Графы атак. Достижимость в графах

Преподаватель: Солодухин Андрей Геннадьевич

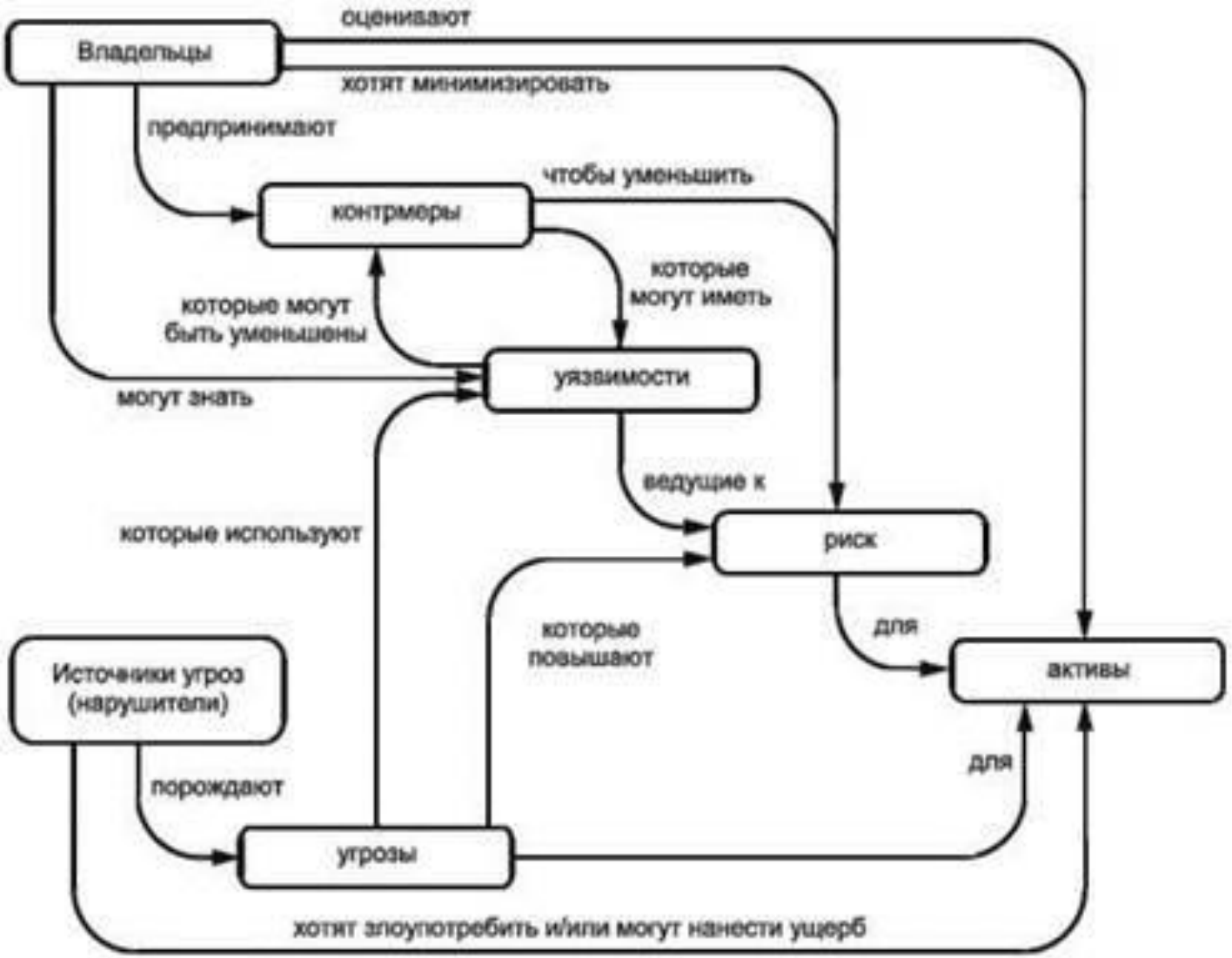
План

- 1. Понятие графа атак.
- 2. Достижимость в графах.
- 3. Алгоритмы построения матриц достижимости

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОР

Последовательность действий при анализе защищенности объекта:

ГРАФ АНАЛИЗА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ТЕХ

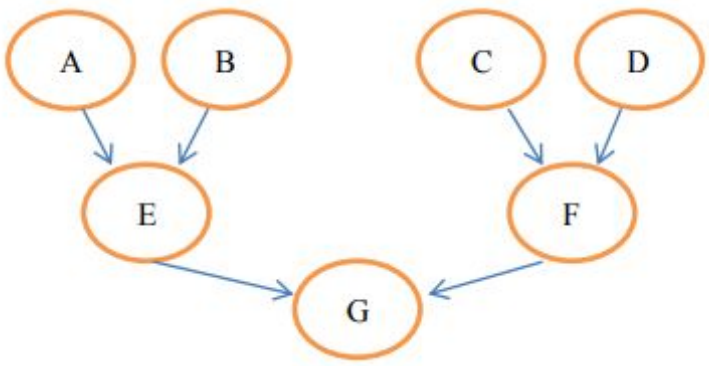


ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

В основном графы атак рассматриваются при анализе защищенности сетей.

