КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ

Громов Роман КБ-41 СО

Введение

- Криптографические методы в настоящее время являются базовыми для обеспечения надежной аутентификации сторон информационного обмена, защиты информации в транспортной подсистеме АС, подтверждения целостности объектов.

К средствам криптографической защиты информации (СКЗИ) относят:

- Аппаратные средства
- Программно-аппаратные средства
- Программные средства

Криптографические алгоритмы преобразования информации реализуются **с целью:**

- Защиты информации при ее обработке, хранении и передаче.
- Обеспечения достоверности и целостности информации.
- Выработки информации, используемой для идентификации и аутентификации субъектов АС.

//Для справки

- **Аутентифика́ция** (англ. *Authentication*) — процедура проверки подлинности.

Например : проверка подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных пользователей.

//Для справки

- **Идентификация** (англ. *Identification*) — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе.

Например : идентификация файла по контрольной сумме, результат-имя файла.

//Для справки

- **Авториза́ция** (от англ. *authorization*) — предоставление определённому лицу или группе лиц прав на выполнение определённых действий.

Например : разграничение доступа в операционных системах.

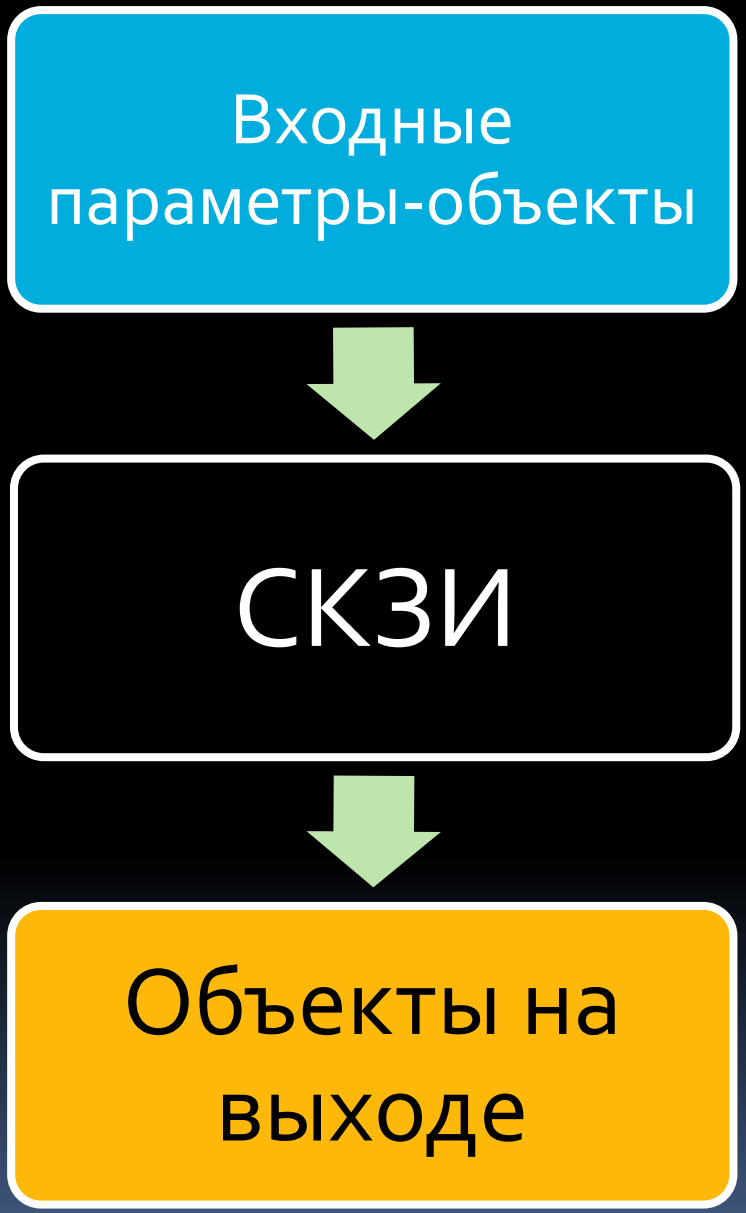
- **Криптографическое преобразование** – это преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом), и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания действующего ключа.

