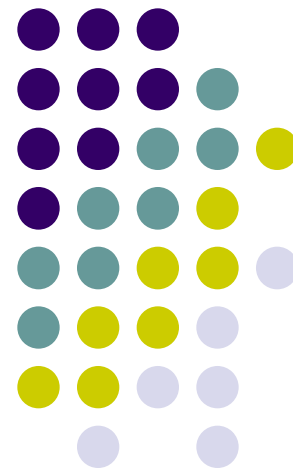
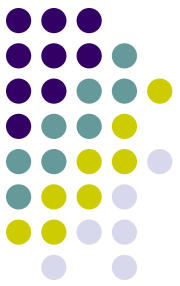


# Администрирование информационных систем

Шифрование



# Информационная безопасность



- Под **информационной безопасностью** понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.
- **Защита информации** – комплекс мероприятий, направленных на обеспечение информационной безопасности.

# Проблемы информационной безопасности



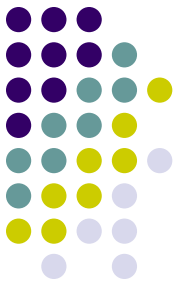
- По данным отчета «Компьютерная преступность и безопасность – 1999: проблемы и тенденции»
  - 32% респондентов – обращались в правоохранительные органы по поводу компьютерных преступлений
  - 30% респондентов – сообщили, что их ИС были взломаны злоумышленниками;
  - 57% - подверглись атакам через Интернет;
  - 55% - отметили случаи нарушений ИБ со стороны собственных сотрудников;
  - 33 % - не смогли ответить на вопрос «были ли взломаны Ваши веб-серверы и системы электронной коммерции?».

# Угрозы информационной безопасности



- **Угроза информационной безопасности (ИБ)** – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
- Попытка реализации угрозы называется **атакой**.
- Классификация угроз ИБ можно выполнить по нескольким критериям:
  - **по аспекту ИБ** (доступность, целостность, конфиденциальность);
  - **по компонентам ИС**, на которые угрозы нацелены (данные, программа, аппаратура, поддерживающая инфраструктура);
  - **по способу осуществления** (случайные или преднамеренные действия природного или техногенного характера);
  - **по расположению источника угроз** (внутри или вне рассматриваемой ИС).

# Свойства информации



- Вне зависимости от конкретных видов угроз информационная система должна обеспечивать базовые свойства информации и систем ее обработки:
  - **доступность** – возможность получения информации или информационной услуги за приемлемое время;
  - **целостность** – свойство актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения;
  - **конфиденциальность** – защита от несанкционированного доступа к информации.

# Примеры реализации угрозы нарушения конфиденциальности

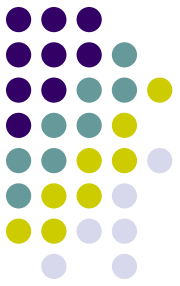


- Часть информации, хранящейся и обрабатываемой в ИС, должна быть сокрыта от посторонних. Передача данной информации может нанести ущерб как организации, так и самой информационной системе.
- Конфиденциальная информация может быть разделена на **предметную** и **служебную**. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, однако ее раскрытие может привести к несанкционированному доступу ко всей информации.
- Предметная информация содержит информацию, раскрытие которой может привести к ущербу (экономическому, моральному) организации или лица.
- Средствами атаки могут служить различные технические средства (подслушивание разговоров, сети), другие способы (несанкционированная передача паролей доступа и т.п.).
- Важный аспект – непрерывность защиты данных на всем жизненном цикле ее хранения и обработки. Пример нарушения – доступное хранение резервных копий данных.

# Средства защиты информационных систем



- Такие средства могут быть классифицированы по следующим признакам:
  - **технические средства** – различные электрические, электронные и компьютерные устройства;
  - **физические средства** – реализуются в виде автономных устройств и систем;
  - **программные средства** – программное обеспечение, предназначенное для выполнения функций защиты информации;
  - **криптографические средства** – математические алгоритмы, обеспечивающие преобразования данных для решения задач информационной безопасности;
  - **организационные средства** – совокупность организационно-технических и организационно-правовых мероприятий;
  - **морально-этические средства** – реализуются в виде норм, сложившихся по мере распространения ЭВМ и информационных технологий;
  - **законодательные средства** – совокупность законодательных актов, регламентирующих правила пользования ИС, обработку и передачу информации.