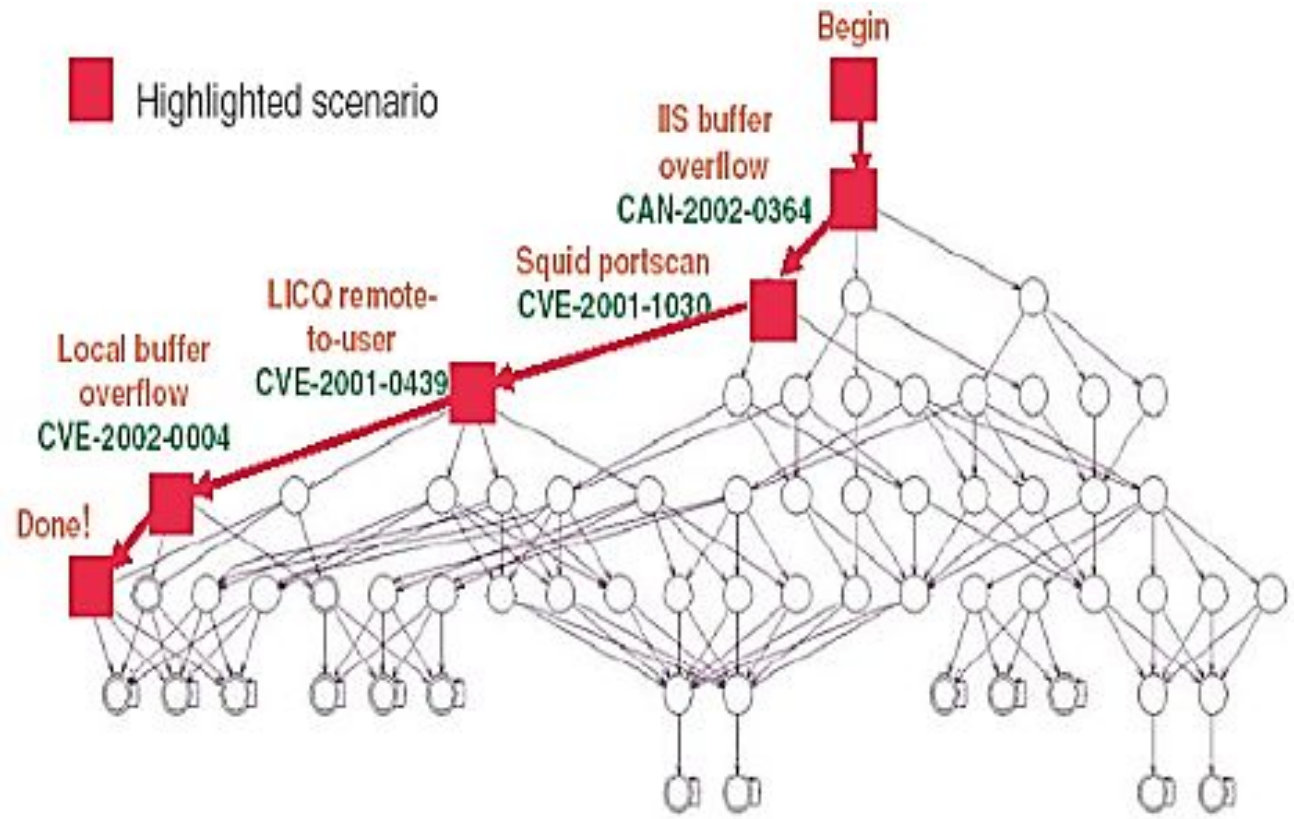
Топологический анализ защищенности сетей предполагает построение графа атак на основе результатов сканирования сети, модели нарушителя и данных о конфигурации сети

Граф атак – это граф, представляющий всевозможные последовательности действий нарушителя для достижения угроз (целей)



