Экзаменационные билеты по курсу

«Методы и средства защиты информации»

(Кафедра ЭФИС)

1. Взаимно однозначное отображение.

Соответствие, при котором каждому из элементов множества X сопоставляется единственный элемент из множества Y, называется отображением.

Образ при отображении f – множество всех элементов f(x):

$$f(x) = \{f(x) | x \in X\}, f(x) \in Y$$

Прообраз элемента $y \in Y$:

$$f^{-1}(y) = \{x \in X | f(x) = y\}$$

Отображение f: X→Y называется инъективным, если для ∀y∈Y функция y=f(x) является образом единственного x∈X.

$$\forall x_1 \in X, \forall x_2 \in X: f(x_1) = f(x_2) \rightarrow x_1 = x_2$$

Отображение f: X→Y называется сюръективным, если ∀y∈Y является образом какого-либо x∈X (отображение множества X на множество Y).

$$\forall y \in Y, \exists x \in X: f(x) = y$$

Отображение f: X→Y называется биективным, если оно является инъективным и сюръективным. Биективное отображение – **взаимно однозначное отображение** (равномощное отображение).

2. Свойства бинарных операций.

Свойства бинарных операций:

1) ассоциативность:
   для ∀a, b, c ∈ X: (a * b) * c = a * (b * c);
2) коммуникативность:
   для ∀a, b ∈ X: a + b = b + a (перестановки);
3) дистрибутивность слева:
   для ∀a, b, c ∈ X: a * (b + c) = a * b + a * c;
4) дистрибутивность справа:
   для ∀a, b, c ∈ X: (a + b) * c = a * c + b * c.

3. Определение алгебраической группы.

Алгебраическая группа – множество G с определённой на нём бинарной операцией *, удовлетворяющей следующим аксиомам:

1) операция * ассоциативна: для $\forall a, b, c \in G \rightarrow (a * b) * c = a * (b * c)$;
2) определен единичный элемент: $\exists e \in G$ такой, что $a * (a^{-1}) = e$;
3) для каждого элемента есть обратный: для $\forall a \in G \; \exists a^{-1}$ такой, что $(a^{-1})^{-1} = a$.

Группа G, обладающая конечным числом элементов, называется конечной. При этом число элементов группы называется порядком группы.

Группа G называется абелевой (коммутативной), если для $\forall a, b \in G$ справедливо равенство $a*b = b*a$.

Группа G с мультипликативной операцией называется циклической, если она порождена одним элементом, то есть в ней имеется такой элемент a (образующий), что любой другой элемент b представим в виде $b = a^n$, где $n \in Z$.

4. Обратный элемент, методы его определения.

Обратным (a^{-1}) к числу a по модулю m называется такое число b, что:

$$a \cdot b \equiv 1 (mod\ m)$$

Обратный элемент по модулю m существует только для тех элементов, которые взаимно просты с модулем m. Взаимно простыми называются числа, не имеющие никаких общих делителей, кроме числа 1.

Пусть M – множество с определенной на нем бинарной операцией *, $x \in M$ – произвольный элемент множества M, $e \in M$ – единичный элемент множества M. Тогда:

1) $x * y = e$, $y \in M$, то y – обратный элемент справа для элемента x;
2) $y * x = e$, $y \in M$, то y – обратный элемент слева для элемента x;
3) если $x * y = e = y * x$, то y – просто обратный элемент для x (и справа, и слева).

Методы определения обратного числа:

- (расширенный) алгоритм Евклида;
- функция Эйлера;
- полный перебор.

5. Поле, основные операции в бинарном поле GF(2).

Полем называется множество F с операциями сложения и умножения, которые удовлетворяют ассоциативным, коммуникативным и дистрибутивным законам. В поле имеются как аддитивные (0), так и мультипликативные (1) единицы, и любой элемент поля имеет обратный.

Число элементов поля F называется порядком k поля F.

Поле W такое, что $F \in W$, называется расширением поля F.

Поля бывают бесконечными и конечными. Конечные поля называются полями Галуа GF(m). Простейшее конечное поле – бинарное поле GF(2) с операциями сложения и умножения по модулю 2.

Отношение конгруэнтности (сравнимости) по модулю m на расширенном множестве натуральных чисел N+ (включая 0), является отношением эквивалентности и разбивает множество N+ на смежные классы (эквивалентности) по модулю m.

Множество смежных классов по модулю m с операциями сложения и умножения по модулю m на множестве обозначений классов является полем, если m = p, где p – простое число. Единицами по сложению и умножению этого поля GF(p) являются классы, содержащие числа 0 и 1 соответственно.

Поле классов конгруэнтности GF(p) целых чисел по модулю простого числа p называется простым полем.

Если многократное сложение единицы (1) не позволяет получить ноль (0), то поле называется полем характеристики ноль, в этом случае он содержит копию поля рациональных чисел. В противном случае, если существует такое простое число p, что p-кратное сложение единицы (1) дает 0, то p – характеристика поля.

6. Полная и приведенная система вычетов, функция Эйлера.

Полной системой вычетов по модулю **m** называют совокупность **m** целых чисел, содержащую по одному представителю из каждого класса вычетов по модулю **m**. Числа $\mathbf{x_1, \ldots, x_m}$ образуют полную систему вычетов по модулю **m** тогда, когда они попарно не сравнимы по модулю **m** (их остатки от деления на m отличны).

Если два целых числа **a** и **b** имеют одинаковый остаток от деления на **m**, то они называются сравнимыми по модулю **m**. Иначе они не сравнимы по модулю **m**.

Приведенной системой вычетов по модулю **m** называют подмножество полной системы вычетов, члены которого взаимно просты с **m**. Если **m** – простое число, то приведенную систему вычетов по модулю **m** составляют все числа от **1** до **m-1**.

Функция Эйлера **φ(m)** («фи») указывает число элементов в приведенной системе вычетов по модулю **m**. Иными словами, **φ(m)** – количество положительных целых чисел, меньших **m** и взаимно простых с **m** (для любого **m**, большего 1).

Если **n** – простое число, то **φ(n) = n - 1**.

Если **n = p * q**, где **p** и **q** – простые числа, то **φ(n) = (p - 1) * (q - 1)**.

7. Классификация алгоритмов в соответствии с их сложностью.

Теория сложности обеспечивает методологию анализа вычислительной сложности криптографических методов и алгоритмов. Сложность алгоритма определяется вычислительными мощностями, необходимыми для выполнения алгоритма.

