Тема 4

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Занятие 3

Программно-аппаратная защита информации.

Учебные вопросы.

1. Программно-аппаратная защита информации от локального несанкционированного доступа.
2. Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях.

1-й учебный вопрос

Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях

Элементами аппаратного обеспечения могут быть:

- магнитные диски, не требующие установки на компьютере пользователя КС никаких дополнительных аппаратных средств, но наиболее уязвимые с точки зрения копирования хранящейся на них ключевой информации;
- элементы Touch Memory (аналогичные изделия других производителей именуются iButton), включающие в себя энергонезависимую память в виде постоянного запоминающего устройства (ПЗУ) с уникальным для каждого изделия серийным номером и (в более дорогих вариантах)

- оперативного запоминающего устройства (ОЗУ) для хранения идентифицирующей пользователя информации, а также встроенный элемент питания со сроком службы до 10 лет (элемент Touch Memory напоминает миниатюрную батарейку диаметром 16 мм и толщиной 3...6 мм, он имеет один сигнальный контакт и один контакт заземления, а для контакта элемента с устройством чтения достаточно простого касания);

- пластиковые карты с магнитной полосой, на которой помимо ключевой информации могут размещаться и дополнительные реквизиты пользователя (его фамилия, имя, отчество, фотография, название организации и ее подразделения и т.п.); подобные карты наиболее дешевы, но и наименее защищены от копирования и подделки;

- маркеры eToken (USB-брелки), представляющие собой подключаемое к USB-порту компьютера устройство, которое включает в себя аналогичную смарткарте микросхему с процессором и защищенной от несанкционированного доступа памятью (в отличие от пластиковых карт не требуется установка устройства их чтения с кабелем для подключения этого устройства к компьютеру).

- карты со штрихкодом, покрытым непрозрачным составом, считывание информации с которых происходит в инфракрасных лучах, эти карты также относительно дешевы, но уязвимы для подделки;
- смарткарты, носителем ключевой информации в которых является специальная бескорпусная микросхема, включающая в себя только память для хранения ключевой информации (простые смарткарты) или микропроцессор (интеллектуальные карты), позволяющий реализовывать достаточно сложные процедуры аутентификации.

• маркеры eToken (USB-брелки), представляющие собой подключаемое к USB-порту компьютера устройство, которое включает в себя аналогичную смарт-карте микросхему с процессором и защищенной от несанкционированного доступа памятью (в отличие от пластиковых карт не требуется установка устройства их чтения с кабелем для подключения этого устройства к компьютеру).

Порядок работы программ после включения питания компьютера и до загрузки операционной системы:

- программа самопроверки устройств компьютера POST (Power On — Self Test);
- программа BIOS Setup (может быть вызвана пользователем во время выполнения программы POST, обычно для этого необходимо нажать клавишу Delete);
- программы BIOS;
- программы расширения BIOS (BIOS Extension), если соответствующая плата установлена на компьютере;

- программа начальной загрузки, которая размещается в первом секторе нулевой головки нулевого цилиндра жесткого диска компьютера (Master Boot Record, MBR) и в функции которой входят определение активного раздела жесткого диска и вызов программы загрузки операционной системы;
- программа загрузки операционной системы, которая размещается в первом секторе активного раздела жесткого диска, загрузочного компакт-диска или загрузочной дискеты;
- оболочка операционной системы.

Определим модель (возможности) нарушителя:

- установка системы защиты производится в его отсутствие;
- нарушитель не может вскрыть системный блок компьютера;
- нарушитель не может перезаписать информацию в ПЗУ BIOS при работающем компьютере;
- нарушитель не имеет пароля установки системы защиты;
- нарушитель не имеет пароля пользователя КС;
- нарушитель не имеет копии ключевой информации пользователя, хранящейся в элементе аппаратного обеспечения (например, в элементе Touch Memory).