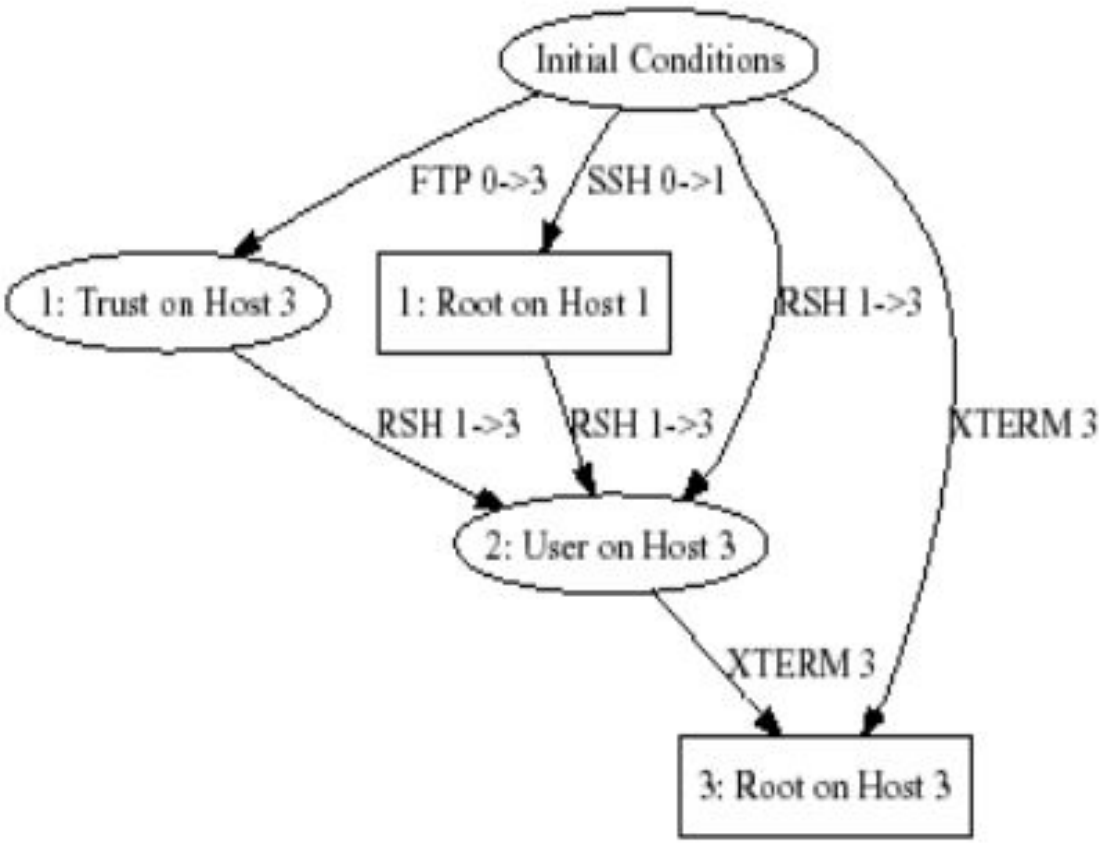
ТИПЫ ГРАФОВ АТАК

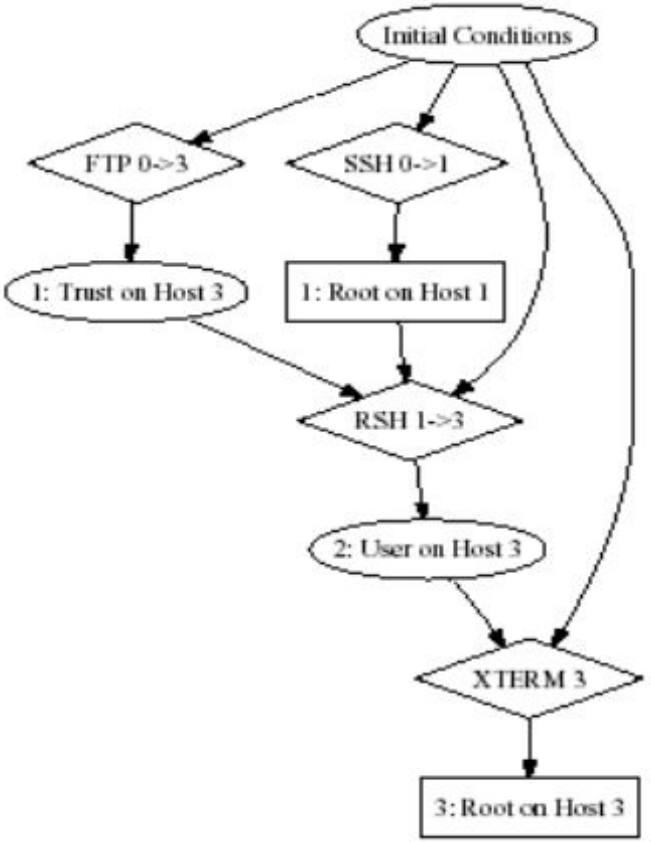
state enumeration graph –вершинам соответствуют тройки (s,d,a), где s – источник атаки, d – цель атаки,
a – элементарная атака



дуги обозначают переходы из одного состояния в другое

condition-oriented dependency graph – вершинам соответствуют результаты атак, а дугам – элементарные атаки, приводящие к таким результатам





exploit dependency graph – вершины соответствуют результатам атак, дуги отображают условия, необходимые для выполнения атаки и следствие атаки

Под элементарной атакой (atomic attack) понимают использование нарушителем уязвимости.

Граф может быть ***моделью организации***, в которой люди представлены вершинами, а дуги интерпретируют каналы связи. При рассмотрении такой модели можно поставить вопрос, может ли информация от одного лица xi быть передана другому лицу xj

т. е. существует ли путь, идущий от вершины xi к вершине xj. Если такой путь существует, то говорят, что вершина xj достижима из вершины xi. Можно интересоваться достижимостью вершины xj из вершины xi только на таких путях, длины которых не превосходят заданной величины или длина которых меньше наибольшего числа вершин в графе и т. д.

Граф атак может строиться в одном из следующих режимов:
- из одного объекта-источника атаки;
- конечного набора объектов-источников атаки

Перед построением графа атак необходимо построить ***матрицу достижимости***

Матрица достижимости может рассчитываться между объектами сети, или между объектами сети и источниками угроз. При расчете матрицы достижимости учитываются следующие особенности:
- ***динамическая маршрутизация*** : объект считается достижимым, если он достижим хотя бы по одному маршруту;
- возможность наличия ***нескольких оконечных точек для объекта*** (источника угроз) : угроза считается достижимой, если она достижима хотя бы на одной оконечной точке;
- при расчете матрицы учитываются ***возможности преобразования адресов источника и получателя*** (источника угроз и узла сети).

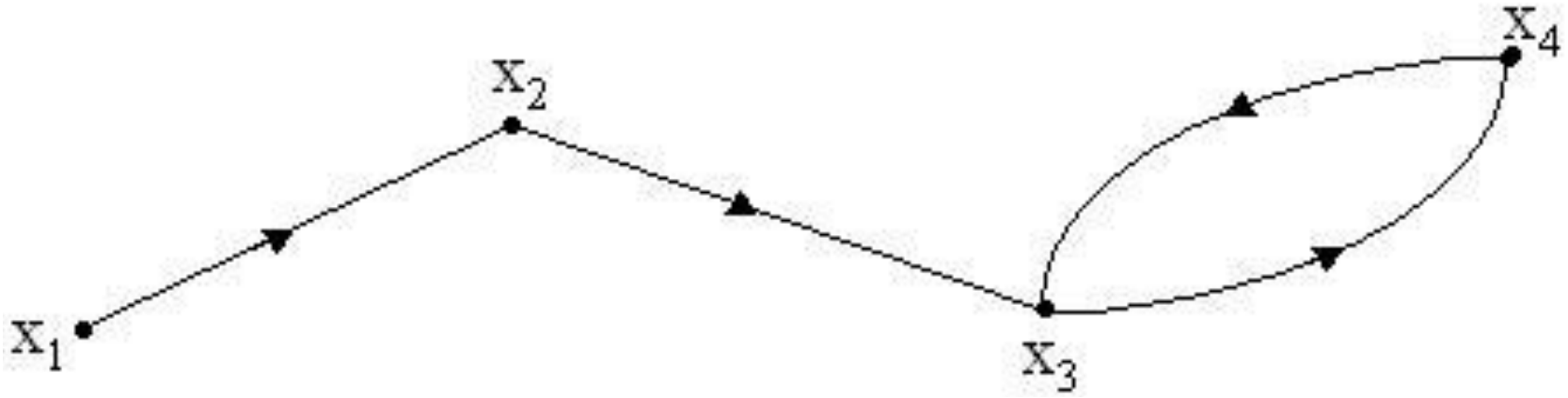
ПОНЯТИЕ ДОСТИЖИМОСТИ

Вершина графа v_i называется ***достижимой*** из вершины v_j того же графа, если существует по крайней мере один путь из v_i в v_j. Множество вершин $R(v_i)$, достижимых из некоторой вершины $v_i \in V$, определяется следующим выражением:

$$R(v_i) = \{v_i\} \cup \Gamma(v_i) \cup \Gamma^2(v_i) \cup \cdots \cup \Gamma^p(v_i)$$

$\Gamma(v_i)$ - множество вершин v_j, достижимых из v_i с использованием путей длины единица; $\Gamma^2(v_i)$ - множество вершин, достижимых из v_i с использованием путей длины два; $\Gamma^p(v_i)$ - множество вершин, достижимых из v_i с использованием путей длины *p*.