Параметры сложности алгоритма:

- Временная сложность T, не зависит от реализации алгоритма.
- Пространственная сложность S (требования к памяти).

n – размер (длина) входных данных.

Нотация «O» – порядок величины вычислительной сложности.

Пример. Вычислительная сложность $n^2 + 7n + 12$ равна $O(n^2)$.

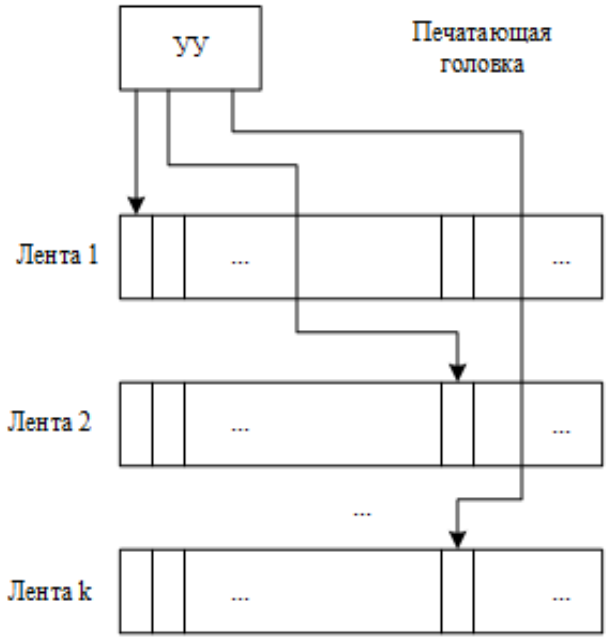
Классификация алгоритмов по временной и пространственной сложности:

- Алгоритмы с полиномиальным временем (сложность $O(n^k)$, k = const):
  - постоянный алгоритм (O не зависит от n, O(1));
  - линейный алгоритм (временная сложность O(n));
  - квадратичный (кубический и так далее) алгоритмы ($O(n^2)$).
- Экспоненциальные алгоритмы (сложность алгоритма $O(t^{f(n)})$, t>1, t = const, f(n) – некоторая полиномиальная функция):
  - Алгоритмы с суперполиномиальным временем (f(n) – функция, которая растет быстрее, чем постоянная, но медленнее, чем линейная функция).

С ростом n (размера входных данных) временная сложность алгоритмов может стать настолько большой, что повлияет на практическую реализуемость алгоритма.

8. Детерминированная машина Тьюринга.

Теория сложности рассматривает минимальное время и объем памяти, необходимые для решения самого трудного варианта проблемы на теоретическом компьютере, известном как машина Тьюринга. **Машина Тьюринга** – конечный автомат с бесконечной лентой памяти для чтения-записи и является реалистичной моделью вычислений.



Машина Тьюринга состоит из управляющего устройства (УУ) с конечным числам состояний, k лент и k головок.

УУ контролирует операции, выполняемые головками, считывающими информацию с лент или записывающими на ленту.

Каждая лента разделена на бесконечное количество ячеек.

Каждая головка в любой момент времени имеет доступ к своей ленте и способна перемещаться вдоль нее влево и вправо. Операция доступа головки к ленте называется тактом.

Количество тактов $T_м$, которые машина Тьюринга M должна выполнить при распознавании строки (исходных данных), называется временной сложностью.

Машина Тьюринга решает задачу, перемещая головку вдоль строки (исходные данные задачи), состоящей из конечного количества символов, расположенных последовательно, начиная с крайней левой ячейки.

Каждый символ занимает одну ячейку, оставшиеся ячейки ленты, что справа, – пустые. Сканирование начинается с крайней левой ячейки ленты, содержащей строку, когда машина находится в предписанном начальном состоянии.

Если машина начинает работу с начального состояния, последовательно выполняет такты, сканирует исходную строку и завершает работу, достигая заключительного состояния, то машина распознает исходные данные.

Класс P – класс языков, имеющих следующие характеристики.

Язык L принадлежит классу P, если существует машина Тьюринга M и полином p(n), такие что машина M распознает любое предложение $I \in L$ за время $T_M(n)$, где $T_M(n) \leq p(n)$ для всех неотрицательных целых чисел n, n – параметр, задающий длину предложения I.

В этом случае говорят, что язык L распознается за полиномиальное время.

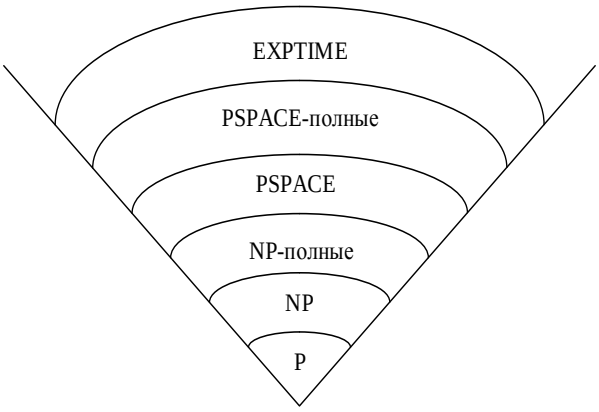
Все машины Тьюринга, распознающие язык L из класса P, называются детерминированными.

Результат работы **детерминированной машины Тьюринга** предопределен её начальными установками и исходными данными.

9. Классы сложности.

Классом сложности X называется множество предикатов P(x), вычислимых на машинах Тьюринга и использующих для вычисления O(f(n)) ресурса, где n – длина слова x. В качестве ресурсов берутся время вычисления (количество рабочих тактов машины Тьюринга) или рабочая зона (количество использованных ячеек на ленте во время работы). Все классы сложности находятся в иерархическом отношении: одни включают в себя другие.

Язык принадлежит классу, если распознается недетерминированной машиной Тьюринга (НДМТ) за полиномиальное время.



Класс NP состоит из всех задач, решаемых за полиномиальное время на НДМТ, способной параллельно выполнять неограниченное количество независимых вычислений. Класс NP-полных задач включает все самые трудные NP задачи.

Класс PSPACE состоит из задач, требующих полиномиальных объемов машинной памяти, но не обязательно решаемых за полиномиальное время.

Класс EXPTIME состоит из задач, решаемых за экспоненциальное время.

Таким образом, выбор наиболее сложных задач, для которых известно решение, и использование их в основе построения криптосистемы позволяет создавать практически устойчивые шифры, раскрытие которых в принципе возможно, но для этого потребуется столько времени, что эта процедура дешифрования потеряет практический смысл.

10. Равномерное распределение.

