**Нестеренко Пётр Алексеевич**

**Билет № 22**

**1*. Как реализуется ролевая модель безопасности?*** **Ответ:** В организациях, связанных с обработкой информации, для большинства сотрудников **разграничение полномочий** по доступу к информационным ресурсам строится в соответствии с **занимаемой ими должностью**. При этом многие должности объединяет достаточно большие группы работников, имеющих одинаковые функциональные обязанности. Т. е. **должность работника можно трактовать как роль**, предоставляющую ему некоторые обобщенные права по доступу к данным свойственные целой группе пользователей ИС, имеющих такую же должность.

Для каждого пользователя одновременно могут быть активными **несколько ролей**, каждая из которых дает ему определенные права. РУД не является отдельной самодостаточной моделью, регламентирующей все детали доступа. **Детальная регламентация доступа субъектов к объектам ИС в Ролевое управление доступом осуществляется на основе Дискреционная модель безопасности или Мандатная модель безопасности**. По этой причине ролевое управление доступом не выделяется в отдельную модель, а рассматривается как внешний каркас, облегчающий администрирование.

**2.** ***Протоколы аутентификации с симметричными алгоритмами шифрования (В чем заключается идея строгой аутентификации? Приведите и поясните следующие методы: односторонняя аутентификация, основанная на метках времени; односторонняя аутентификация, основанная на использовании случайных чисел).*Ответ:** Идея строгой аутентификации заключается в следующем**: Проверяемая сторона доказывает свою подлинность проверяющей стороне**, демонстрируя знание некоторого секрета. Доказательство знания секрета осуществляется с помощью **последовательности запросов** и ответов с использованием **криптографических методов.** Может быть одна/двух и трёхсторонней.

Для работы протоколов аутентификации, построенных на основе симметричных алгоритмов шифрования, необходимо, чтобы проверяющий и доказывающий **с самого начала имели один и тот же секретный ключ.** Для закрытых систем с небольшим количеством пользователей каждая пара пользователей может заранее разделить его между собой. В больших распределённых системах часто используются протоколы аутентификации с участием **доверенного сервера**, с которым каждая сторона разделяет знание ключа. В больших распределённых системах часто используются протоколы аутентификации с участием доверенного сервера, с которым каждая сторона разделяет знание ключа. (ISO/IEC9798–2)

**Односторонняя аутентификация, основанная на метках времени: *A*→*B*:*EK*(*tA,B*)**

После получения и расшифровывания данного сообщения участник *В* убеждается в том, что метка *tA* времени действительна и идентификатор *В*, указанный в сообщении , совпадает с его собственным. Предотвращение повторной передачи данного сообщения основывается на том, что без знания ключа невозможно оценить метку времени *tA* и идентификатор *В*.

**Односторонняя аутентификация, основанная на использовании случайных чисел: *A* ← *B*:*rB*  *A*→*B*:*EK*(*rB,B*)**

Участник *В* отправляет участнику *А* случайное число *rB* . Участник *А* шифрует сообщение, состоящее из полученного числа *rB* и идентификатора *В*, и отправляет зашифрованное сообщение участнику *В*. Участник *В* расшифровывает полученное сообщение и сравнивает полученную информацию с отправленной.