# Шифрование

- Одним из способов защиты данных, предоставляемых Интернет-службами, является метод SSL-шифрования/аутентификации на веб-сайтах.
- Используются три вида сертификатов:
  - Сертификаты сервера;
  - Сертификаты клиента;
  - Сертификаты подписывания кода.



# Типы сертификатов.

## Сертификаты сервера



- Сертификаты сервера обеспечивают метод шифрования данных, передаваемых через сеть посредством SSL и методы идентификации сервера.
- Методы позволяют клиенту быть уверенным в подлинности сайта, который он посетил.

# Типы сертификатов.

## Сертификаты клиента.



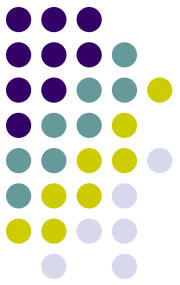
- Сертификаты клиента обеспечивают идентификацию клиента на сервере, что позволяет серверу определить, кем на самом деле является клиент.
- Данная аутентификация является более предпочтительной по сравнению с базовой.
- Сертификаты клиентов не поддерживают шифрование данных.

# Типы сертификатов.

## Сертификаты подписывания кода.



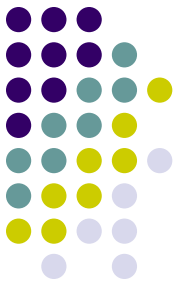
- Сертификаты подписывания кода обеспечивают метод шифрового «подписывания» приложения посредством цифрового идентификатора, созданного на основе содержимого приложения.
- Если в приложении произошли изменения, то цифровой идентификатор теряет соответствие этому приложению и пользователь получает уведомление.
- Сертификаты подписывания не поддерживают шифрования приложений.