Наиболее часто в криптографии применяются случайные величины, имеющие равномерное распределение:

$$\mathrm{Prob}[\varepsilon = x_i] = \frac{1}{\#S}, i = \{1, \dots, \#S\}$$

Пусть S — множество неотрицательных чисел, состоящих из не более чем k бит (бинарных цифр). Выберем из множества S случайную точку x, придерживаясь равномерного распределения. Покажем, что вероятность извлечь число, состоящее из k бит, равна 1/2. Множество $S = \{0, ..., 2k - 1\}$ можно разбить на подмножества, которые не пересекаются: $S_1 = \{0, ..., 2^{k-1} - 1\}$ и $S_2 = \{2^{k-1}, 2^{k-1} + 1, ..., 2k - 1\}$, где множество S_2 состоит из всех k-разрядных чисел, $\#S_1 = \#S_2 = \#S/2$.

Применяя второе правило сложения вероятностей, получаем следующее:

$$Prob[x \in S_2] = Prob \bigcup_{i=2^{k-1}}^{2^k-1} \{x = i\} = \sum_{i=2^{k-1}}^{2^k-1} \{x = i\} = \sum_{i=2^{k-1}}^{2^k-1} \frac{1}{\#S} = \frac{\#S_2}{\#S} = \frac{1}{2}$$

11. Позначная модель открытого текста.

Учет частот k-грамм приводит к следующей модели открытого текста.

Пусть $\mathbf{P^{(k)}(A)}$ – массив, состоящий из приближений для вероятностей $\mathbf{p(b_1, ..., b_k)}$ появления k-грамм $\mathbf{b_1, ..., b_k}$ в открытом тексте, $\mathbf{k \in N}$, $\mathbf{A = (a_1 ,..., a_n)}$ – алфавит открытого текста, $\mathbf{b_i \in A}$, $\mathbf{i = 1, k}$.

Источник «открытого текста» генерирует последовательность $\mathbf{c_1, \ldots, c_{k+1}}$ знаков алфавита **A**, где k-грамма $\mathbf{c_1...c_k}$ появляется с вероятностью $\mathbf{p(c_1, ..., c_k) \in P^{(k)}(A)}$, следующая k-грамма $\mathbf{c_2...c_{k+1}}$ появляется с вероятностью $\mathbf{p(c_2, ..., c_{k+1}) \in P^{(k)}(A)}$. Эта модель – вероятностная модель k-го приближения.

Простейшая модель открытого текста – вероятностная модель 1-го приближения – представляет собой последовательность знаков $\mathbf{c_1, ..., c_L}$, в которой каждый знак $\mathbf{c_i}$ появляется с вероятностью $\mathbf{p(c_i) \in P^{(1)}(A)}$, независимо от других знаков. Будем называть эту модель позначной моделью открытого текста. Открытый текст $\mathbf{c_1...c_L}$ имеет вероятность:

$$p(c_1, \ldots, c_L) = \prod_{i=1}^{L} p(c_i)$$

Модели открытого текста более высоких приближений учитывают зависимость каждого знака от большего числа предыдущих знаков. Чем больше степень приближения, тем более "читаемыми" являются соответствующие модели.

12. Модулярная арифметика.

Соотношение $\mathbf{a \equiv b \pmod n}$ справедливо для целых значений **a**, **b** и $\mathbf{n \neq 0}$, если: $\mathbf{a = b + k * n}$ для некоторого целого **k**. Если $\mathbf{a \equiv b \pmod n}$, то **b** называют вычетом числа **a** по модулю **n**. Операцию нахождения вычета числа **a** по модулю **n** называют приведением числа по модулю. Набор целых чисел от **0** до $\mathbf{(n-1)}$ называют полным набором вычетов по модулю **n**.

Для любого целого $\mathbf{a>0}$ его вычет **r** по модулю **n** есть некоторое целое число в интервале от **0** до $\mathbf{(n-1)}$, определяемое из соотношения $\mathbf{r = a - k * n}$, где **k** – целое число.

Можно либо сначала приводить по модулю **n**, а затем выполнять операции, либо сначала выполнять операции, а затем уже приводить результат по модулю **n**.

$(a + b) \bmod n = [a \pmod n + b \pmod n] \bmod n$

$(a * b) \bmod n = [a \pmod n * b \pmod n] \bmod n$

$[a * (b + c)] \bmod n = \{[a * b \pmod n] + [a * c \pmod n]\} \bmod n$

$a^8 \bmod n = ((a^2 \bmod n)^2 \bmod n)^2 \bmod n$

13. Расширенный алгоритм Евклида.

Расширенный алгоритм Евклида

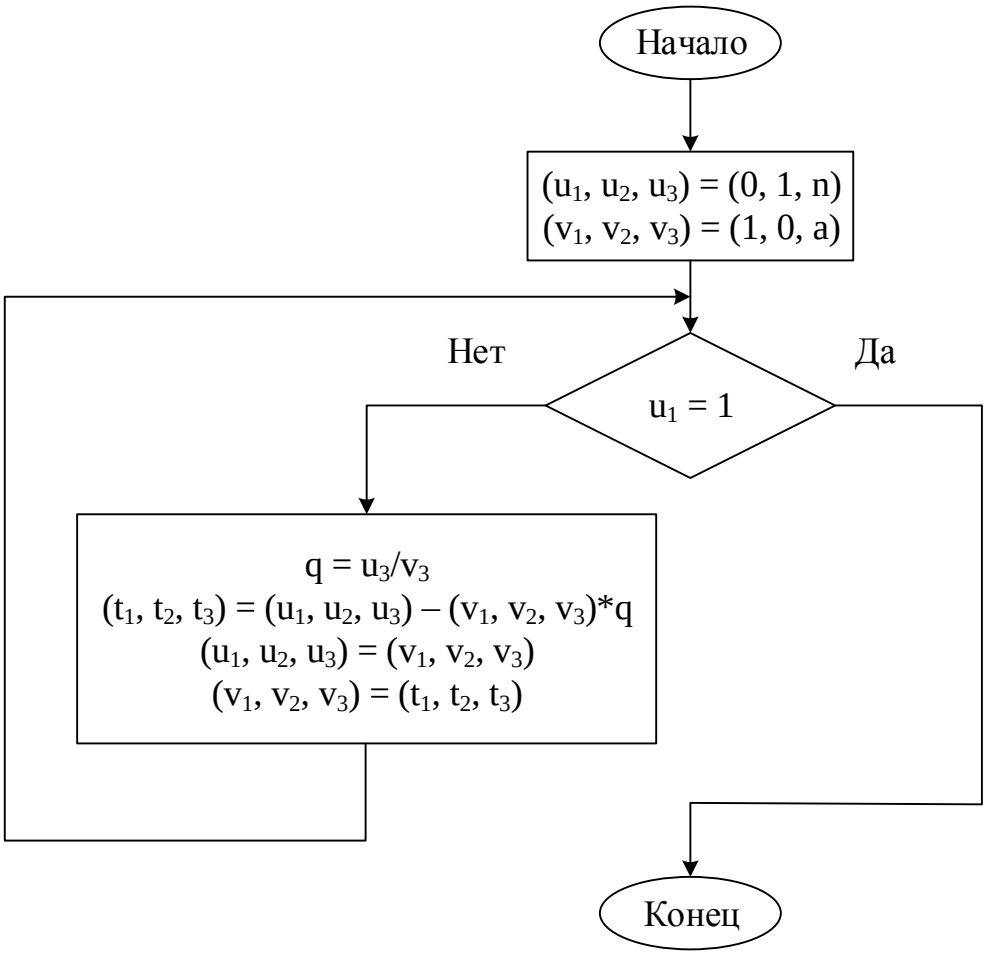
Пусть $a \in Z$, $b \in Z$ и определен вектор (u_1, u_2, u_3) такой, что $a*u_1 + b*u_2 = u_3$.