После установки платы расширения BIOS выполняется процедура установки системы защиты информации:

- после включения питания компьютера программа, записанная на плате расширения BIOS, выдает запрос на ввод пароля;
- после ввода пароля установки PS (как правило, администратором системы) происходят загрузка операционной системы и запуск собственно программы установки (проверочные функции системы защиты при этом отключаются);

- по запросу программы установки вводятся пароль пользователя P, ключевая информация с элемента аппаратного обеспечения (например, серийный номер элемента Touch Memory) KI и имена подлежащих проверке системных и пользовательских файлов F_L, F_2, ..., ¥,,;
- для каждого указанного файла вычисляется и сохраняется проверочная информация в виде E,(H(PS, P, KI, F,)), где E — функция шифрования; *к* — ключ шифрования; H — функция хеширования.

Процедура входа пользователя в КС при использовании данной системы защиты:

- после включения питания компьютера программа на плате расширения BIOS запрашивает пароль пользователя и просит установить элемент аппаратного обеспечения с его ключевой информацией;
- осуществляется проверка целостности выбранных при установке системы защиты файлов путем вычисления хешзначения для них по приведенному выше правилу и сравнения с расшифрованными эталонными хешзначениями;

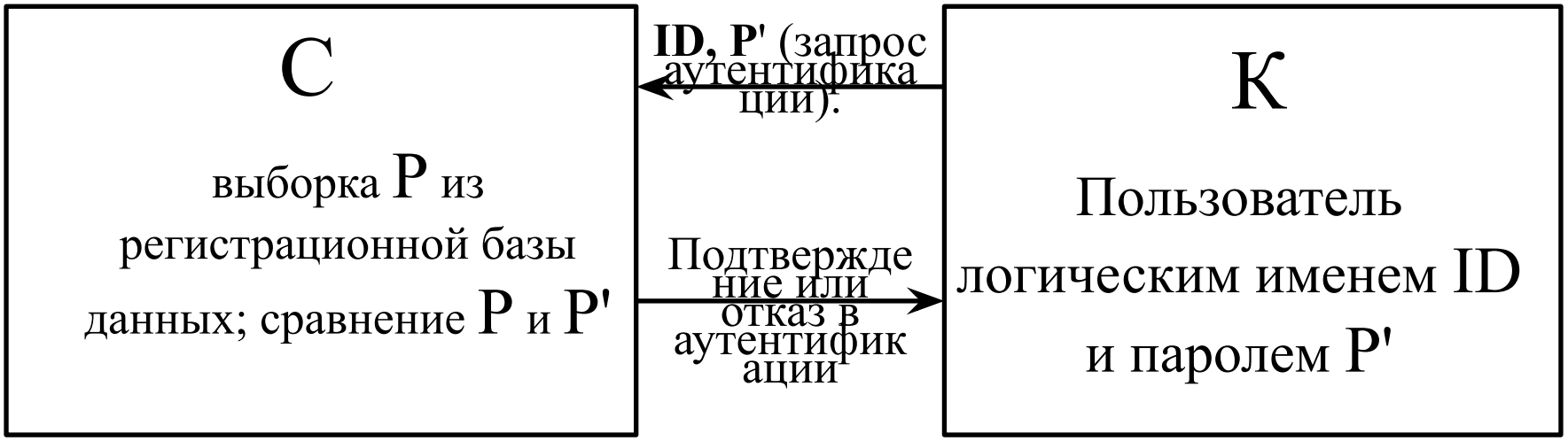
- в зависимости от результатов проверки выполняется либо загрузка операционной системы, либо запрос на повторный ввод пароля.

2-й учебный вопрос

Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях

Протоколы - это стандарты, определяющие формы представления и способы пересылки сообщений, процедуры их интерпретации, правила совместной работы различного оборудования в сетях.

