Тема 4

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Занятие 2

Способы несанкционированного доступа к информации и понятие аутентификации.

Учебные вопросы.

1. Способы несанкционированного доступа к информации в компьютерных системах и защиты от него.
2. Аутентификация пользователей на основе паролей и модели «рукопожатия».
3. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью

В руководящих документах по защите информации Республики Казахстан. приведены следующие основные способы несанкционированного доступа к информации в КС:

- непосредственное обращение к объекту с конфиденциальной информацией (например, с помощью управляемой пользователем программы, читающей данные из файла или записывающей их в него);
- создание программных и технических средств, выполняющих обращение к объекту в обход средств защиты (например, с использованием случайно или намеренно оставленных разработчиком этих средств, так называемых люков);

- модификация средств защиты для осуществления несанкционированного доступа (например, внедрение программных закладок);
- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих структуру и функции этих средств для осуществления несанкционированного доступа (например, путем загрузки на компьютере иной, незащищенной операционной системы).

Можно выделить следующие уровни возможностей нарушителя, предоставляемые ему штатными средствами КС (каждый сле

дующий уровень включает в себя предыдущий):

1. Запуск программ из фиксированного набора (например, подготовка документов или получение почтовых сообщений).

2. Создание и запуск собственных программ (возможности опытного пользователя или пользователя с полномочиями отладки программ).

3. Управление функционированием КС — воздействие на ее базовое программное обеспечение, состав и конфигурацию КС (например, внедрение программной закладки);

4. Весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт средств КС, вплоть до включения в состав КС собственных СВТ с новыми функциями.

Вспомогательные способы несанкционированного доступа к информации в КС:

- ручной или программный подбор паролей путем их полного перебора или при помощи специального словаря (взлом КС);
- подключение к КС в момент кратковременного прекращения работы легального пользователя, работающего в интерактивном режиме и не заблокировавшего свой терминал;

- подключение к линии связи и перехват доступа к КС после отправки пакета завершения сеанса легального пользователя, работающего в удаленном режиме;
- выдача себя за легального пользователя с применением похищенной у него или полученной обманным путем (с помощью так называемой социальной инженерии) идентифицирующей информации — «маскарад»;

- создание условий для связи по компьютерной сети легального пользователя с терминалом нарушителя, выдающего себя за легального объекта КС (например, одного из ее серверов), — «мистификация»;
- создание условий для возникновения в работе КС сбоев, которые могут повлечь за собой отключение средств защиты информации или нарушение правил политики безопасности;
- тщательное изучение подсистемы защиты КС и используемой в ней политики безопасности, выявление ошибочных участков в программных средствах защиты информации в КС, введение программных закладок, разрешающих доступ нарушителю.

К основным функциям СРД относятся:

- реализация правил разграничения доступа субъектов и их процессов к информации и устройствам создания ее твердых копий;
- изоляция процессов, выполняемых в интересах субъекта доступа, от других субъектов;
- управление потоками информации в целях предотвращения ее записи на носители несоответствующего уровня конфиденциальности;

- реализация правил обмена информацией между субъектами в компьютерных сетях.

К функциям обеспечивающих средств для СРД относятся:

- идентификация и аутентификация субъектов и поддержание привязки субъекта к процессу, выполняемому для него;
- регистрация действий субъекта и активизированного им процесса;
- исключение и включение новых субъектов и объектов доступа, изменение полномочий субъектов;

- реакция на попытки несанкционированного доступа (сигнализация, блокировка, восстановление объекта после несанкционированного доступа);
- учет выходных печатных форм в КС;
- контроль целостности программной и информационной части СРД и обеспечивающих ее средств.

Итак, основными способами защиты от несанкционированного доступа к информации в компьютерных системах являются аутентификация, ***авторизация*** (определение прав доступа субъекта к объекту с конфиденциальной информацией) и шифрование информации.

Под ***протоколом*** в общем случае последовательность однозначно и точно определенных действий, выполняемых двумя или более сторонами для достижения желаемого результата за конечное время.

