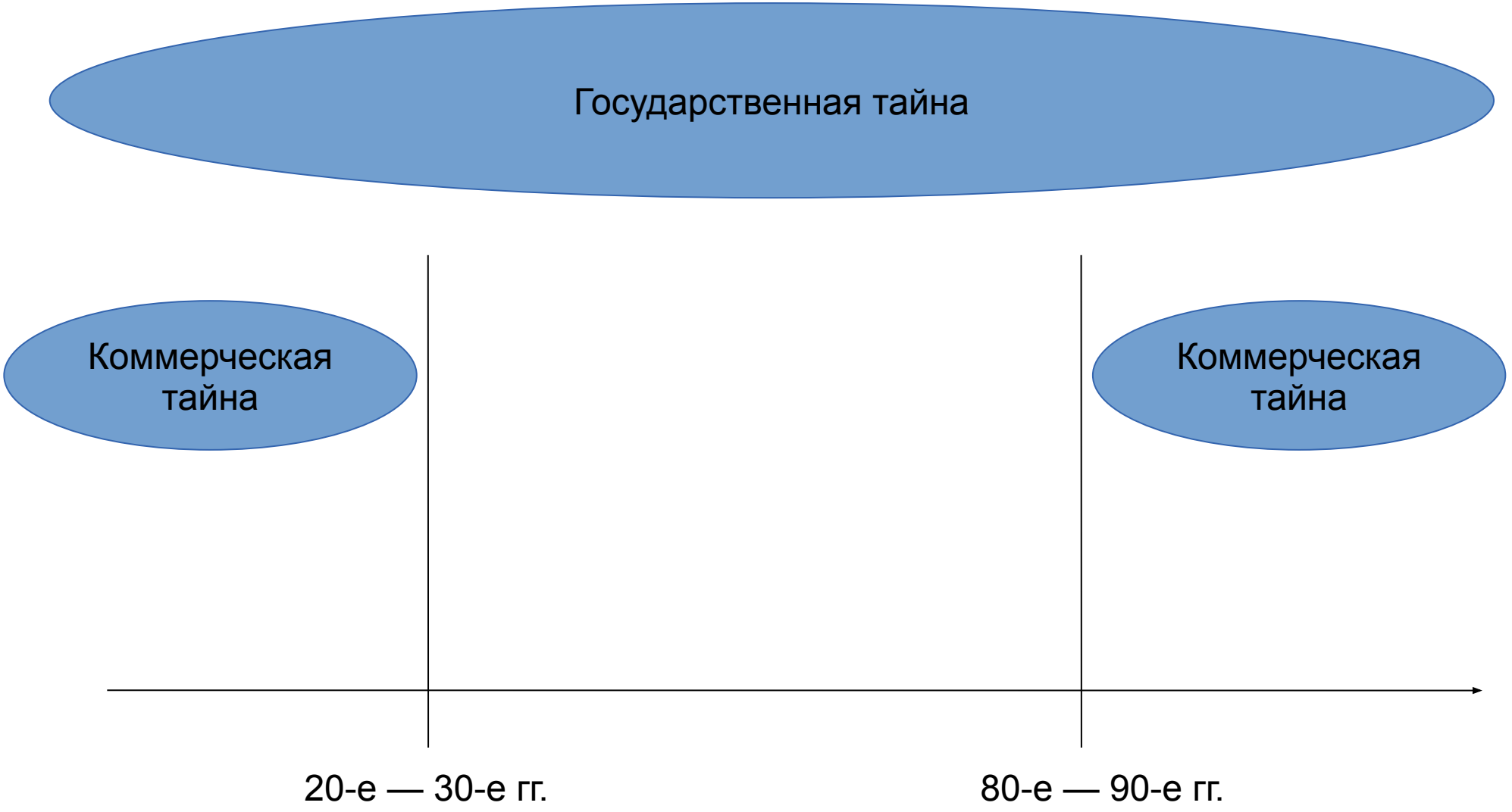
Тема лекции:

ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

План лекции:

1. Понятие государственной и коммерческой тайны
2. Причины искажения и потери компьютерной информации
3. Методы защиты информации

Понятия государственной и коммерческой тайны в России



Государственная тайна —

это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, распространение которых может нанести ущерб безопасности государства

Принцип секретности данных

Степень секретности сведений, составляющих государственную тайну, соответствует степени тяжести ущерба, который может быть нанесен государственной безопасности в результате распространения указанных сведений

Классификация секретной информации

Степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности:

- «особой важности»
- «совершенно секретно»
- «секретно»

Коммерческая тайна —

это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Под режимом конфиденциальности информации понимается введение и поддержание особых мер по защите информации.

Также под **коммерческой тайной** могут подразумевать саму информацию, то есть, научно-техническую, технологическую, производственную, финансово-экономическую или иную, в том числе составляющую секреты производства (ноу-хау)

Характеристики коммерческой тайны:

1)наличие действительной или потенциальной коммерческой ценности информации в силу неизвестности ее третьим лицам

2)отсутствие свободного доступа к информации на законном основании

3) обладателем информации введен режим коммерческой тайны

Обладатель информации имеет право отнести ее к **коммерческой тайне**, если эта информация обладает вышеперечисленными характеристиками и не входит в перечень информации, которая не может составлять коммерческую тайну (ст.5 закона «О коммерческой тайне»).

