***Билет 16***

При выборе методов и средств защиты данных нужно учитывать, что существует несколько принципов защиты от несанкционированного доступа (НСД). На них основана работа средств программно-аппаратной защиты:

* доступ к данным предоставляется только тем пользователям, которые уполномочены его получить на уровне внутренних документов компании;
* каждый уполномоченный пользователь имеет доступ только к своему уровню информации, его прав недостаточно для работы с данными, находящимися в сфере ответственности других пользователей;
* перечень операций, которые допустимо выполнять с данными, строго регламентирован, и зависит от изначально заданных прав пользователей.

Для защиты от НСД в аппаратно-программных средствах должен быть механизм распознавания уполномоченного пользователя и его авторизации (идентификации и аутентификации).

Процесс авторизации состоит из трех этапов:

**1. Идентификация.** Пользователь должен передать системе свой идентифицирующий признак, например, логин и пароль. При использовании аппаратных средств становится возможной и более глубокая степень идентификации по отпечатку пальца, сетчатке глаза, иным биометрическим признакам или на основании владения определенным устройством (магнитная карточка, электронный ключ);

**2. Аутентификация.** Этот процесс в работе программно-аппаратных средств нацелен на сравнение заявленного пользователем идентифицирующего признака с теми, которые хранятся в памяти устройства. В ходе аутентификации устанавливается подлинность пользователя. Она может реализовываться на основе простой или усложненной PIN-идентификации. В обоих случаях персональный идентификационный номер пользователя сравнивается с эталоном. При простом механизме идентификации система проводит обычное сравнение и в случае совпадения выдает разрешение на дальнейшую работу. При сложном, защищенном, система посылает запрос ключу, тот «отвечает» отправкой 64-разрядного ключа. Система складывает число с введенным пользователем PIN-кодом, направляя полученный результат ключу, тот проводит итоговую идентификацию, при положительном результате которой выдает разрешение на работу;

**3. Авторизация.** После того как подлинность пользователя установлена, аппаратно-программным средством определяется объем предоставленных ему прав.

**Электронные ключи**

Работа программно-аппаратных средств защиты информации становится невозможной, если их архитектурой не предусмотрено наличие электронных ключей. Они представляют собой явление предметного мира, физическое устройство, снабженное электронной начинкой и содержащее уникальную информацию, позволяющую идентифицировать пользователя.

Ключи бывают трех видов:

1. Специализированный электронный чип.
2. Микросхема перепрограммируемой памяти, имеющая собственные источники электропитания.
3. Ключ на базе микропроцессора.