Рассмотрим протокол идентификации пользователя при его входе в КС (под «С» понимается система, под «|П» — пользователь):

- С: запрос имени, под которым пользователь зарегистрирован в базе данных учетных записей КС (логического имени пользователя или так называемого логина).
- П: ввод логического имени (ID).
- С: проверка наличия ID в регистрационной базе данных. Если пользователь с таким именем зарегистрирован, то запрос его идентифицирующей информации, в противном случае — возврат к п. 1.
- П: ввод идентифицирующей информации (Р).
- С: проверка совпадения Р с идентифицирующей информацией для пользователя ID в регистрационной базе данных. Если совпадение есть, то допуск пользователя к работе в КС, в противном случае — возврат к п. 3.

структура учетной записи

- относительный номер учетной записи R1D,;
- логическое имя пользователя ID,;
- полное имя пользователя и его должность в организации D;
- случайное значение $S_{(}$, генерируемое при регистрации пользователя в КС (используется для предотвращения возможности получения одним пользователем полномочий другого пользователя при случайном совпадении идентифицирующей информации);
- идентифицирующая пользователя информация P,;
- информация о правах пользователя в КС R,.

К ***первой группе*** относятся способы аутентификации, основанные на том, что пользователь знает некоторую подтверждающую его подлинность информацию (парольная аутентификация и аутентификация на основе модели «рукопожатия»).

Ко ***второй группе*** относятся способы аутентификации, основанные на том, что пользователь имеет некоторый материальный объект, который может подтвердить его подлинность (например, пластиковую карту с идентифицирующей пользователя информацией).

К ***третьей группе*** относятся способы аутентификации, основанные на таких данных, которые позволяют однозначно считать, что пользователь и есть тот самый субъект, за которого себя выдает (биометрические данные, особенности клавиатурного почерка и росписи мышью и т.п.).

2-й учебный вопрос

Аутентификация пользователей на основе паролей и модели «рукопожатия».

при использовании парольной аутентификации должны быть:

- максимальный срок действия пароля (любой секрет не может сохраняться в тайне вечно);
- несовпадение пароля с логическим именем пользователя, под которым он зарегистрирован в КС;
- неповторяемость паролей одного пользователя.

Правила противодействия системы попыткам подбора паролей

- ограничение числа попыток входа в систему;
- скрытие логического имени последнего работавшего пользователя (знание логического имени может помочь нарушителю подобрать или угадать его пароль);
- учет всех попыток (успешных и неудачных) входа в систему в журнале аудита.

Реакцией системы на неудачную попытку входа пользователя могут быть:

- блокировка учетной записи, под которой осуществляется попытка входа, при превышении максимально возможного числа попыток (на заданное время или до ручного снятия блокировки администратором);
- нарастающее увеличение временной задержки перед предоставлением пользователю следующей попытки входа.

При первоначальном вводе или смене пароля пользователя обычно применяются два классических правила:

- символы вводимого пароля не отображаются на экране (это же правило, применяется и для ввода пользователем пароля при его входе в систему);
- для подтверждения правильности ввода пароля (с учетом первого правила) этот ввод повторяется дважды.

Недостатки схемы одноразовых паролей:

- организация защищенного хранения длинного списка паролей (либо его запоминание, что маловероятно);
- неясность с номером следующего пароля, если после ввода предыдущего пароля из списка вход пользователя в систему не был осуществлен из-за сбоя в работе КС.

Преимущества аутентификации на основе модели «рукопожатия» перед парольной аутентификацией:

- между пользователем и системой не передается никакой конфиденциальной информации, которую нужно сохранять в тайне;
- каждый следующий сеанс входа пользователя в систему отличен от предыдущего, поэтому даже длительное наблюдение за этими сеансами ничего не даст нарушителю.

Аутентификацию пользователей на основе модели «рукопожатия».

В соответствии с этой моделью пользователь П и система С і согласовывают при регистрации пользователя в КС функцию *f*, известную только им. Протокол аутентификации пользователя в этом случае выглядит следующим образом:

1) С: генерация случайного значения x; вычисление $y = f(x)$; вывод x.