Особенности криптографического преобразования:

Входные и выходные аргументы криптографического преобразования присутствуют в АС в некоторой материальной форме

Реализовано в виде материального объекта, взаимодействующего с окружающей средой

- Можно говорить о том, что СКЗИ оперирует вполне самостоятельными объектами – параметрами, которые могут быть объектами некоторой политики безопасности (например, ключи шифрования должны быть защищены от НСД)
- СКЗИ в составе защищенных АС имеют конкретную реализацию -это может быть отдельное специализированное устройство, встраиваемое в компьютер, либо специализированная программа.


Входные параметры-объекты
СКЗИ
Объекты на выходе


Venus and Adonis

// Для справки:

- **Политика безопасности организации** (англ. *organizational security policies*) — совокупность руководящих принципов, правил, процеду р и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

// Для справки:

Политика безопасности зависит:

- от конкретной технологии обработки информации
- от используемых технических и программных средств
- от расположения организации

// Для справки:

- **Несанкционированный доступ** — доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации. Также несанкционированным доступом в отдельных случаях называют получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

Важные моменты СКЗИ

Обменивается информацией с внешней средой: в него вводятся ключи, открытый текст при шифровании

В случае аппаратной реализации возможны неисправности или отказы техники

В случае программной реализации возможны программные сбои и влияние посторонних программ

Хранится на материальном носителе и может быть преднамеренно или непреднамеренно искажено

Важные моменты СКЗИ

Взаимодействует с внешней средой косвенным образом (питается от электросети, излучает электромагнитные поля и т.д.)

Изготавливает или/и использует человек, который может допустить ошибки (преднамеренные или случайные) при разработке и эксплуатации.

Причины нарушения безопасности информации при ее обработке СКЗИ

Возможные утечки по техническим каналам:

- излучение электронно-лучевой трубки дисплея
- излучение системного блока
- звуки и вибрации от нажатий клавиш
- Звуки работы периферийных устройств (принтер, сканер)
- голоса операторов СКЗИ

Неисправности в элементах СКЗИ:

- Могут сказаться на виде шифрующего преобразования (скачки напряжения)
- Могут привести к упрощению реализации шифрующего преобразования
- Могут нанести недопустимый вред всей системе в целом

Работа совместно с другими программами:

- Непреднамеренное влияние : программы борются за ресурсы операционной системы, ошибки допущенные разработчиками
- Преднамеренное влияние: разработка специальных «закладок» (они же вирусы, программы-шпионы, троянские кони), которые воздействуют на СКЗИ