Пусть $b = n$, НОД$(a, n) = 1$.

Алгоритм определяет вектор (u_1, u_2, u_3) такой, что:

$$a * u_1 + n * u_2 = \text{НОД}(a, n) = 1,$$
$$(a * u_1 + n * u_2) \bmod n \equiv a * u_1 \pmod n = 1,$$
$$a^{-1} \pmod n \equiv u_1 \pmod n$$

Вспомогательные вектора: (v_1, v_2, v_3) и (t_1, t_2, t_3).



14. Типы секретных систем.

Криптография – метод защиты информации.

Типы секретных систем:

1) Системы маскировки (факт наличия сообщения скрывается от противника);
2) Тайные системы (раскрытие сообщения требует специального оборудования);
3) Секретные системы (смысл сообщения скрывается при помощи шифра или кода, но существование сообщения не скрывается и предполагается, что противник обладает любым специальным оборудованием, необходимым для перехвата и записи переданных сигналов).

15. Определение информации. Классификация защищаемой информации.

Информация – некоторые сведения, являющиеся объектом хранения, передачи и преобразования.

Классификация информации:

- По принадлежности (праву собственности):
    1) государственная тайна (владелец – государство и его структуры);
    2) служебная тайна (владелец – государство и его структуры);
    3) коммерческая тайна (владелец – государство, предприятие);
    4) партийная тайна (владелец – общественная организация, государство);
    5) тайна переписки, личная жизнь (владелец – гражданин государства).
- По степени секретности:
    1) особой важная (ОВ);
    2) совершенно секретная;
    3) секретная;
    4) для служебного пользования;
    5) несекретная.
- По содержанию:
    1) политическая;
    2) экономическая;
    3) военная;
    4) разведовательная;
    5) научно-техническая;
    6) технологическая;
    7) деловая.

16. Энтропия и неопределенность. Количество информации в сообщении.

Энтропия и неопределенность – количественные характеристики определения информации.

Энтропия – мера неопределённости информации, неопределённость появления какого-либо символа алфавита. При отсутствии информационных потерь равна количеству информации на символ передаваемого сообщения.

Количество информации – минимальное число бит, необходимое для кодирования всех возможных значений сообщения, если полагать все сообщения равновероятными. Формально количество информации в сообщении измеряется энтропией сообщения.

$$H(M) = \log_2 n$$

Где n – число возможных значений.

Пусть имеется сообщение, содержащее N последовательных ячеек, (текст из N букв). В каждой из ячеек может быть одна из M букв, где M – мощность алфавита. Тогда вероятность встречаемости конкретного символа:

$$p_i = \frac{N_i}{N}, i = \overline{1, n}$$

Где N_i – количество благоприятных событий.

Общее число различных последовательностей из N букв (при мощности M):

$$P = \frac{N!}{N_1! \times N_2! \times \ldots \times N_M!}$$

Количество информации в сообщении:

$$I = \log_2 P = \frac{\ln P}{\ln 2} = \frac{1}{\ln 2} \times \ln \frac{N!}{N_1! \times N_2! \times \ldots \times N_M!}$$

Количественная энтропия (формула Стирлинга):

$$H(M) = -N \times \sum_{i=1}^{M} p_i \times \log p_i$$

17. Энтропия языка. Абсолютная энтропия языка.

Энтропия языка – мера неопределённости появления какого-либо символ:

$$r = \frac{H(M)}{N} = -\sum_{i=1}^{M} p_i \times \log p_i$$

Абсолютная энтропия языка – максимальное количество бит, которое может быть передано каждым символом при равновероятности всех последовательностей символов (при равных корреляциях – частотах встречаемости сочетаний букв).

18. Избыточность информации.

Язык характеризуется определенной избыточностью информации, или возможностью прочитать осмысленный текст и при нехватке букв.

Избыточность языка:

$$D = R - r$$

$$R = \log_2 M$$

$$r = \frac{H(M)}{N} = \frac{\log_2 n}{N}$$

Где R – энтропия сообщения, содержащего все символы алфавита; r – энтропия языка, H(M) – энтропия сообщения, содержащего n символов алфавита, N – длина сообщения, M – мощность алфавита.

Истинная избыточность:

$$D = 1 - \frac{I_\infty}{I_0}$$

19. Стойкость криптосистем. Расстояние единственности.

Существуют криптосистемы, которые обеспечивают совершенную секретность: шифртекст не представляет никакой информации об открытом тексте. По Шеннону число возможных ключей столь же велико, что и число возможных сообщений. Иными словами, ключ должен быть не короче самого сообщения.

Энтропия криптосистемы – мера пространства K ключей:

$$H(K) = \log_2 K$$

Цель работы криптоаналитика при расшифровке некоторого набора символов заключается в определении ключа K, открытого текста M, либо их обоих.

Расстояние (точка) единственности U – приблизительный размер шифртекста, для которого сумма реальной информации в открытом тексте и энтропии ключа равна числу использованных битов шифртекста; U – мера объема шифртекста, необходимого для достижения единственности результата криптоанализа.

$$U = H(K)/D$$

Шифртексты длиннее расстояния единственности можно дешифровать одним осмысленным способом.