Матрицей достижимостей $\boldsymbol{D} = [\boldsymbol{d_{ij}}]$ называется квадратная матрица порядка *n*, элемент которой $\boldsymbol{d_{ij}}$ равен ***1***, если $x_j \in R(x_i)$ т.е. ***вершина i достижима из вершины j,*** и 0 в противном случае.



$$D(x_1) = \{x_1\} \cup \{x_2\} \cup \{x_3\} \cup \{x_4\} \cup \{x_3\} = \{x_1, x_2, x_3, x_4\}$$
$$D(x_2) = \{x_2\} \cup \{x_3\} \cup \{x_4\} \cup \{x_3\} = \{x_2, x_3, x_4\}$$
$$D(x_3) = \{x_3\} \cup \{x_4\} \cup \{x_3\} = \{x_3, x_4\}$$
$$D(x_4) = \{x_4\} \cup \{x_3\} \cup \{x_4\} = \{x_3, x_4\}$$

$$D = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Матрица контрдостижимостей (обратных достижимостей) $\boldsymbol{Q} = [q_{ij}]$ определяется следующим образом: q_{ij}=1, если $x_j \in Q(v_i)$ т.е. из вершины j можно достигнуть вершину *i,* и 0 в противном случае

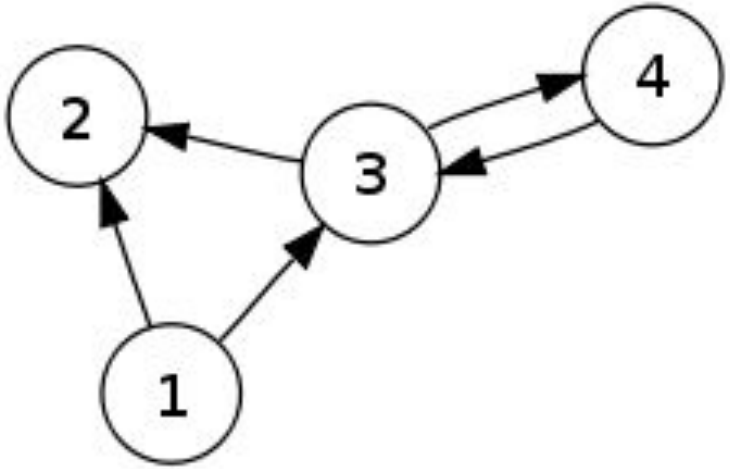
в матрице контрдостижимости в каждом столбце x_j ставится 1 напротив того узла x_i, с которым узел x_j связан - неважно, непосредственно или через другие узлы.

$$Q(x_1) = \{x_1\}; Q(x_2) = \{x_2\} \cup \{x_1\} = \{x_1, x_2\}$$
$$Q(x_3) = \{x_3\} \cup \{x_2, x_4\} \cup \{x_1, x_3\} = \{x_1, x_2, x_3, x_4\}$$
$$Q(x_4) = \{x_4\} \cup \{x_3\} \cup \{x_2, x_4\} \cup \{x_1, x_3\} = \{x_1, x_2, x_3, x_4\}$$

Матрица контрдостижимостей будет иметь вид:

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} = D^T$$

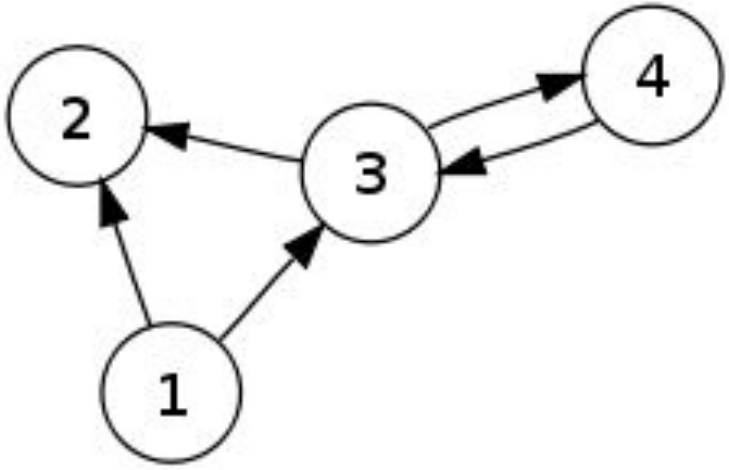
СПОСОБЫ ПОСТРОЕНИЯ МАТРИЦЫ ДОСТИЖИМОСТИ



Матрица достижимости может быть получена в результате операций логического сложения матриц

$$\boldsymbol{E}^* = E \cup E^2 \cup E^3 \cup E^4$$

где E^2, E^3, E^4 – булевы степени матрицы смежности E.