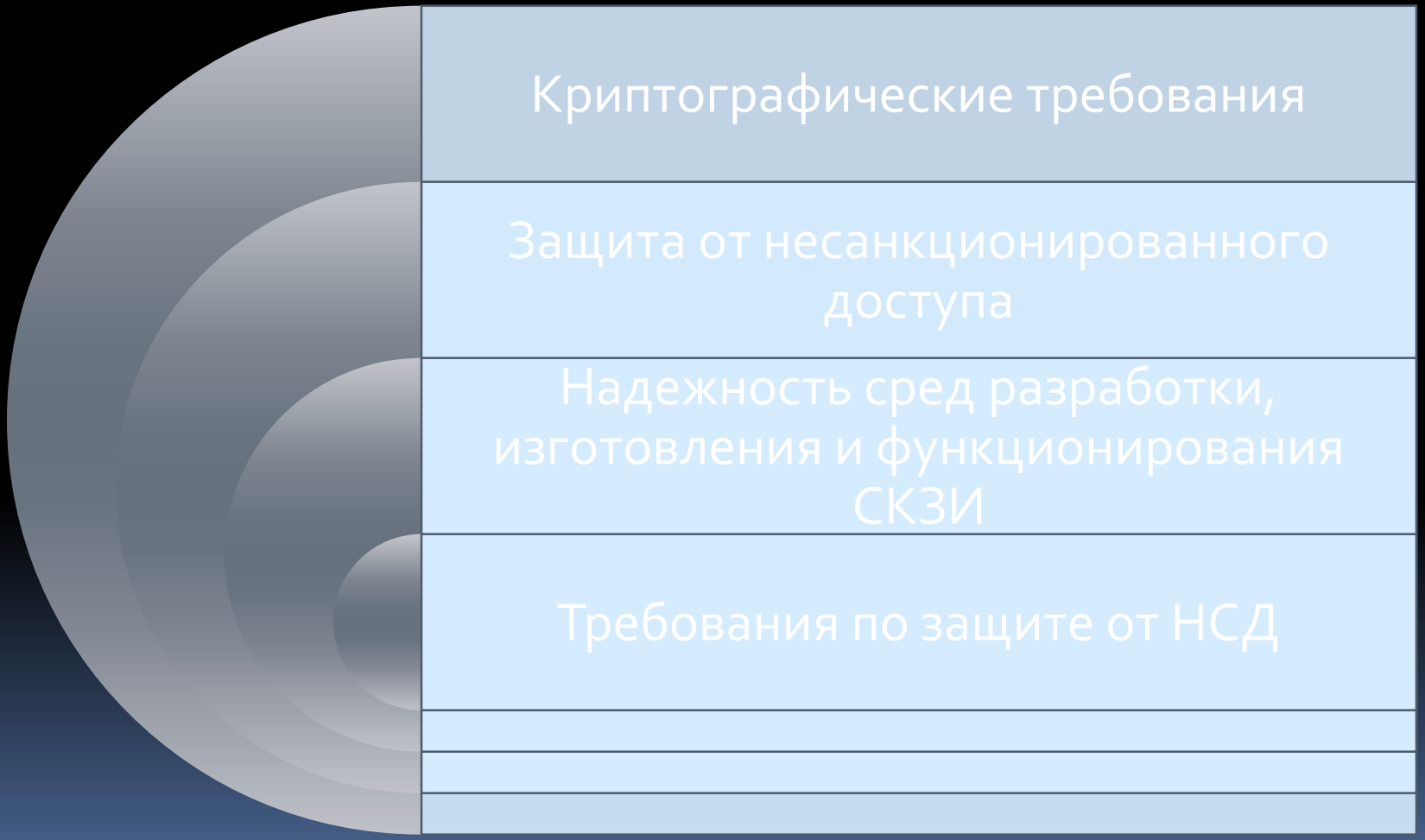
Разделяют режимы работы программ-закладок:

- Пассивный : сохранение вводимых ключей или открытых текстов без влияния на информацию
- Активный: влияние на процессы записи – считывания информации (например, чтение информации из оперативной памяти)