Чтобы информация получила **статус коммерческой тайны**, ее обладатель должен исполнить установленные процедуры (составление перечня, нанесение грифа и т.д.). После получения статуса коммерческой тайны информация начинает охраняться законом.

Определения и суть основных понятий, относящихся к вопросу о государственной и коммерческой тайне, подробно **раскрыты в следующих документах**:

1. Федеральный закон от 27.07.2006 № 149-ФЗ “**Об информации, информационных технологиях и о защите информации**”

2. Указ Президента РФ от 06.03.1997 “**Об утверждении перечня сведений конфиденциального характера**”

С целью защиты информации и сведений, составляющих государственную тайну, используются самые различные носители информации, среди которых:

- Бумага
- Микрографика
- Электронные носители

Сравнение носителей информации

	Бумага	Микрографика	Электронные носители
1. Наличие юридической силы	+	+	±
2. Длительность хранения	±	+	-
3. Компактность	-	±	+

Таким образом, можно считать целесообразным **решение, объединяющее несколько разнородных носителей**, которые не конкурируют, а дополняют друг друга

2. Причины искажения и потери компьютерной информации

При защите информации необходимо применять **системный подход**, т.е. нельзя ограничиваться отдельными мероприятиями.

Системный подход к защите информации включает следующие средства и действия:

- Организационные
- Физические
- Программно-технические

Все они представляют единый комплекс взаимосвязанных, взаимодополняющих и взаимодействующих мер

Основной принцип системного подхода —

это <u>принцип «разумной достаточности»</u>

Принцип «разумной достаточности»

заключается в том, что 100%-ной защиты не существует ни при каких обстоятельствах, поэтому стремиться стоит не к теоретически максимально достижимому уровню защиты, а к минимально необходимому в данных конкретных условиях и при данном уровне возможной угрозы

Накапливаемая и обрабатываемая на ЭВМ информация является достаточно уязвимой, подверженной:

- Разрушению
- Стиранию
- Искажению
- Хищению

Данные действия могут быть как случайными, так и несанкционированными

Классификация угроз для информации

Защита информации

— это способ обеспечения безопасности в вычислительной системе, то есть совокупность средств и методов, позволяющих управлять доступом выполняемых в системе программ к хранящейся в ней информации

Методы защиты информации, основываются на классификации угроз для информации.

1. Основной *способ защиты информации, предотвращающий снижение ее достоверности* - это своевременное обновление.

2. Защитой от разрушения является *резервное копирование данных*

Основные средства резервного копирования:

- программные средства, входящие в состав большинства комплектов утилит, для создания резервных копий
- аппаратные средства создания архивов на внешних носителях информации и raid массивы

Резервное копирование рекомендуется делать регулярно, причем **частота проведения** данного процесса **зависит от:**

- частоты изменения данных
- ценности информации
- сложности восстановления информации

Резервное копирование осуществляется с использованием соответствующих программных средств, при этом аппаратные устройства позволяют поддерживать копии в актуальном состоянии на протяжении всего периода работы.

В случае потери, информация может быть восстановлена:

- с использованием резервных данных
- без использования резервных данных

Во втором случае, для успешного восстановления данных необходимо чтобы:

- После удаления файла на освободившееся место не была записана новая информация
- Файл не был фрагментирован (для этого необходимо регулярно выполнять операцию дефрагментации)

3. Проблема несанкционированного доступа к информации обострилась и приобрела особую значимость в связи с развитием компьютерных сетей, прежде всего, глобальной сети Internet

Несанкционированный доступ - это чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий

Основные пути несанкционированного доступа:

- хищение носителей информации;
- копирование информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- использование недостатков операционных систем и языков программирования;
- использование программных закладок и программных блоков типа «троянский конь» и т.д.

Несанкционированный доступ осуществляется за счет:

- использования чужого имени
- изменения физических адресов устройств
- применения информации, оставшейся после решения задач
- модификации программного обеспечения
- хищения носителя информации
- установки аппаратуры записи

Для защиты информации от несанкционированного доступа применяются:

1. Организационные мероприятия.
2. Технические средства.
3. Программные средства.
4. Криптография.

Организационные мероприятия включают:	**Технические средства включают:**	**Программные средства включают:**
• пропускной режим на предприятии; • хранение носителей и устройств в сейфе; • ограничение доступа лиц в компьютерные помещения.	• ключ для блокировки ПК; • устройства аутентификации — для чтения отпечатков пальцев, формы руки, радужной оболочки глаза и т.д.;	• блокировка экрана и клавиатуры; • использование средств парольной защиты для доступа к данным и ПК (пары логин-пароль).

В качестве *основных видов несанкционированного доступа* к данным выделяют **чтение** и **запись**. В связи с этим, необходимо обеспечение защиты от чтения и записи информации

Защита данных от чтения автоматически подразумевает и защиту от записи, поскольку возможность записи при отсутствии возможности чтения практически бессмысленна

Защита от чтения и записи информации осуществляется:

- наиболее просто - на уровне ОС установкой соответствующих прав доступа пользователям ПК
- наиболее эффективно — шифрованием

На практике обычно используются комбинированные способы защиты информации от несанкционированного доступа