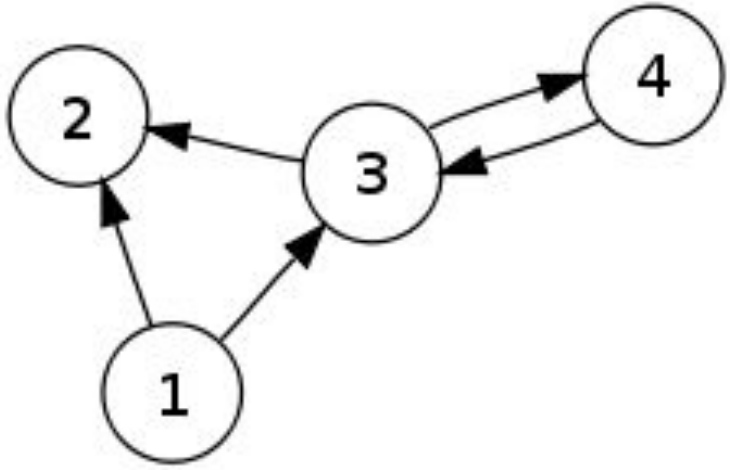


$$\boldsymbol{E} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \boldsymbol{E^2} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\boldsymbol{E^3} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \boldsymbol{E^4} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

```
const m=5; p=5; n=5;
var
  e: array [1..m,1..p] of real;
  b: array [1..p,1..n] of real;
  c: array [1..m,1..n] of real;
  s: Real;
  i, j, k: Integer;
begin
  ...
  for i:=1 to m do
    for j:=1 to n do begin
      s:=0; for k:=1 to p do
                              s:=s+e[i,k]*b[k,j];
      c[i,j]:=s;
    end;
  ...
end.
```

```
const m=5; p=5; n=5;
var
  e: array [1..m,1..m] of integer;
  // b: array [1..p,1..n] of integer;
  c: array [1..m,1..m] of integer;
  s: integer;
  i, j, k: Integer;
begin
  ...
  for i:=1 to m do
    for j:=1 to n do begin
      s:=0; for k:=1 to p do
                              s:=s+e[i,k]*e[k,j];
      c[i,j]:=s;
    end;
  ...
end.
```

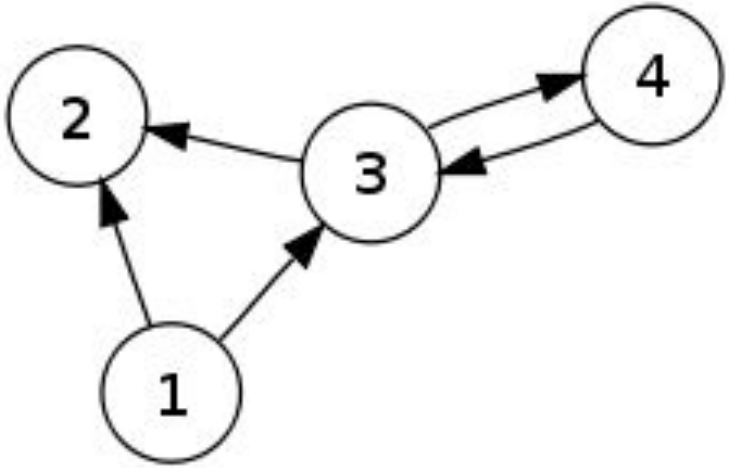


$$\boldsymbol{E^*} = \boldsymbol{E} \cup \boldsymbol{E^2} \cup \boldsymbol{E^3} \cup \boldsymbol{E^4} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\boldsymbol{E^*} = \boldsymbol{E} + \boldsymbol{E^2} + \boldsymbol{E^3} + \boldsymbol{E^4} = \begin{pmatrix} 0 & 3 & 2 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 \end{pmatrix}$$

АЛГОРИТМ ФЛОЙДА-УОРШЕЛЛА

1. Берем *k*-ый столбец матрицы смежности *E*.
2. Строки, у которых в *k*-ом столбце стоит 0, копируем в новую матрицу.
3. Строки с номером *i*, у которых в *k*-ом столбце стоит 1, объединяем с помощью операции ***ИЛИ*** с *k*-ой строкой, результат записываем в ту же новую матрицу.



$$E_0 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Вычисляем матрицу E1. Учитывая первый шаг, рассматриваем 1-ый столбец матрицы E0. Следуя указаниям шага 2, скопируем строки матрицы E0, в первом столбце которой стоят 0:

$$E_1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 0 & 1 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix}$$

В первом столбце единиц нет. Переходим к рассмотрению второго столбца и вычислению матрицы E2. Рассчитываем значения в строке 1-ой и 3-ей, выполняя дизъюнкцию k-ой строки (второй) со строками, у которых на k-ом месте стоит 1

$$E_2 = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Вычисляем матрицу E3. Рассматриваем 3-ий столбец матрицы E2. Копируем строки, у которых в 3-ем столбце 0: вторую и третью Рассчитываем значения в строке 1-ой и 4-ой, выполняя дизъюнкцию k-ой строки (третьей) со строками, у которых на k-ом месте стоит 1. Получаем матрицу E3:

Вычисляем матрицу E4. Рассматриваем 4-ый столбец матрицы E3. Копируем строки, у которых в 4-ом столбце 0: вторую. Рассчитываем значения в строке 1-ой, 3-ей и 4-ой, выполняя дизъюнкцию k-ой строки (четвертой) со строками, у которых на k-ом месте стоит 1. Полученная матрица является матрицей достижимости – E*

$$\boldsymbol{E_3} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \qquad \boldsymbol{E_4} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

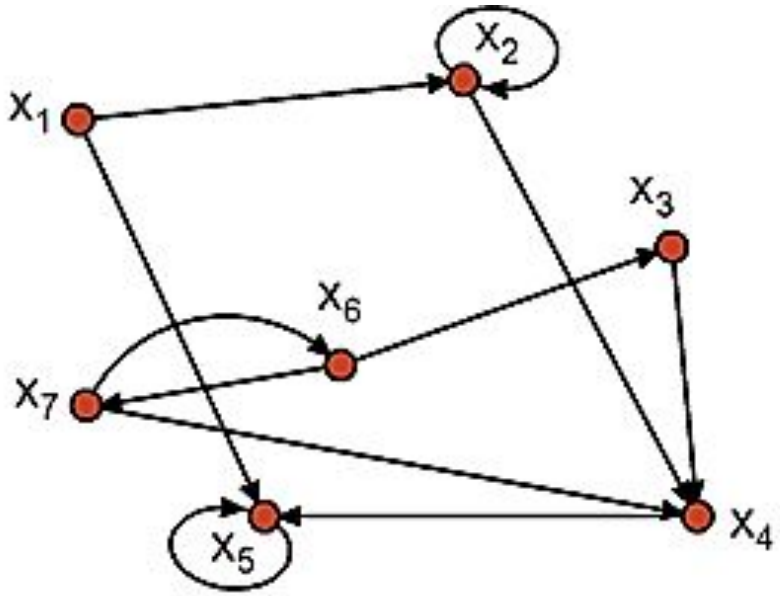
АЛГОРИТМ ФЛОЙДА-УОРШЕЛЛА: программная реализация

