Лабораторная работа № 6 АИБ

**Оценка состояния информационной безопасности на основе графа перехода состояний**

**Цель занятия:** получить практические навыки оценки состояния информационной безопасности (ИБ) на основе графа перехода состояний.

**1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн)» под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

В соответствии со статьей 19 Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных» ПДн должны быть защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн и(или) потребителей, пользующихся услугами, предоставляемыми ИСПДн в соответствии с ее назначением, так и со специально осуществляемыми неправомерными действиями иностранных государств, криминальных сообществ, отдельных организаций и граждан, а также иными источниками угроз.

Угрозы безопасности ПДн могут быть реализованы за счет утечки ПДн по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

Детальное описание угроз, связанных с утечкой ПДн по техническим каналам, приведено в «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Выявление технических каналов утечки ПДн осуществляется на основе нормативных и методических документов ФСТЭК России.

Для характеристики исходной степени защищенности используют следующие градации: **высокая, средняя и низкая**.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

**маловероятно** – отсутствуют объективные предпосылки для осуществления угрозы;

**низкая вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию;

**средняя вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

**высокая вероятность** – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Очевидно, что на степень защищенности ИСПДн влияют как принимаемые меры по ее повышению, так и реализуемые угрозы с учетом их вероятностей. Различные степени защищенности ИСПДн характеризуют различные состояния ИБ, а переход из одного состояния в другое под действием мероприятий повышения уровня ИБ или реализации угроз можно представить в виде графа перехода состояний. Пример такого графа показан на рис. 1.

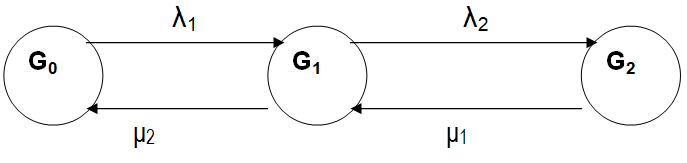


Рисунок 1 – Граф перехода состояний

На рисунке 1 обозначено: G0, G1, G2 – различные состояния ИБ ИСПДн; λ1, λ2, μ1 и μ2 - интенсивности переходов системы из состояния в состояние.

Интенсивности переходов имеют размерность [1/единица времени], например, 1/час или 1/год.

Граф перехода состояний составляется экспертами на основе анализа исходного состояния ИБ и вероятностей реализации тех или иных угроз ИБ. Угроз может быть множество, поэтому состояний может быть обозначено также много, каждое из которых будет отражать состояние ИБ ИСПДн после реализации той или иной угрозы.

Целью анализа графа перехода состояний является определение вероятностей нахождения ИСПДн в том или ином состоянии и вычисления коэффициента готовности ИСПДн, который равен сумме вероятностей нахождения ИСПДн в тех состояниях, которые допустимы с точки зрения обеспечения ИБ.

Граф считается заданным, если заданы состояния, указаны стрелки переходов между состояниями и интенсивности этих переходов. Для вычислений вероятностей состояний составляется система дифференциальных уравнений (СДУ) Колмогорова по следующим правилам:

1. Уравнений записывается столько, сколько состояний, плюс одно нормировочное (сумма вероятностей состояний равна единице).
2. Слева в каждом уравнении записывается производная от вероятности рассматриваемого состояния.

3. Справа от знака равно записывается **сумма произведений** **вероятностей** состояний, из которых стрелка выходит **на интенсивность** перехода по соответствующей стрелке. В каждом уравнении учитываются только те стрелки, которые входят или выходят из состояния, производная которого записана слева от знака равенства. Если стрелка **входит** в рассматриваемое состояние (стоящее слева от знака равенства), то произведение берется со знаком **плюс**. Если стрелка **выходит** из состояния, производная которого записанного слева в уравнении – то произведение берется со знаком минус.

Для данного примера СДУ имеет вид:

P0 **‘**(t) = - λ1 P0 (t) + μ2 P1(t),

P1 **‘**(t) = λ1 P0 (t) –( λ2 + μ2)P1(t) + μ1P2(t),

P2 **‘**(t) = λ2 P1 (t) – μ1 P2(t),

P0 (t)+P1(t)+P2(t)=1 – нормировочное уравнение,

где P0 (t), P1 (t), P2 (t) – вероятности соответствующих состояний.

Решая полученную СДУ находят вид функций P0(t), P1(t) и P2(t).

На практике интерес часто представляют установившиеся значения вероятностей, при t →∞, когда закончились все переходные процессы. В этом случае производные слева становятся равными нулю и система диф. уравнений превращается в систему из четырех линейных алгебраических уравнений, которые можно решать методом Гаусса или в каком либо математическом программном пакете.

Задавшись конкретными значениями интенсивностей потоков λ1 = 9 .10-4 час-1, λ2 = 9.10-4 час-1, μ1 =2.10-4 час-1 μ2 = 10-4 час-1, можно получить P0(∞)=0,0198, P1(∞)=0,178 и P2(∞)=0,802. Их сумма равна 1.

Если считать, например, состояния G1 и G2 как удовлетворяющие требованиям к уровню ИБ, а G0 как не удовлетворяющее, то коэффициент готовности системы будет равен: kг = P1 (∞)+ P2 (∞) =0,178 + 0,802 = 0.98.