Шифртексты, которые заметно короче расстояния единственности, можно дешифровать несколькими способами, причем каждый из них может быть корректен. Таким образом можно защитить сообщение от злоумышленника, предложив ему несколько осмысленных вариантов.

20. Совершенный и идеальный шифры.

Совершенный шифр (по Шеннону) – шифр, который не раскрывает никаких сведений о соответствующем ему открытом тексте. При этом для совершенных шифров апостериорные вероятности открытых текстов совпадают с их априорными вероятностями.

Идеальный шифр (по Шеннону) – шифр с бесконечным расстоянием единственности U. Даже при успешном криптоанализе идеального шифра существует неопределенность.

Связь совершенного и идеального шифров: идеальный шифр не обязательно должен быть совершенным, но совершенный шифр всегда является идеальным.

21. Основные угрозы безопасности АСОИ.

Автоматизированная система обработки информации (АСОИ) – совокупность технических средств, программного обеспечения, методов обработки информации и действия персонала, которая обеспечивает выполнение автоматизированной обработки информации.

Безопасность АСОИ – защищенность системы от случайных и преднамеренных вмешательств в нормальный процесс функционирования АСОИ, а также от попыток хищения, изменения или разрушения компонентов системы.

Основные угрозы безопасности АСОИ:

- По характеру воздействия:
  1) случайные (отключение питания, сбои оборудования, ошибки в ПО и пр.);
  2) преднамеренные (целенаправленные действия злоумышленника);
- По типу воздействия:
  1) угрозы нарушения конфиденциальности информации;
  2) угрозы нарушения целостности информации;
  3) угрозы нарушения работоспособности системы (отказы в обслуживании).

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ.

Угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению.

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АСОИ, либо блокируют доступ к некоторым ее ресурсам.

22. Несанкционированный доступ (НСД). Основные каналы НСД.

Доступ к информации – возможность ознакомления с информацией, в частности копирование, модификация или уничтожение информации. Доступ к информации бывает санкционированным (СД) и несанкционированным (НСД).

Несанкционированный доступ (НСД) – доступ к информации, нарушающий установленные правила разграничения доступа.

Основные каналы НСД:

- Через персонал:
    1) хищение носителей информации;
    2) чтение информации с экрана или клавиатуры;
    3) чтение информации из распечатки.
- Через программу:
    1) перехват паролей;
    2) расшифровка зашифрованной информации;
    3) копирование информации с носителя.
- Через аппаратуру:
    1) подключение специально разработанных аппаратных средств, которые обеспечивают доступ к информации;
    2) перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания.

23. Основные этапы процесса построения системы защиты АСОИ.

Система защиты АСОИ – единую совокупность правовых и морально-этических норм, административных мер и программно-технических средств, направленных на противодействие угрозам АСОИ с целью сведения до минимума возможного ущерба пользователям и владельцам системы.

Основные этапы построения системы защиты:

- Анализ возможных угроз АСОИ (фиксирование состояние системы на время и определение возможных воздействий на каждый компонент системы).
- Планирование (формирование системы защиты).
- Реализация системы защиты.
- Сопровождение системы защиты.

24. Меры обеспечения безопасности компьютерных систем.

Меры обеспечения безопасности компьютерных систем:

- Правовые (действующие законы и нормативные акты, которые регламентируют правила обращения с информацией ограниченного пользования и ответственности за их нарушения).
- Морально-этические (нормы поведения, которые сложились в обществе по мере распространения компьютеров в стране).
- Организационные (регламентация процесса функционирования АСОИ, а также использования ресурсов АСОИ, деятельности персонала и порядка взаимодействия пользователей с системой).
- Физические (механические и электромеханические устройства или сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа нарушителей).
- Аппаратно-программные (электронные устройства и специальные программы, которые обеспечивают конфиденциальность и контроль целостности данных, разграничение доступа к ресурсам, резервирование ресурсов, аудит событий, шифрование данных, идентификацию и аутентификацию субъектов АСОИ).

25. Структура системы безопасности АСОИ. Функции подсистем безопасности.

Функции подсистем безопасности АСОИ:

1. Управление доступом:
   - идентификация субъектов;
   - проверка подлинности субъектов;
   - контроль доступа субъектов к объектам доступа.
2. Регистрация и учет:
   - регистрация входа субъектов в систему;
   - запуск и завершение программ и процессов;
   - изменение полномочий субъектов доступа;
   - учет защищаемых объектов доступа.
3. Криптографическая защита:
   - шифрование конфиденциальной информации;
   - шифрование информации, принадлежащей разным субъектам доступа на разных ключах;
   - использование криптографических средств.
4. Система обеспечения целостности:
   - обеспечение целостности программных средств и данных;
   - физическая охрана средств ВТ и носителей информации;
   - тестирование средств защиты информации на НСД;
   - восстановление средств защиты информации на НСД.

26. Классы защищенности АСОИ.

Установлено 9 классов защищенности АСОИ от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на 3 группы, отличающиеся особенностями обработки информации. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации.

Группы классов защищенности АСОИ:

1) Группа 1 (многопользовательские системы с разными правами доступа).
2) Группа 2 (многопользовательские системы с равными правами доступа).
3) Группа 3 (однопользовательские системы).

Обозначения:
ГТ – государственные тайны.
КИ – конфиденциальная информация.
СТ – служебные тайны.
ПД и КТ – персональные данные и коммерческие тайны.
ОВ – гриф «особой важности».
СС – гриф «совершенно секретно».
С – гриф «секретно».

Группы	ГТ			КИ		Системы по количеству пользователей	Права доступа пользователей
	С			ПД и КТ	СТ		
	СС						
	ОВ						
1	1А	1Б	1В	1Г	1Д	многопользовательские	разные права
2	2А	2Б					равные права
3	3А	3Б				однопользовательские системы	

27. Основные положения защиты информации, хранимой на НЖМД.

Основные положения защиты информации, хранимой на НЖМД:

1. Физическая защита информации, которая включает в себя инвентаризацию и ограничения доступа к НЖМД.
2. Систематический контроль над процессом замены, передачи и уничтожения информации на НЖМД.
3. Использование стандартизированных приложений и методик по уничтожению информации на НЖМД.
4. Систематическая проверка процессов уничтожения информации на НЖМД.
5. Периодический контроль надежности уничтожения информации с произвольно выбранных НЖМД.
6. Выбор способов для уничтожения информации на неисправных НЖМД путем анализа уровня конфиденциальности информации, хранимой на них.
7. Ведение отчетности по каждому уничтоженному НЖМД.

