Лекция 12
РИС, III курс, ИСиТ

Защита (безопасность)

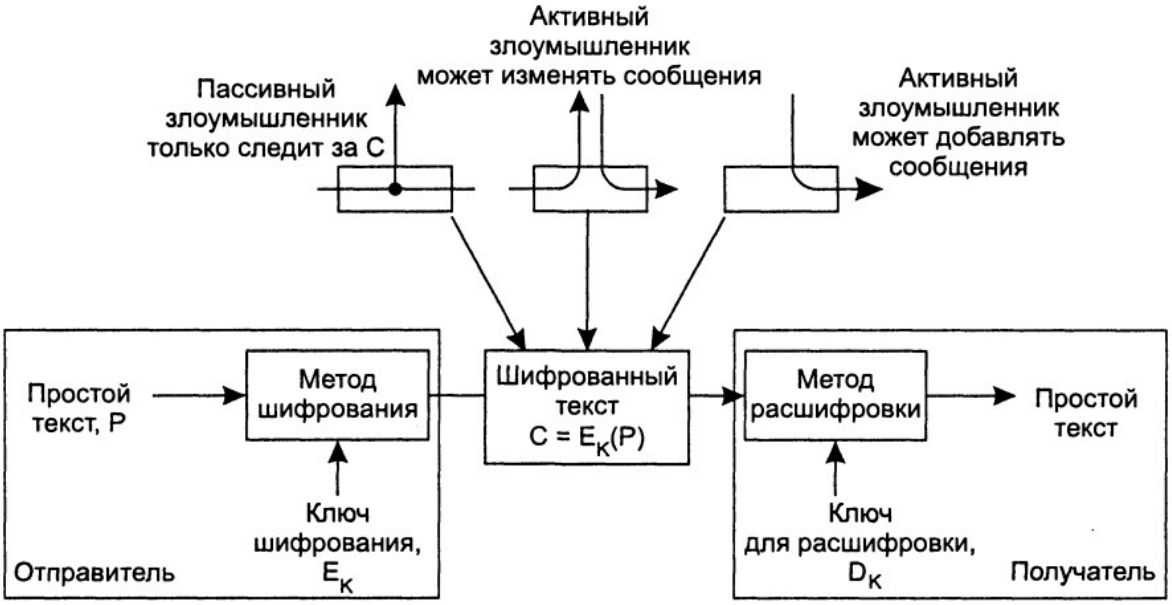
1. **Безопасность в распределенных системах:** 1) защищенный канал между узлами системы (идентификация, целостность сообщений, конфиденциальность); 2) авторизация (авторизированный доступ процессов к ресурсам).
2. **Конфиденциальность распределенной системы:** доступ к данным системы ограничен кругом доверенных лиц.
3. **Целостность:** изменения в систему могут внести только авторизованные на выполнение этих изменений лица или процессы. Незаконные изменения должны обнаруживаться и исправляться.
4. **Угрозы защиты (security threads):**
   - перехват;
   - прерывание;
   - модификация;
   - подделка.
5. **Перехват:** неавторизованный агент получает доступ к данным. Пример: прослушиваемый канал связи.
6. **Прерывание:** злонамеренное повреждение или уничтожение файла данных; действия, приводящие к отказу службы.
7. **Модификация:** неавторизированное изменение данных или фальсификацию служб.
8. **Подделка:** создание данных или осуществление действия от лица распределенной системы, невозможной при нормальной работе системы.
9. **Правила защиты системы:** полное описание разрешенных и запрещенных действий для компонентов системы (пользователи, службы, данные, …).
10. **Механизмы защиты:**
    - шифрование;
    - аутентификация;
    - авторизация;
    - аудит.

11. **Шифрование:** преобразование данных в вид недоступный для понимания злоумышленника; шифрование – средство реализации конфиденциальности и целостности.
12. **Аутентификация:** механизм идентификации подлинности компонента системы (пользователя, клиента, процесса, …).
13. **Авторизация:** механизм разграничения прав доступа, аутентифицированных компонентов системы, к ресурсам системы.
14. **Аудит:** механизм контроля, позволяющий выяснить последовательность действий всех активных компонент системы.
15. **Разработка системы защиты:** 1) защита данных (данные защищены независимо от их применения); 2) контроль доступа к данным (доступ к данным возможен только четко определенным компонентам системы); 3) защита приложения от неавторизированного доступа.
16. **Многоуровневая организация механизмов защиты**

17. **Доверенная вычислительная база (Trusted Computing Base, TCB):** набор всех механизмов системы, необходимый для реализации правил защиты. TCB распределенной системы может включать в себя механизмы безопасности локальных операционных систем, серверов СУБД, серверов приложений, служб, … Например: файловый сервер в распределенной системе, сервер печати, IIS-сервер, …
18. **Криптография:** наука о методах обеспечения конфиденциальности данных (невозможности прочтения),

целостности данных (невозможности изменения), аутентификации данных (проверка авторства)

19. **Шифрование данных:** обеспечение конфиденциальности.



20. **Симметричные криптосистемы:** для шифрования и расшифровки применяется один и тот же ключ. DES (56 бит),2DES (112 бит), 3DES (168 бит)
21. **Ассиметричные криптосистемы:** для шифрования и расшифровки применяется разные ключи, но вместе эти ключи образуют уникальную пару. Один из ключей – отрытый, другой – закрытый (секретный). Алгоритм Диффи-Хеллмана. RSA. PGP Цифровая подпись.
22. **Хэш-функция:** механизм преобразующий битовую последовательность произвольной длины в битовую последовательность фиксированной длины. Хэш-функция – односторонняя функция(необратимая функция). По результату хэш-функции не должен просто вычисляться аргумент. Применяются для цифровой подписи. MD5