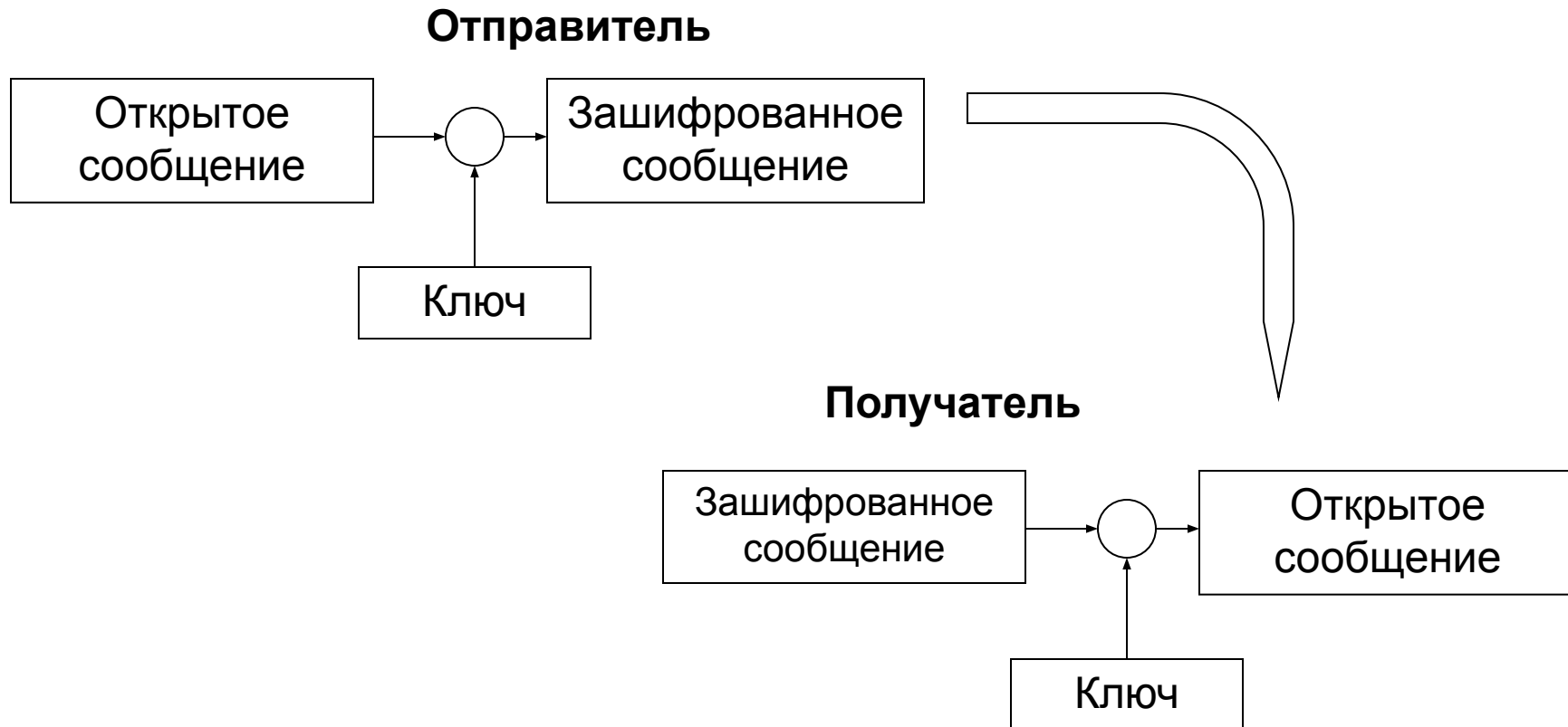
# Ключи сертификатов

- Цифровые сертификаты используют ключи при шифровании данных.
- **Ключ** – фрагмент данных, используемых криптографической системой для преобразования открытого текста в зашифрованный текст.
- Криптографическое преобразование (шифрование) – это математический алгоритм преобразования цифровых данных.

# Криптографические средства защиты данных



- Для обеспечения защиты информации в распределенных информационных системах активно применяются криптографические средства защиты информации.
- Сущность криптографических методов заключается в следующем:



# Бюро сертификатов и доверие



- При создании пары ключей (в алгоритмах несимметричного шифрования) для использования на веб-сайте, запрашивается сертификат SSL X.509 у бюро сертификатов – сервера, выпускающего сертификаты.
- Бюро сертификатов может авторизовать (уполномочить) любое число сертификатов, те, в свою очередь, другие бюро и т.д.
- Первое бюро сертификатов называется корневым.

# Использование бюро сертификатов на компьютере клиента



- На клиенте может быть установлен набор сертификатов по умолчанию, выпустившие их бюро сертификатов являются доверенными.
- При представлении клиенту сертификата SSL клиент выяснит, имеется ли в его кэше соответствующий сертификат.
- При наличии сертификата клиент проверяет подпись бюро сертификатов при помощи открытого ключа, находящегося в кэше, осуществив аутентификацию сервера.
- Если сертификат отсутствует в кэше, клиент запросит сертификат и повторит проверку сертификата.

# Список доверенных бюро сертификатов



Сертификаты

Назначение: Проверка подлинности клиента

Доверенные корневые центры сертификации | Доверенные издатели | Издатели, не

Кому выдан	Кем выдан	Срок де...	Понятное имя
Class 3 Public Prima...	Class 3 Public Primary ...	08.01.2004	VeriSign Class 3 ...
dima-home	dima-home	06.04.2011	<нет>
Entrust.net Secure ...	Entrust.net Secure Se...	25.05.2019	Entrust.net Secu...
First Data Digital C...	First Data Digital Certi...	03.07.2019	First Data Digital...
GTE CyberTrust Glo...	GTE CyberTrust Globa...	14.08.2018	GTE CyberTrust ...
GTE CyberTrust Root	GTE CyberTrust Root	04.04.2004	GTE CyberTrust ...
GTE CyberTrust Root	GTE CyberTrust Root	24.02.2006	GTE CyberTrust ...
Microsoft Root Aut...	Microsoft Root Authority	31.12.2020	Microsoft Root A...
Microsoft Root Cert...	Microsoft Root Certifi...	10.05.2021	Microsoft Root C...

Импорт... Экспорт... Удалить Дополнительно...