28. Способы уничтожения информации на магнитных носителях.

Способы уничтожения информации на магнитных носителях:

- Без разрушения носителя информации:
  - программные (средства стирания записи в устройствах воспроизведения и записи информации);
  - физические (неразрушающее изменение материала рабочей поверхности путем размагничивания или намагничивания до состояния магнитного насыщения).
- С разрушением носителя информации:
  - механические (повреждение носителя механическим воздействием, в том числе его измельчение);
  - термические (нагревание носителя до температуры разрушения основы носителя);
  - химические (разрушение рабочего слоя и основы носителя химическими средствами);
  - радиационные (разрушение носителя ионизирующим излучением).

29. Методы аутентификации.

Аутентификация пользователя – это проверка, действительно ли проверяемый пользователь является тем, за кого он себя выдает.

Аутентификационная информация – некая уникальная информация, которой владеет только конкретный пользователь.

Этапы аутентификации:

1. У пользователя однократно запрашивается аутентификационная информация – образец (или генерируется случайным образом и записывается на смарт-карту пользователя). Образец сохраняется в модуле аутентификации.
2. При каждой попытке входа пользователя модуль аутентификации запрашивает аутентификационную информацию и сравнивает её с образцом, при совпадении с которым делается вывод о подлинности пользователя и разрешается вход.

Факторы аутентификации:

1. Пользователь знает некую уникальную информацию (пароль, логин).
2. Пользователь имеет некий предмет с уникальным свойствами (смарт-карта).
3. Пользователь обладает некой биологической особенностью (отпечаток пальца).

Методы аутентификации:

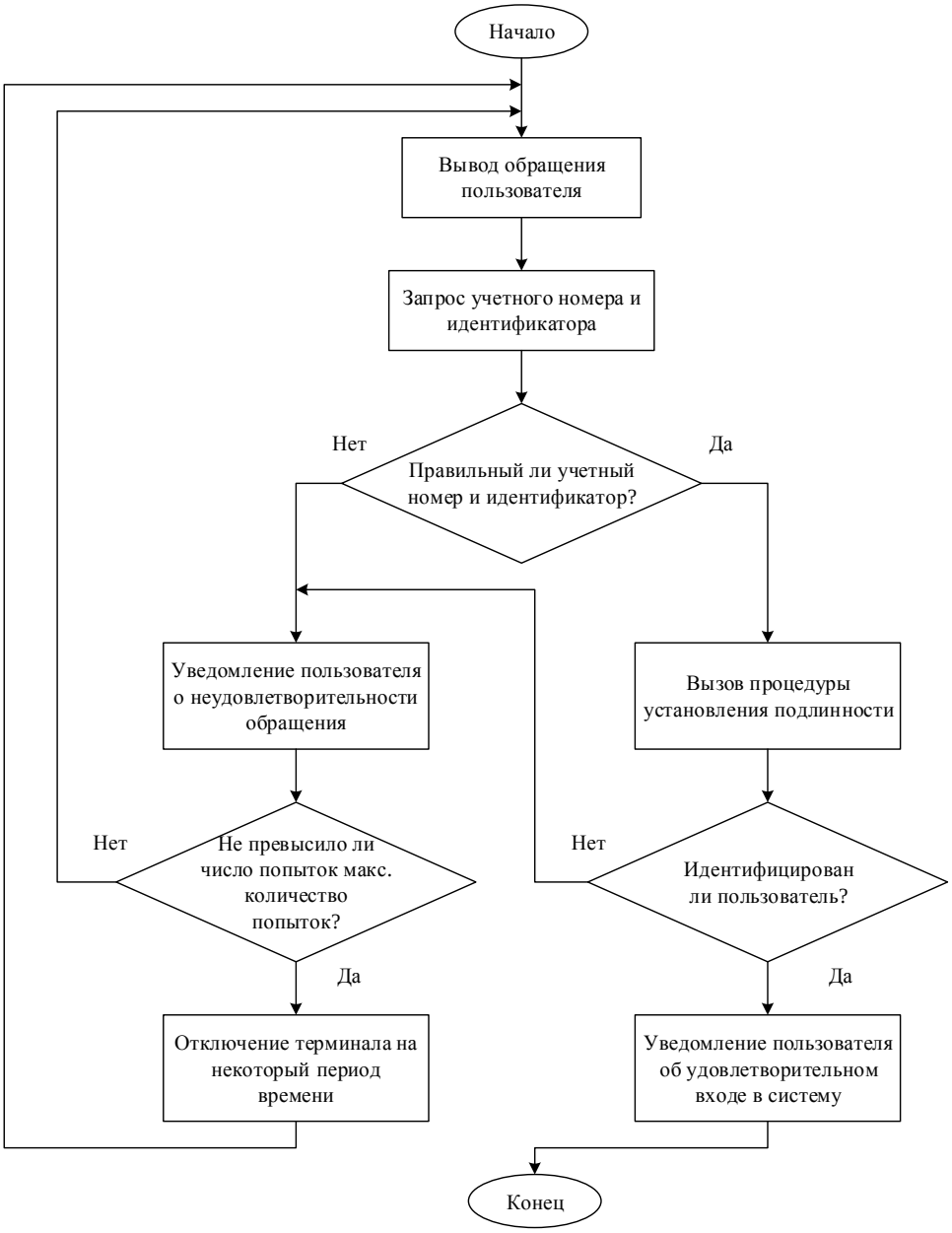
- Парольная аутентификация (по фактору 1). Образец (символьная запись) служит аутентификационной информацией, которая фиксируется ОС.
- Аутентификация с помощью уникального предмета (по фактору 2). Предмет содержит аутентификационную информацию в открытом или защищенном виде.
- Биометрическая аутентификация (по фактору 3). Образец (например, необработанное изображение или запись физиологической характеристики пользователя) регистрируется устройством (сканером или камерой).
- Многофакторная аутентификация (комбинация нескольких различных методов аутентификации для большей надежности проверки на подлинность).

30. Алгоритм непосредственной аутентификации.

Способы аутентификации делятся на **непосредственные** и **косвенные**. Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, то она называется **непосредственной аутентификацией**.

Непосредственная аутентификация требует явного предъявления доказывающим проверяющему некоторого уникального (присущего лишь ему) идентификатора.

Алгоритм непосредственной аутентификации:



31. Угрозы безопасности парольных систем.