расчет кратчайших путей в графе

```
for k = 1 to n
  for i = 1 to n
    for j = 1 to n
      W[i,j] = min(W[i,j], W[i,k] + W[k,j])
```

Для нахождения матрицы достижимости оператор **min** заменяется дизъюнкцией, сложение заменяется конъюнкцией

```
 for k = 1 to n
  for i = 1 to n
    for j = 1 to n
      W[i,j] = W[i,j] or (W[i,k] and W[k,j])
```



а

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	0	1	0	0	1	0	0
x_2	0	1	0	1	0	0	0
x_3	0	0	0	1	0	0	0
x_4	0	0	0	0	1	0	0
x_5	0	0	0	0	1	0	0
x_6	0	0	1	0	0	0	1
x_7	0	0	0	1	0	1	0

б

R=

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	1	1	0	1	1	0	0
x_2	0	1	0	1	1	0	0
x_3	0	0	1	1	1	0	0
x_4	0	0	0	1	1	0	0
x_5	0	0	0	0	1	0	0
x_6	0	0	1	1	1	1	1
x_7	0	0	1	1	1	1	1

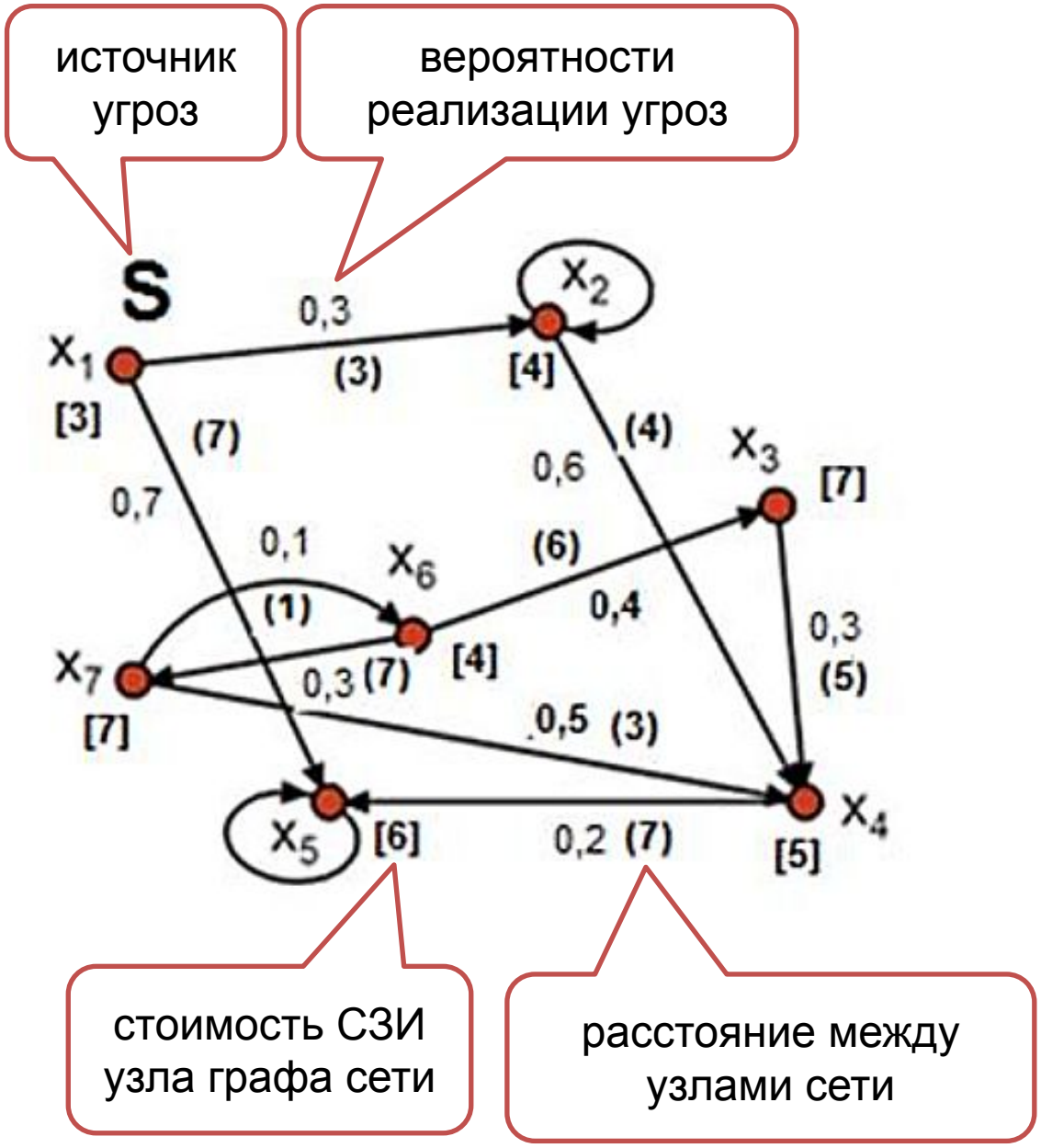
в

Q=

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	1	0	0	0	0	0	0
x_2	1	1	0	0	0	0	0
x_3	0	0	1	0	0	1	1
x_4	1	1	1	1	0	1	1
x_5	1	1	1	1	1	1	1
x_6	0	0	0	0	0	1	1
x_7	0	0	0	0	0	1	1

г

источник атак воздействует на сеть из узла S – узла №1.