2) П: вычисление $y' = f'(x)$; ввод y'.

3) С: если y и y' совпадают, то пользователь допускается к работе в системе, иначе попытка входа в систему отклоняется.

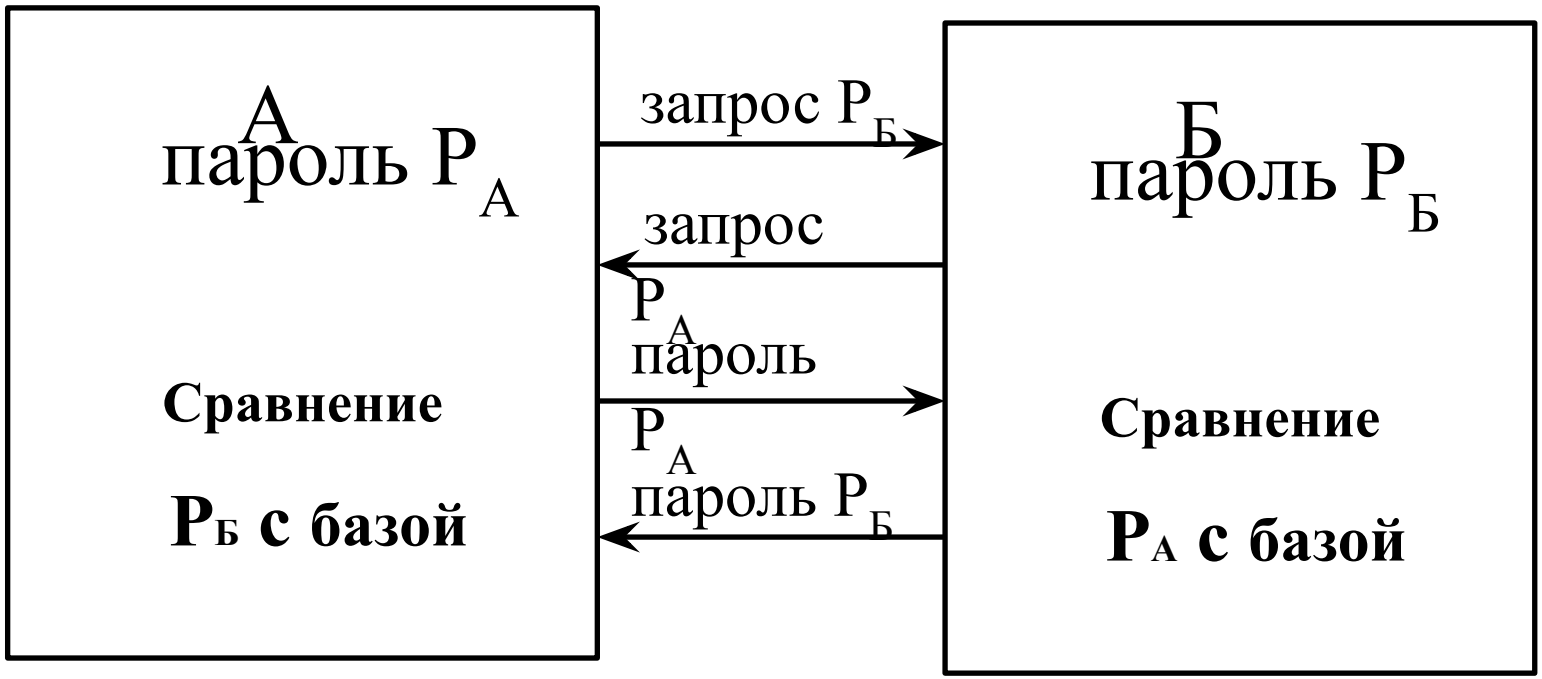
⇨ Парольная аутентификация совершенно неприменима в случае взаимного подтверждения подлинности пользователей компьютерной сети. Действительно, пусть А и Б обозначают двух пользователей сети, имеющих соответственно пароли $P_А$ и $P_Б$. Тогда протокол взаимной аутентификации А и Б мог бы выглядеть следующим образом:

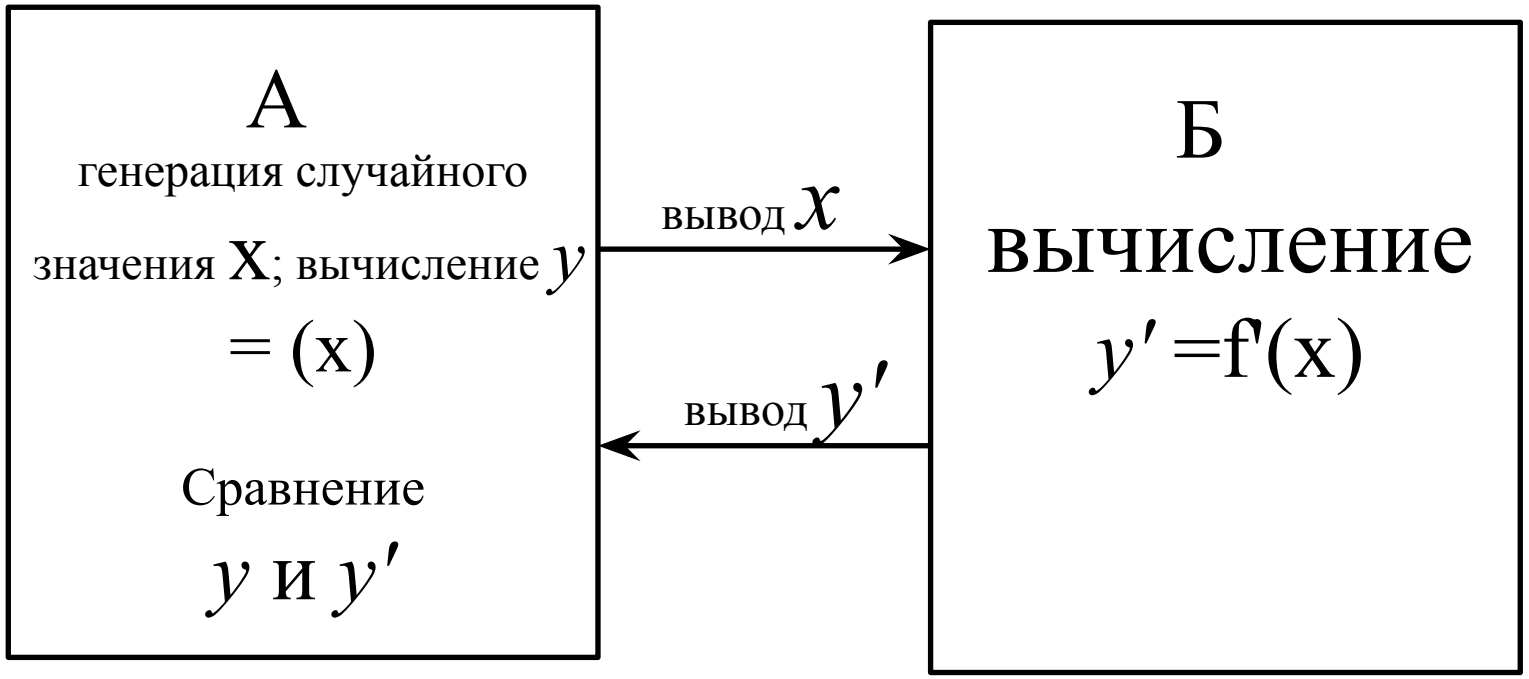
А⇨Б: А, запрос $P_Б$

Б ⇨А: Б, запрос $P_А$.

А ⇨ Б: А, $P_А$.

Б ⇨А: Б, $P_Б$.


А
пароль $P_А$
Сравнение
$P_Б$ с базой
запрос $P_Б$
запрос $P_А$
пароль $P_А$
пароль $P_Б$
Б
пароль $P_Б$
Сравнение
$P_А$ с базой


А
генерация случайного
значения x; вычисление y
= (x)
Сравнение
y и y′
вывод x
вывод y′
Б
вычисление
y′ =f′(x)

Модель «рукопожатия» вполне приемлема для взаимной аутентификации:

А: выбор значения x; вычисление $y = f(x)$.