Основные типы угроз безопасности парольных систем:

1) перебор паролей в интерактивном режиме;
2) подсматривание пароля;
3) преднамеренная передача пароля другому лицу;
4) перехват вводимого пароля путем внедрения в систему программных закладок;
5) перехват пароля, передаваемого по сети;
6) захват базы данных парольной системы;
7) использование ошибок, допущенных на стадии разработки системы;
8) выведение из строя парольной системы.

32. Требования к выбору пароля.

Требования к выбору и использованию паролей:

1) задание минимальной длины пароля;
2) ограничение числа попыток ввода пароля;
3) использование задержки при вводе неправильного пароля;
4) установление максимального срока действия пароля;
5) поддержка режима принудительной смены пароля по истечении срока действия;
6) использование в пароле различных групп символов;
7) проверка и отбраковка пароля по словарю;
8) применение эвристического алгоритма, блокирующего «плохие» пароли;
9) автоматическая генерация паролей (запрет выбора пароля пользователем).

33. Длина пароля и ожидаемое время раскрытия пароля.

Выбор необходимой длины пароля **S** можно производить исходя из заданной вероятности **P** того, что данный пароль может быть раскрыт посторонним лицом за время **T**. Если мы хотим построить систему, где незаконный пользователь имел бы вероятность отгадывания правильного пароля не больше, чем вероятность **P**, то нам следует выбрать такое значение **S**, которое удовлетворяло бы формуле Андерсона:

$$A^S \geq 4.32 \cdot 10^4 \cdot \frac{R \cdot T}{E \cdot P}$$

S – длина сообщения (в символах).

A – число символов в алфавите, из которых составляется пароль.

T – период времени (в месяцах), в течение которого предпринимаются попытки раскрытия пароля.

R – скорость передачи символов пароля (количество символов в минуту).

E – число символов в сообщении, передаваемом в систему при попытке получить к ней доступ (включая пароль и служебные символы).

P – вероятность раскрытия пароля.

Ожидаемое время раскрытия пароля:

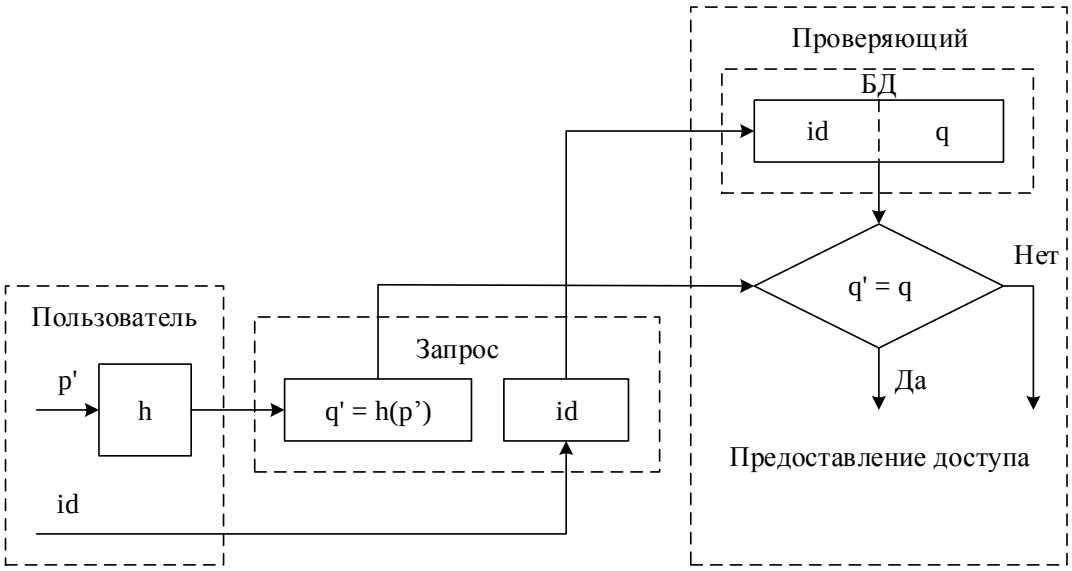
$$T_{раскр} = \frac{1}{2} \cdot A^S \cdot \frac{E}{R}$$

34. Схема защиты парольной системы от пассивного мониторинга.

Угроза пассивного перехвата пароля возникает при удаленном доступе.

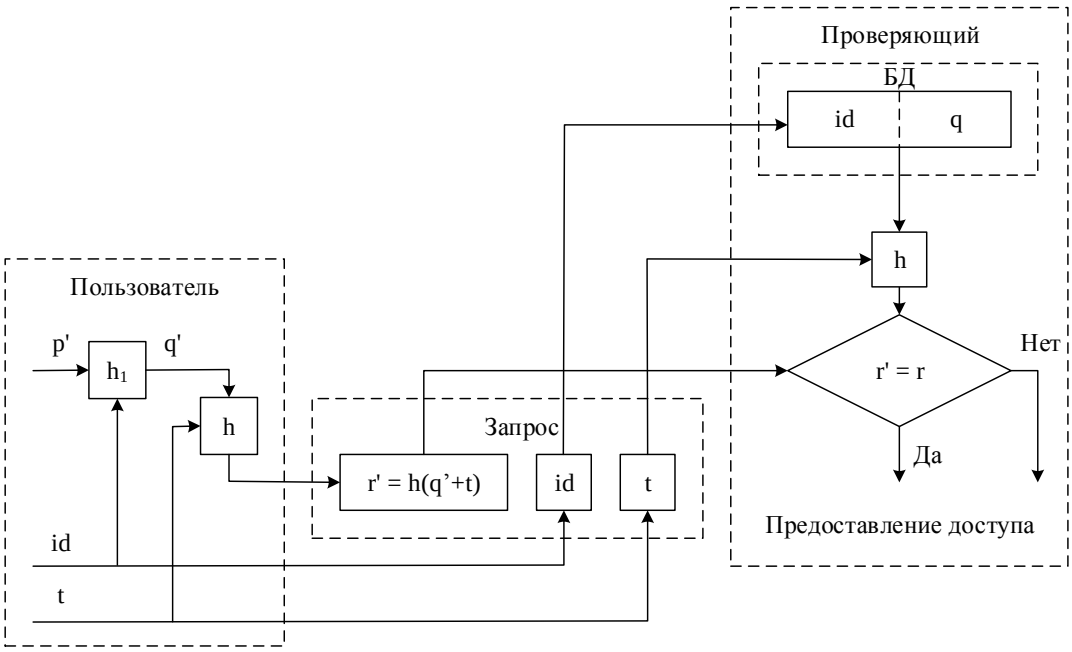
Предположим, что заданы пароль **p** и уникальный идентификатор пользователя **id**. Для получения доступа пользователь (или злоумышленник) вводит **id** и некоторый пароль **p'**. Вычисленное значение хэш-функции от введенного пароля **q' = h(p')** и идентификатор **id** передаются проверяющему. В БД для каждого **id** содержится значение **q = h(p)**. В случае **q' = q** проверяющий заключает, что **p' = p** – истинному паролю. Суть механизма защиты – знание **q** не позволяет просто определить **p** (нужно обратить хэш-функцию, а это вычислительно трудоемкая задача).