Назначения сертификата

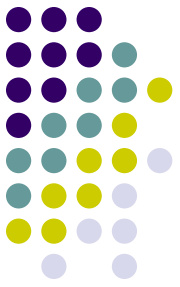
<Все>

Просмотр

Закреть

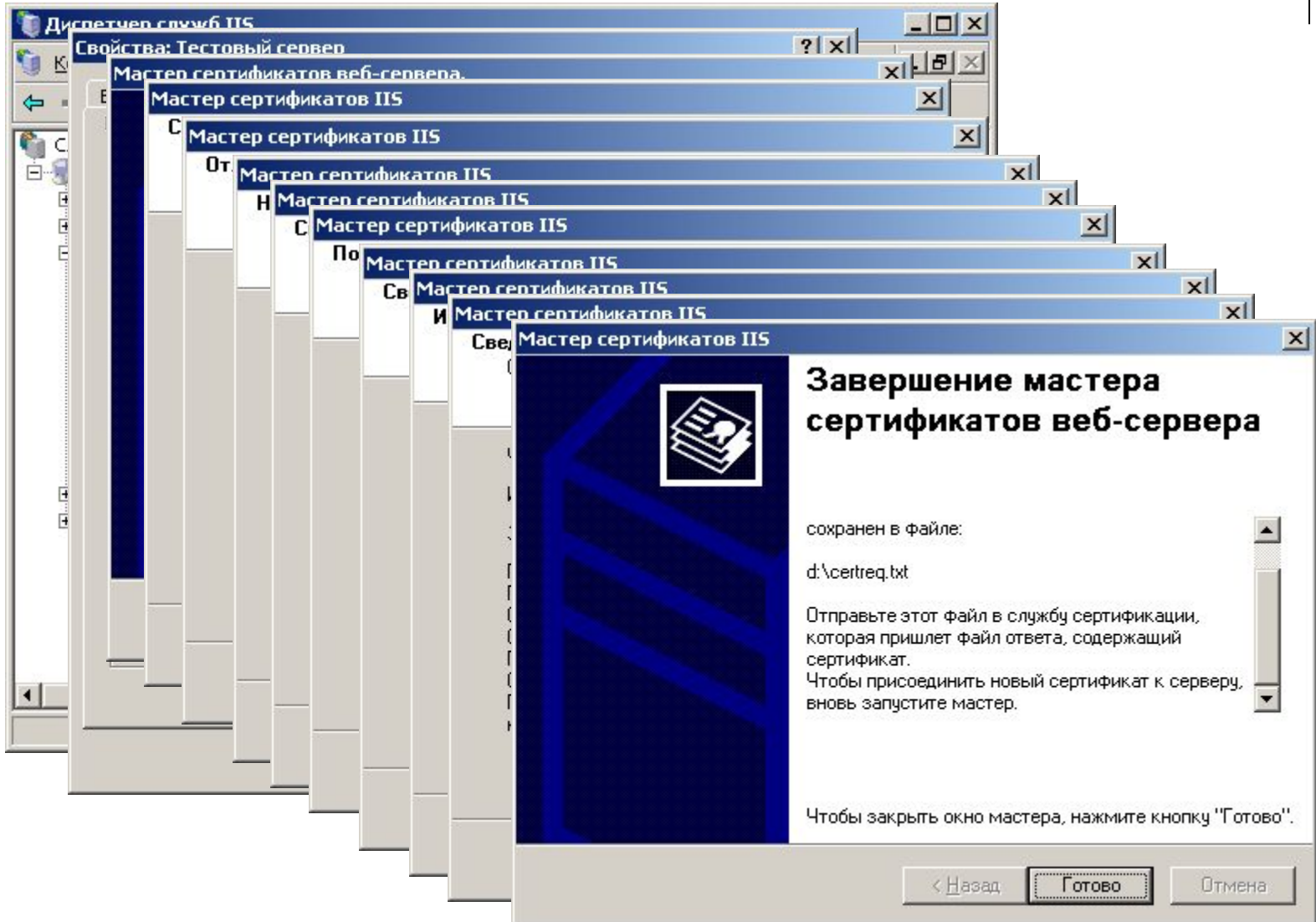
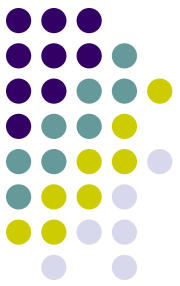


# Создание собственного бюро сертификатов



- Для установки собственного бюро сертификатов необходима установка **служб сертификатов** на сервер.
- Установка выполняется стандартным образом с помощью мастера установки и удаления программ.
- Установка различается для разных типов бюро:
  - Корпоративное корневое бюро сертификатов
  - Корпоративное подчиненное бюро сертификатов
  - Отдельное корневое бюро сертификатов
  - Подчиненное бюро сертификатов.