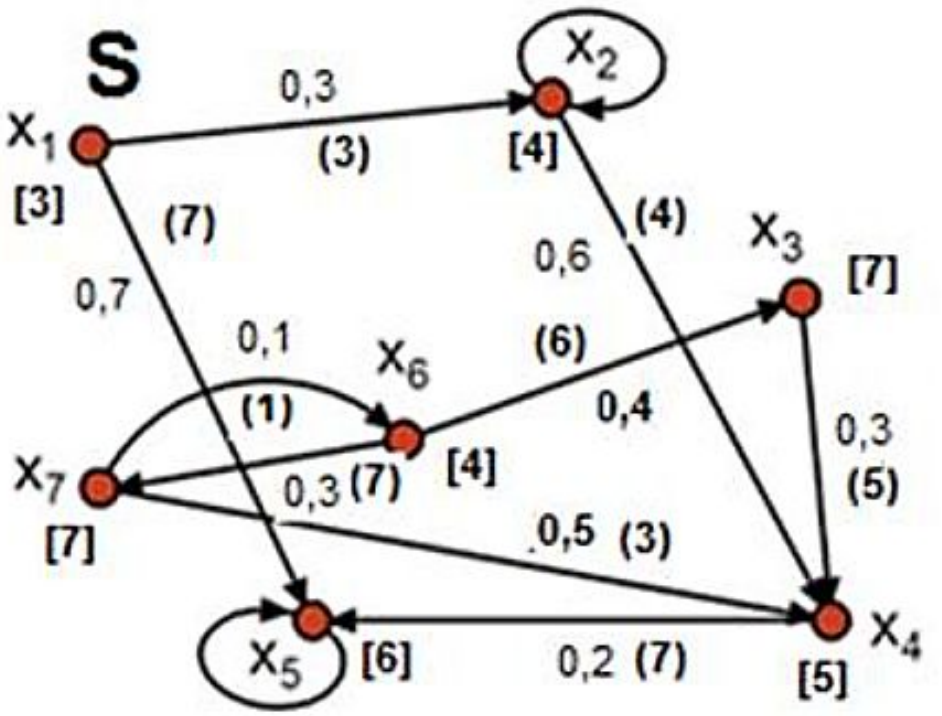


	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	0	1	0	0	1	0	0
x_2	0	1	0	1	0	0	0
x_3	0	0	0	1	0	0	0
x_4	0	0	0	0	1	0	0
x_5	0	0	0	0	1	0	0
x_6	0	0	1	0	0	0	1
x_7	0	0	0	1	0	1	0

матрица достижимости:

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	1	1	0	1	1	0	0
x_2	0	1	0	1	1	0	0
x_3	0	0	1	1	1	0	0
x_4	0	0	0	1	1	0	0
x_5	0	0	0	0	1	0	0
x_6	0	0	1	1	1	1	1
x_7	0	0	1	1	1	1	1

Определим методом Дийкстры кратчайшие маршруты до узлов достижимости сети – целей атак из узла S



S-2-4 длина 7
S-5 длина 7

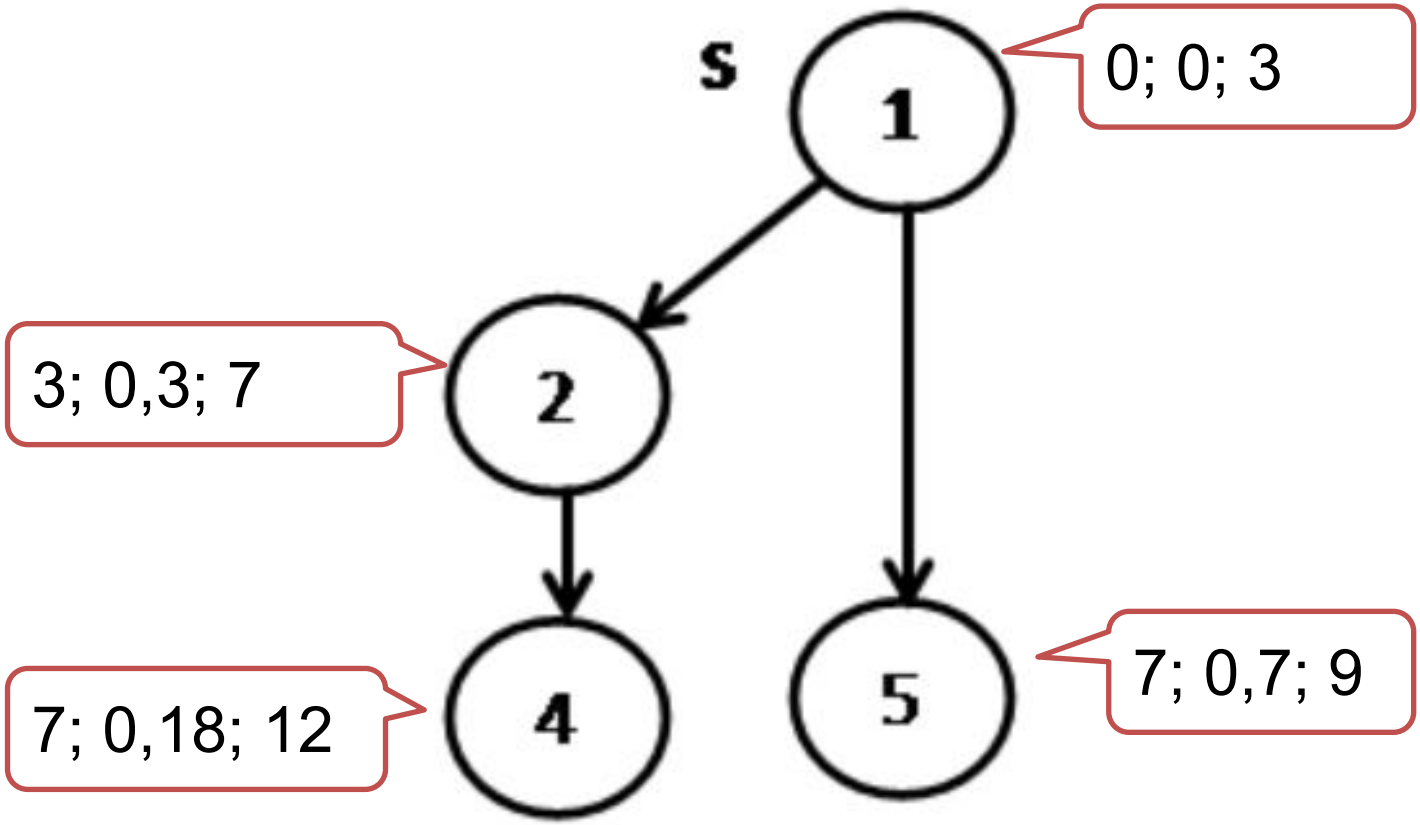
S-2 вероятность 0,3
S-2-4 вероятность 0,18
S-5 вероятность 0,7