Описанная схема имеет существенный недостаток. Предполагаемый злоумышленник может заранее построить таблицу значений **q** для наиболее вероятных **p**. Будет ли раскрыт пароль, зависит от объема данных, полученных в результате мониторинга запросов на предоставление доступа, и от того насколько выбранное распределение вероятностей для **p** соответствует реальному.



35. Схема защиты парольной системы от несанкционир. воспроизведения.

Параметр t, или одноразовое число, обеспечивает уникальность каждого запроса на предоставление доступа. Для принятия положительного решения о предоставлении доступа проверяющий обязан установить, что число t из текущего запроса не использовалось ранее, в противном случае запрос отвергается.



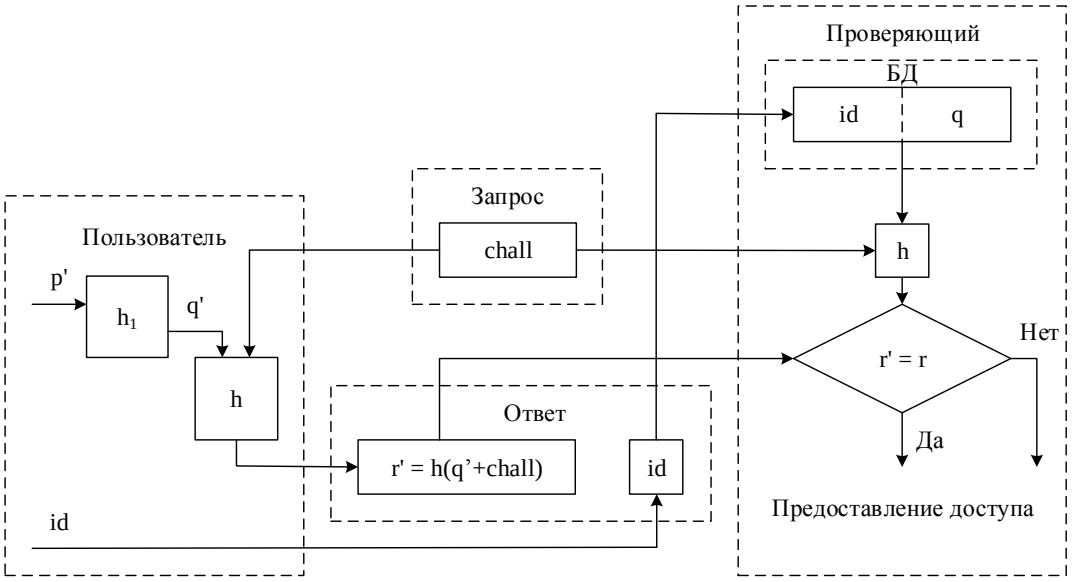
36. Схема аутентификации по методу «запрос-ответ».

Запрашивающий генерирует некоторое случайное число и передает его противоположной стороне. Ответ в виде криптографического преобразования заданного числа используется для принятия решения о предоставлении доступа.

На первом шаге в ответ на запрос компьютера пользователь вводит свое имя (login), далее комп, проверив полномочия доступа на уровне списка имен, выдает запрос в виде семизначного числа.

На втором шаге пользователь вводит запрос и секретный PIN-код в персональное устройство. Преобразование сводится к конкатенации (склеивание) запроса и PIN-кода с последующим шифрованием на секретном ключе устройства.

На третьем шаге пользователь вводит первые 7 цифр результата шифрования.



37. Вариант реализации одноразовых паролей по схеме S-Key.

На начальном этапе легальный пользователь случайно выбирает некое число **r** и для заданного системного параметра **n** при помощи рекурсивного хеширования (**n** раз) вычисляет финальное значение $\mathbf{W_0}$.

$\mathbf{W_0 = h(h(h(\ldots(h(W_n))..)))}$. Где **h(x)** – некоторая хэш-функция. $\mathbf{W_n = r}$.

Значение $\mathbf{W_0}$ вместе с **n** и идентификатором **id** передается проверяющему по аутентичному каналу связи. Записываем $\mathbf{W_0}$, **n**, **id** в БД. На этом заканчивается начальный этап формирования параметров схемы одноразовых паролей.

Потом пользователь вычисляет первый одноразовый пароль.

$\mathbf{W_1 = h(h(\ldots(h(W_n))..))}$ **n-1**-раз и передает его проверяющему по открытому каналу связи.

Проверяющий вычисляет **h(W1)**: $\mathbf{h(W_1) = W_0}$, если $\mathbf{W_0} = \mathbf{W_0}$ из БД, даем доступ.

По факту положительного решения проверяющий записывает в БД $\mathbf{W_1}$ вместо $\mathbf{W_0}$, и **(n-1)** вместо **n**.

И т.д. При **n = 0** все генерируется заново.

Таким образом, при каждом новом запросе используется уникальный пароль.

38. Структурная схема биометрической аутентификационной системы.

Любую биометрическую аутентификационную систему можно представить как систему распознавания образов.

Биометрическая система состоит из следующих элементов:

- Биометрические считыватели или сенсоры.
- Устройства выделения информативных признаков, обеспечивающих извлечение полезных характеристик из поступающих сигналов;
- Мэтчеры – устройства или ПО для сопоставления двух наборов биометрических характеристик.

Биометрическая система состоит из двух подсистем:

1. Регистрация.
2. Аутентификация.

Во время регистрации биометрические параметры объекта фиксируются, значимая информация собирается экстрактором свойств и сохраняется в базе данных.

Для идентификации система получает биометрический образ от объекта, выделяет из него значимую информацию и ищет в БД совпадающие с ним записи.

Для верификации объект предоставляет идентификатор (идентификационный номер) и биометрические параметры. Система считывает биометрические показатели, выделяет основные параметры, сравнивает их с параметрами, зарегистрированными в БД под номером данного пользователя.