# Создание запроса на сертификат в IIS



# Отправка запроса в собственное бюро

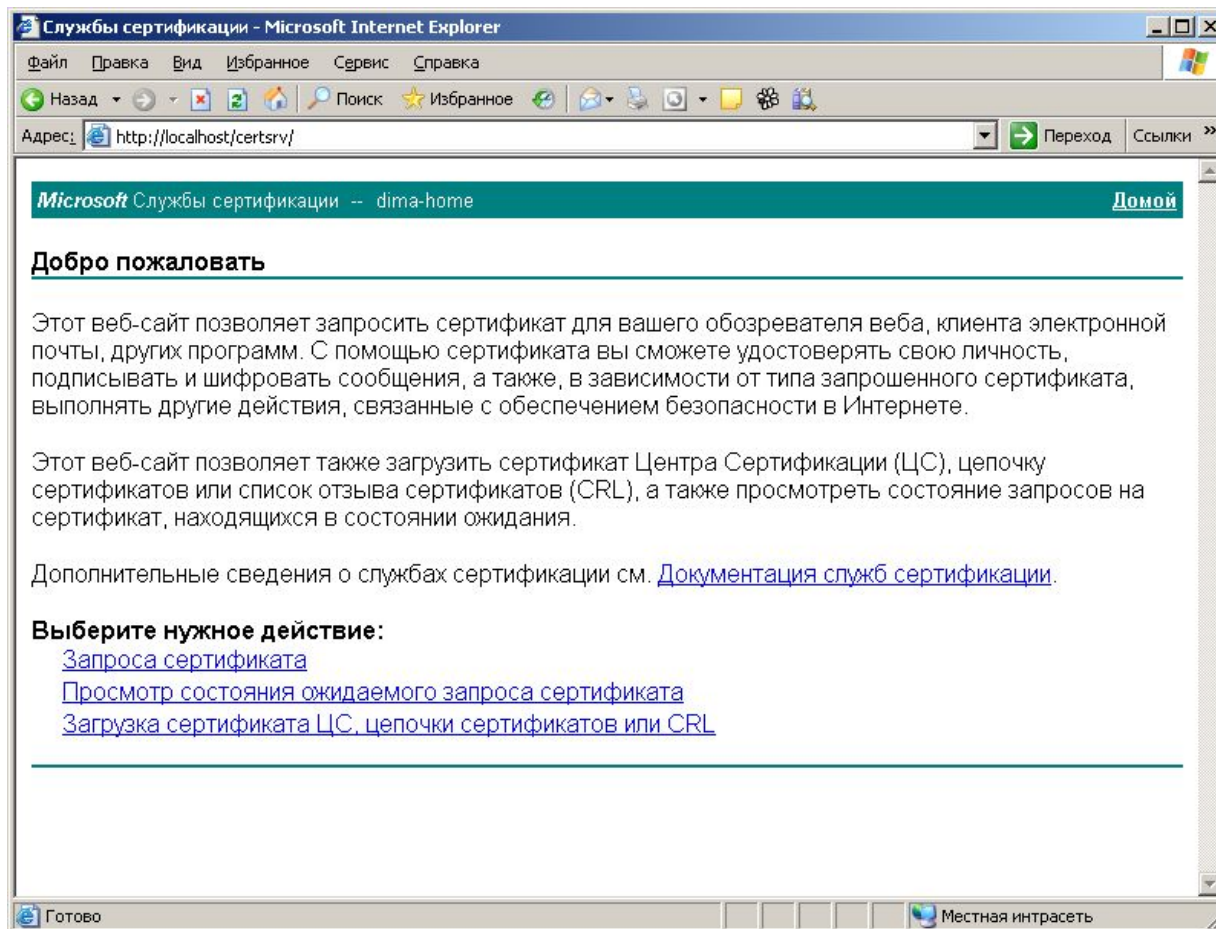


- Для запроса сертификата у собственного бюро сертификации можно двумя способами:
  - С помощью Интернет регистрации;
  - Отправка запроса через оснастку **Сертификаты.**

# Использование Интернет регистрации



- Для доступа к интернет-регистрации бюро сертификатов выполняется через страницу [http://<ваш\\_сервер>/certsrv/](http://<ваш_сервер>/certsrv/).



# Отправка запроса из оснастки Центр сертификатов