А $\Longrightarrow$ Б: А, x.

Б: вычисление $y' = f(\text{x})$.

Б $\Longrightarrow$ А: Б, y'.

А: если y и y' совпадают, то А может доверять Б.

3-й учебный вопрос

Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью.

К основным биометрическим характеристикам пользователей КС, которые могут применяться при их аутентификации, относятся:

- отпечатки пальцев;
- геометрическая форма руки;
- узор радужной оболочки глаза;

- рисунок сетчатки глаза;
- геометрическая форма и размеры лица;
- тембр голоса;
- геометрическая форма и размеры уха и др.

Основные достоинства аутентификации пользователей по их биометрическим характеристикам:

- трудность фальсификации этих признаков;
- высокая достоверность аутентификации из-за уникальности таких признаков;
- неотделимость биометрических признаков от личности пользователя.

Процедура настройки на характеристики регистрируемого в КС пользователя:

- Выбор пользователем ключевой фразы (ее символы должны быть равномерно разнесены по клавиатуре).
- Набор ключевой фразы несколько раз.
- Исключение грубых ошибок (по специальному алгоритму).
- Расчет и сохранение оценок математических ожиданий, дисперсий и числа наблюдений для временных интервалов между наборами каждой пары соседних символов ключевой фразы.

Первый вариант процедуры аутентификации:

- набор ключевой фразы пользователем несколько раз;
- исключение грубых ошибок (по специальному алгоритму);
- расчет оценок математических ожиданий и дисперсий для временных интервалов между нажатиями каждой пары соседних символов ключевой фразы;
- решение задачи проверки гипотезы о равенстве дисперсий двух нормальных генеральных совокупностей для каждой пары соседних символов ключевой фразы (по специальному алгоритму);

- если дисперсии равны, то решение задачи проверки гипотезы о равенстве центров распределения двух нормальных генеральных совокупностей при неизвестной дисперсии для каждой пары соседних символов ключевой фразы (по специальному алгоритму);
- вычисление вероятности подлинности пользователя как отношения числа сочетаний соседних клавиш, для которых подтверждены гипотезы к общему числу сочетаний соседних символов ключевой фразы;
- сравнение полученной оценки вероятности с выбранным пороговым значением для принятия решения о допуске пользователя.

Второй вариант процедуры аутентификации:

- набор ключевой фразы один раз;
- решение задачи проверки гипотезы о равенстве дисперсий двух нормальных генеральных совокупностей для временных интервалов между нажатиями соседних символов ключевой фразы;
- если дисперсии равны, то исключение временных интервалов между нажатиями соседних символов ключевой фразы, которые существенно отличаются от эталонных (полученных при настройке);

- вычисление вероятности подлинности пользователя как отношения числа оставшихся интервалов к общему числу интервалов в ключевой фразе;
- сравнение полученной оценки вероятности с выбранным пороговым значением для принятия решения о допуске пользователя.

Процедура настройки при наборе псевдослучайного текста:

- генерация и вывод пользователю текста из фиксированного множества слов, символы которых максимально разбросаны по клавиатуре;
- набор текста пользователем;
- фиксация и сохранение значений x_0, которые затем используются для расчета статистических характеристик клавиатурного почерка.

Процедура настройки на характеристики пользователя может состоять из следующих этапов:

- ввод нескольких эталонных росписей;
- для каждой росписи получение числа точек в ней и длины ее линии, определение числа и местоположения разрывов в линии росписи;
- для каждой линии росписи выполнение сглаживания, получение числа и местоположения замкнутых контуров;
- расчет среднего значения полученных характеристик росписи и их допустимых отклонений.

Процедура аутентификации состоит из следующих этапов:

- ввод росписи;
- расчет числа точек и длины линии росписи;
- получение числа и местоположения разрывов в линии росписи;
- сглаживание линии росписи;
- сравнение полученных характеристик росписи с эталонными;
- принятие решения о допуске пользователя к работе в КС.