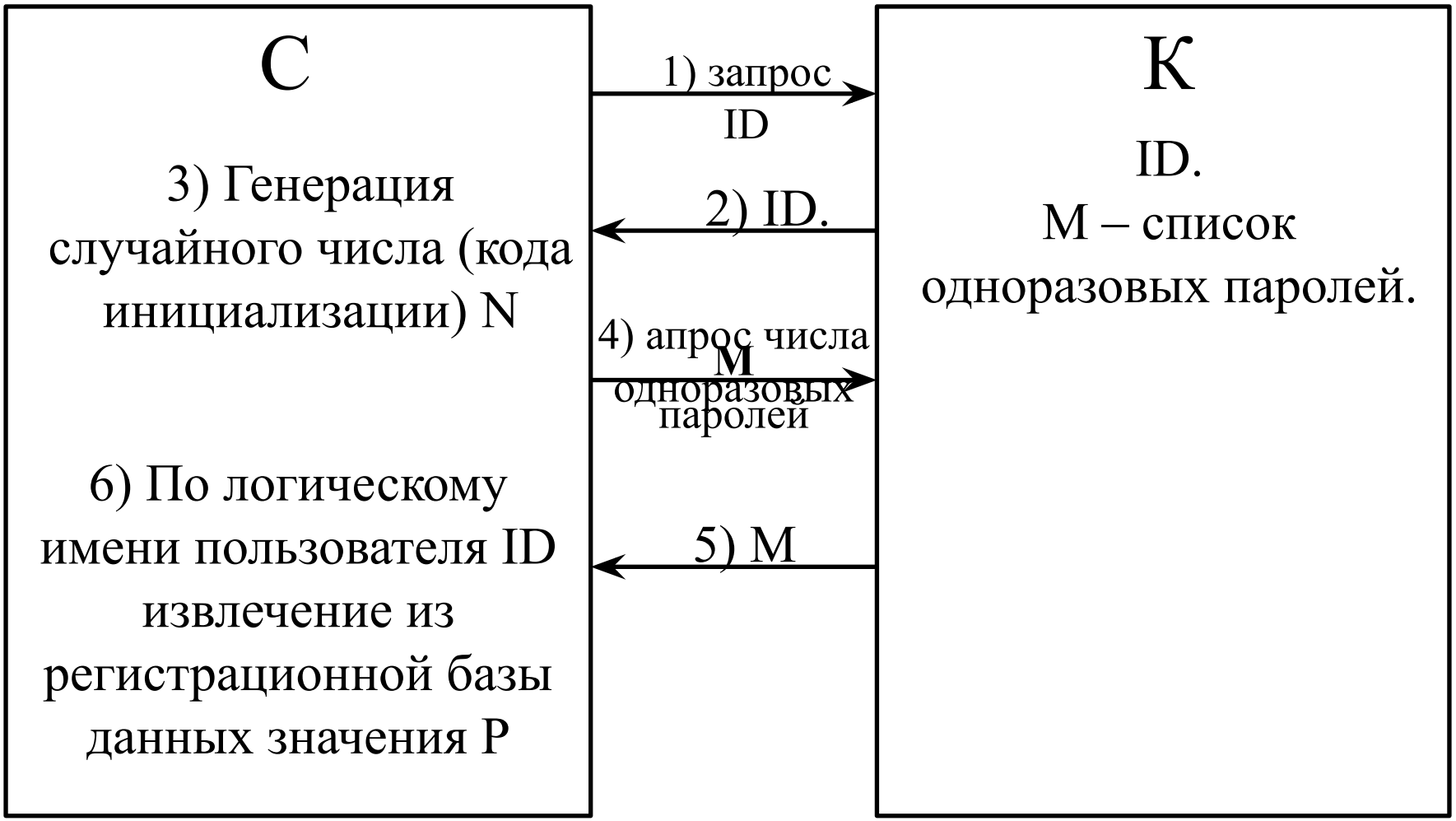
Протокол PAP (Password Authentication Protocol)