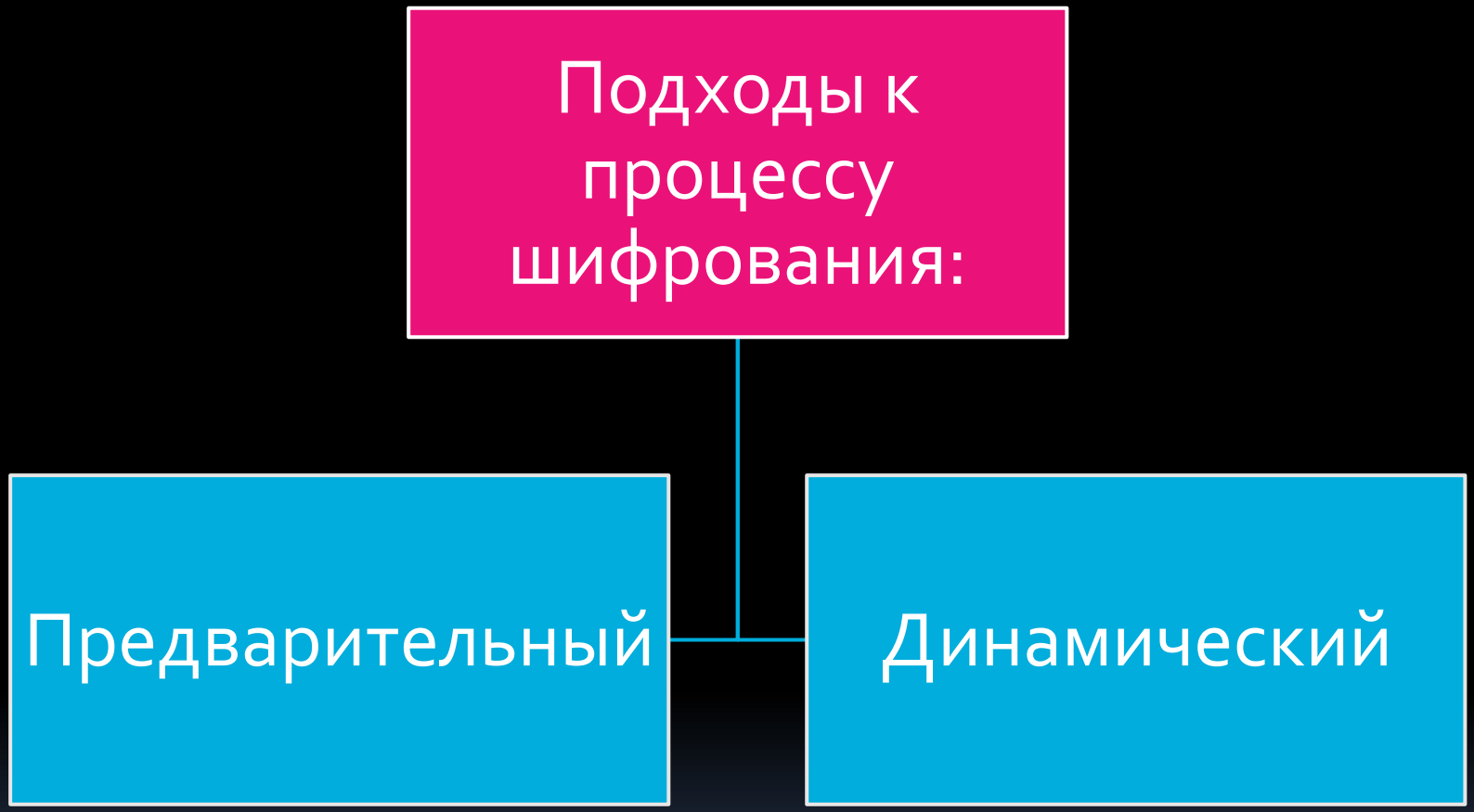
Воздействие человека

- Разработчик преднамеренно или непреднамеренно может внести в программу некоторые не декларированные свойства (например, возможность переключения в отладочный режим с выводом части информации на экран или внешние носители.)
- Человек может неправильно использовать программу (вводить короткие пароли или повторять один и тот же пароль)

Требования к СКЗИ



Способы и особенности реализации СКЗИ



Предварительное шифрование

Предварительное шифрование состоит в зашифровании файла открытого текста программой (субъектом), а затем расшифровании тем же или иным субъектом. Данный подход имеет ряд недостатков:

- необходимость дополнительного ресурса для работы с зашифрованным объектом (дискового пространства)
- потенциальная возможность доступа со стороны активных субъектов
- необходимость задачи гарантированного уничтожения расшифрованного файла после его использования

Динамическое шифрование

- Происходит зашифрование всего файла (аналогично предварительному шифрованию). Затем с использованием специальных механизмов, ведется работа с зашифрованным объектом. При этом расшифрованию подвергается только та часть объекта, которая в текущий момент времени используется прикладной программой.