S-2 стоимость 7
S-2-4 стоимость 12
S-5 стоимость 9

Аналогично определим методом Дийкстры совокупные максимальные вероятности реализации угроз

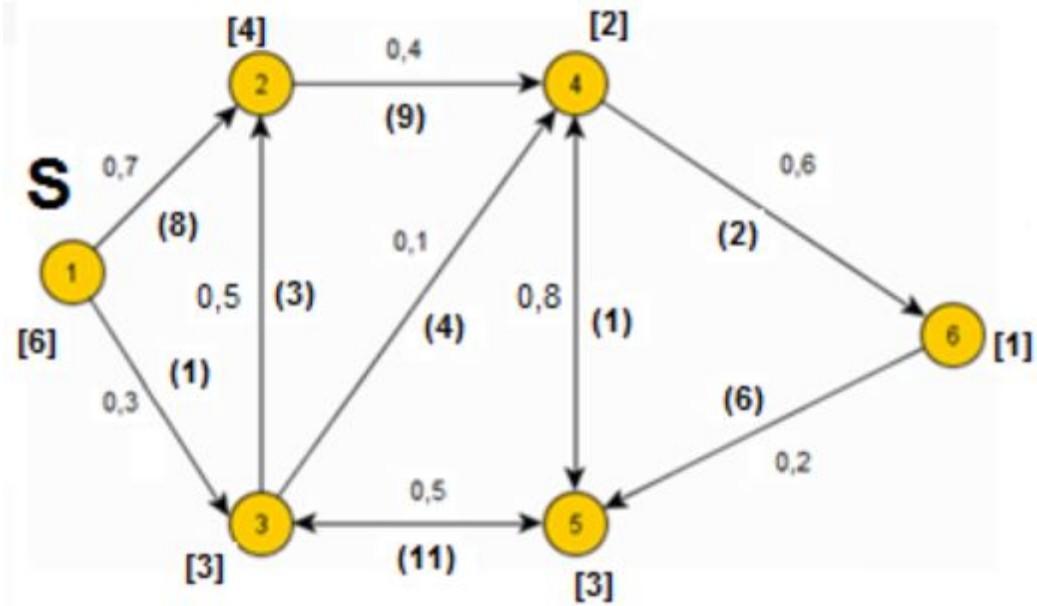
Аналогично определим методом Дейкстры совокупную минимальную стоимость СЗИ узлов графа сети

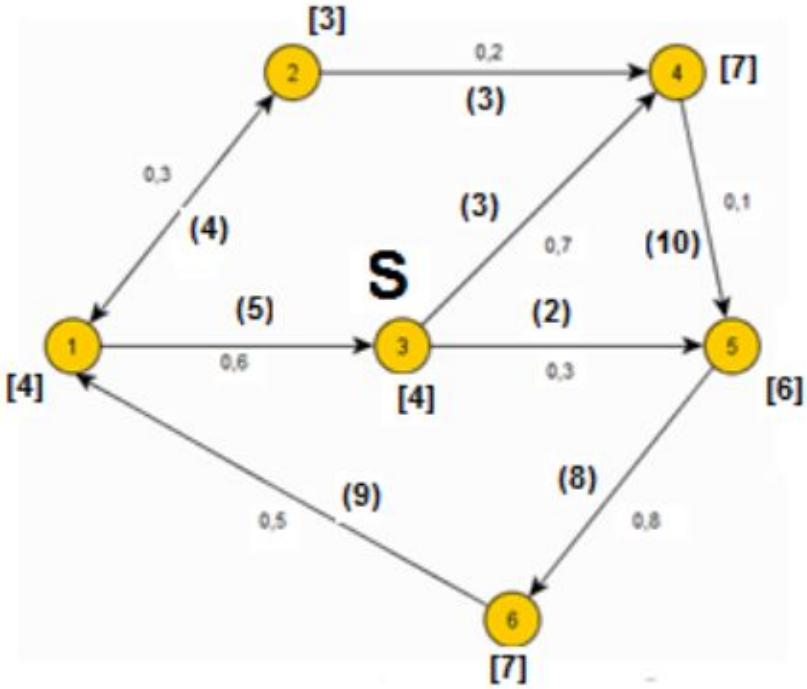
ИТОГОВЫЙ ГРАФ АТАК



Вопросы

1. Опишите последовательность действий при анализе защищенности объекта.
2. Дайте определение графа атак.
3. Какие виды графов атак вы знаете?
4. Определение матрицы достижимости.
5. Определение матрицы контрдостижимости.
6. Опишите матричный способ нахождения матрицы достижимости.
7. Опишите алгоритм Флойда-Уоршелла.


[4]
[2]
0,4
(9)
2
4
S
0,7
(8)
1
0,5
(3)
0,1
(4)
0,8
(1)
0,6
(2)
6
[1]
[6]
(1)
0,3
(6)
0,2
0,5
3
5
(11)
[3]
[3]


[3]
0,2
2
4
[7]
(3)
0,3
(4)
(3)
0,1
0,7
(10)
S
(5)
(2)
1
3
5
0,6
0,3
[4]
[4]
[6]
(9)
(8)
0,5
0,8
6
[7]

Источники информации

- Программирование, компьютеры и сети https://progr-system.ru/

Благодарю за внимание!