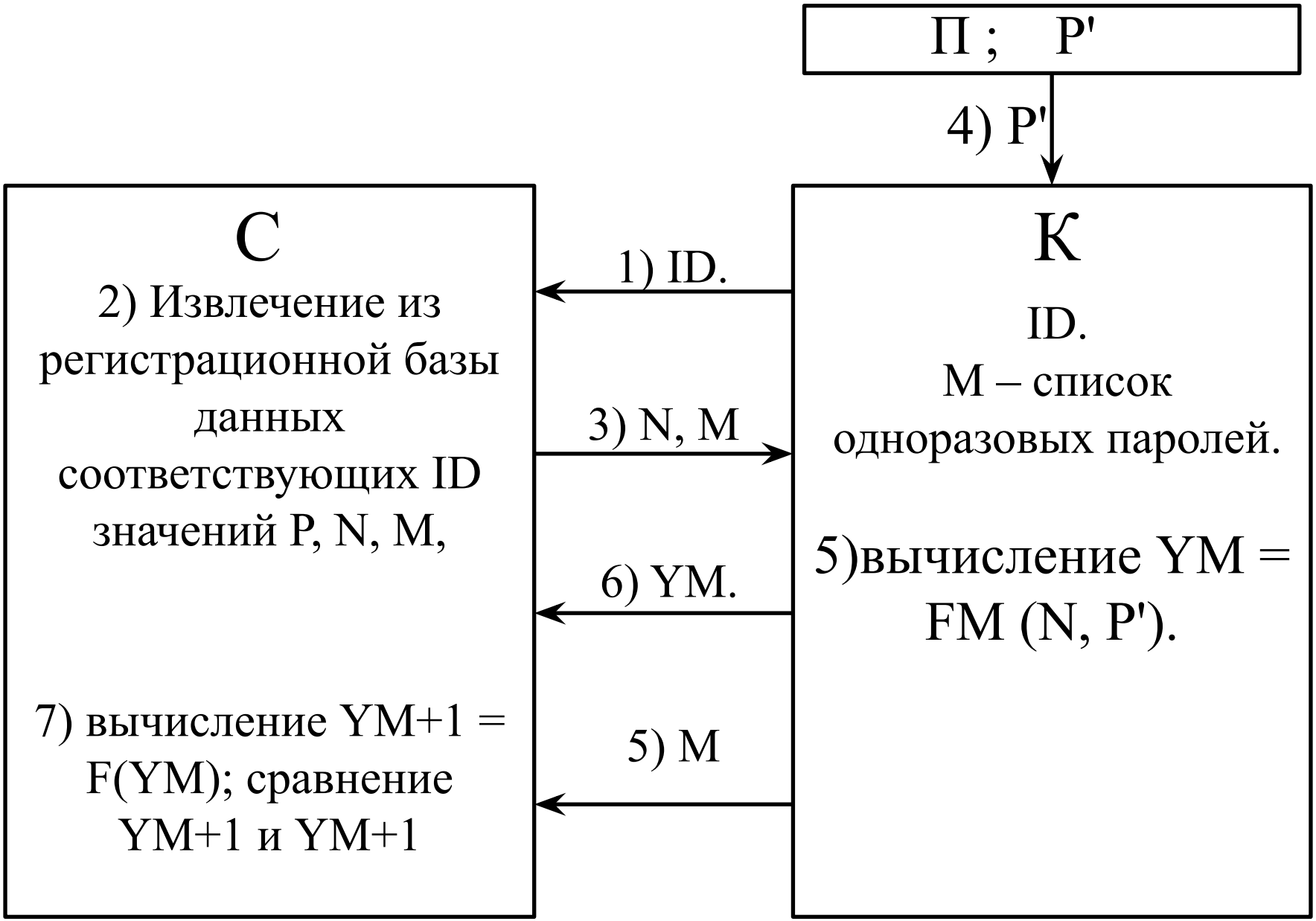
Протокол S/Key состоит из двух частей:

- генерации списка одноразовых паролей (парольной инициализации);
- и собственно аутентификации.

Парольная инициализации протокола S/Key



Аутентификация по протоколу S/Key.



протокол CHAP (Challenge Handshake Authentication Protocol)

1) С: генерация случайного числа N.
2) С ➡ К: идентификатор сервера IDS, N и его длина в байтах (вызов).
3) П ➡ К: P'.
4) К: вычисление хеш-значения D' = H(IDS, N, P').
5) К ➡ С: ID, D' (отклик).
6) С: извлечение из регистрационной базы данных соответствующего ID значения P; вычисление хеш-значения D = H(IDS, N, P); сравнение D' и D.
7) С ➡ К: если значения совпадают, то подтверждение аутентификации, в противном случае — отказ в аутентификации и разрыв соединения.