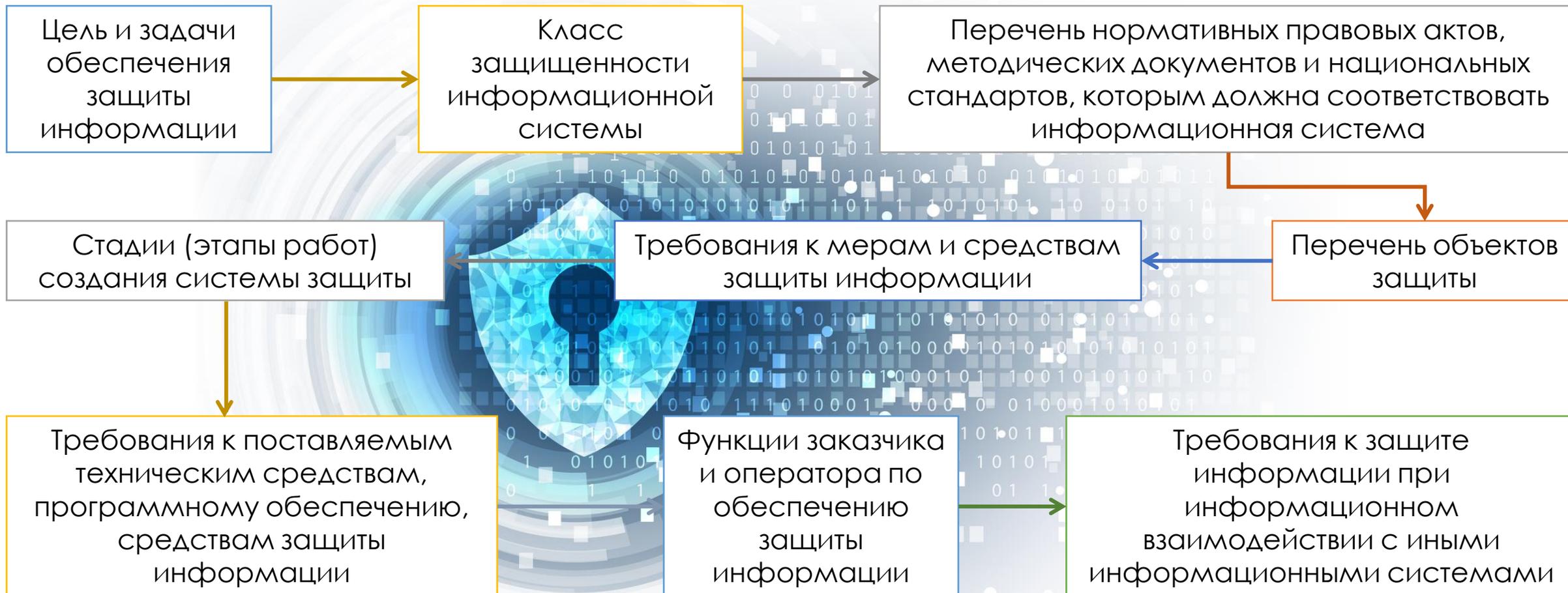


# **Государственные информационные системы и защита информации, не составляющей государственную тайну, в государственных информационных системах**

## **Лекция 4. Разработка систем защиты информации для государственных информационных систем**

## Требования к системе защиты информации



## Разработка системы защиты информации информационной системы



Проектирование системы защиты информации

Модель угроз безопасности информации и (или) техническое задание на создание системы согласуются с ФСБ России и ФСТЭК России (п. 3 ПП РФ № 676)

Техническое задание на создание системы и модель угроз безопасности информации утверждаются должностным лицом органа исполнительной власти, на которое возложены соответствующие полномочия (п. 4 ПП РФ № 676)

Разработку эксплуатационной документации на систему защиты информации

а) перечень действий сотрудников при выполнении задач по эксплуатации системы;  
б) контроль работоспособности системы и компонентов, обеспечивающих защиту информации;  
в) перечень неисправностей и рекомендации в отношении действий при их возникновении;  
г) перечень режимов работы системы и их характеристики, а также порядок и правила перевода системы с одного режима работы на другой с указанием необходимого для этого времени. (п. 7 ПП РФ № 676)

Макетирование и тестирование системы защиты информации

## Организационные и технические меры защиты информации, должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.



## Выбор мер по обеспечению безопасности информации

Определение базового набора мер



Адаптация базового набора мер

Уточнение адаптированного базового набора мер

Дополнение уточненного адаптированного базового набора мер

В случае если меры защиты информации, реализованные в информационно-телекоммуникационной инфраструктуре центра обработки данных, обеспечивают блокирование угроз безопасности информации, актуальных для функционирующей на его базе информационной системы, принятие дополнительных мер защиты информации в данной информационной системе не требуется. При этом полномочия в части защиты информации должны быть распределены между оператором информационной системы и оператором информационно-телекоммуникационной инфраструктуры центра обработки данных.

При проектировании вновь создаваемых или модернизируемых информационных систем, имеющих доступ к информационно-телекоммуникационной сети "Интернет", должны выбираться маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности).