Для численного решения СДУ приведенного примера можно воспользоваться средой MatLAB. Соответствующая программа на языке MatLAB представлена в листинге 1, а на рис. 2 показаны результаты ее работы

**Листинг 1** – Программа численного решения СДУ

clc, clear

global L1 L2 m1 m2 % определили интенсивности переходов как глобальные переменные

L1=0.0009;L2=0.0009;m1=0.0004;m2=0.0001; % определяем значения интенсивностей

tmax=7000; % время расчета, выбирается исходя из условия, чтобы закончились переходные процессы %– графики вероятностей вышли на горизонтальный участок

P= [0.3;0.3;0.4]; % вектор начальных значений, числа произвольные, но их сумма =1

[T,Z] = ode45('diffur1', [0,tmax],P); % решение системы диф. ур.

plot(T,Z(:,1),'k',T,Z(:,2),'k.',T,Z(:,3),'k--') % графики вероятностей по результатам ode45

xlabel('время')<ylabel('Вероятности')

Z(end,1) % берем последнее значение 1-го столбца, это установившееся значение Р0

Z(end,2) % берем последнее значение 2-го столбца - установившееся значение Р1

Z(end,3) % берем последнее значение 2-го столбца - установившееся значение Р2

disp('проверяем, сумма должна быть равна 1'),Z(end,1)+Z(end,2)+Z(end,3)

disp('Коэффициент готовности:'),Z(end,1)+Z(end,2)

**function** [dP]=diffur1(t,P) % эту функцию разместить в отдельном файле **diffur1.m**

% функция, описывающая СДУ Коломогорова. Учтем, что индексация массивов в MatLAB %начинается с 1, поэтому нумерация вероятностей смещена на 1 в сторону увеличения

global L1 L2 m1 m2

dP=zeros(3,1);

dP(1,1)=-L1\*P(1,1)+m2\*P(2,1);

dP(2,1)=L1\*P(1,1)-(L2+m2)\*P(2,1)+m1\*P(3,1);

dP(3,1)=L2\*P(2,1)-m1\*P(3,1);

end

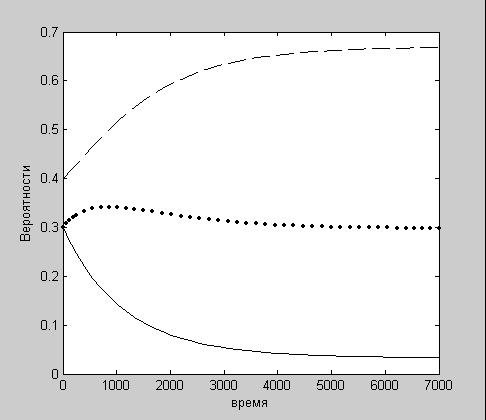


Рисунок 2 – Графики вероятностей

На рисунок 2 надо нанести надписи – где какая вероятность. Для этого в программу надо добавить команды gtext(‘P0’), gtext(‘P1’), gtext(‘P2’). После запуска программы появятся курсоры-перекрестья – надо ими щелкнуть мышкой в том месте, где требуется соответствующая надпись.

В задании надо будет найти максимальное значение kг при изменении значений λ1 и μ1 и построить соответствующий график. На рисунке 3 показана структура программы, позволяющая это сделать, на рисунке 4 – результат ее применения.

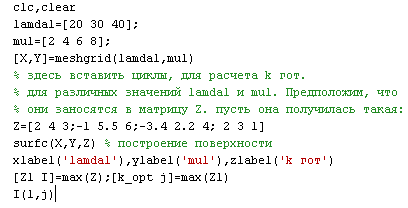


Рисунок 3 – Программа построение 3D-графика

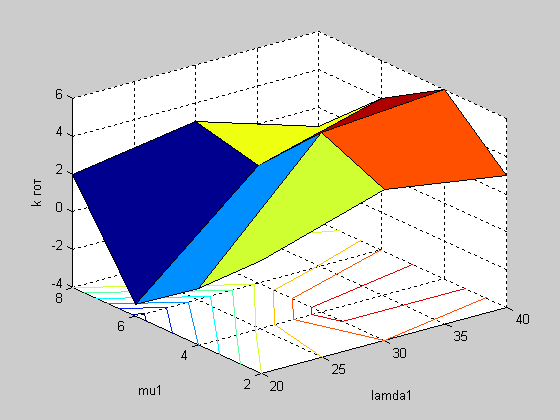


Рисунок 4 – 3D-график в MatLAB

**2 ЗАДАНИЕ**

1. Изучить теоретические положения. Выбрать вариант задания – взять его по номеру фамилии в журнале группы. Варианты заданий представлены в Приложении А.
2. Записать для своего варианта СДУ Колмогорова, перейти от нее к системе линейных алгебраических уравнений (СЛАУ) и решить ее – найти Pi(∞).

3. Численно решить СДУ ее в любой программной среде (например, MatLAB) и построить графики изменения вероятностей состояния во времени Pi(t) (см. программу в теоретической части). Сравнить установившиеся значения вероятностей Pi(∞) с найденными в пункте 2 для СЛАУ. Если они не совпадают – найти причину.

4. Вычислить коэффициент готовности kг, считая допустимыми состояния под номерами 2 и 3.

5. Найти оптимальные значения λ1 и μ1, обеспечивающие **максимальное** значение коэффициента готовности kг. Для этого доработать ранее написанную в п. 3 программу (не забыв сохранить ее под другим именем) с целью построения трехмерного графика kг(λ1, μ1) – зависимости коэффициента готовности kг от значений интенсивностей λ1 и μ1. Диапазоны варьирования λ1 и μ1 взять ± 50% от исходно заданных значений. Количество точек разбиения диапазона взять не менее пяти по каждому параметру λ1 и μ1. Программно и визуально (по графику) найти **максимальное**  значение kг, а также соответствующие ему оптимальные значения λ1 и μ1.

**Содержание отчета**

Отчёт по лабораторной работе должен содержать:

– ответы на контрольные вопросы;

– задание в соответствии с вариантом;

– текстовый и графический материал, отражающий этапы выполнения рабочего задания (п.1 – 5), в том числе листинги программ и выводы.

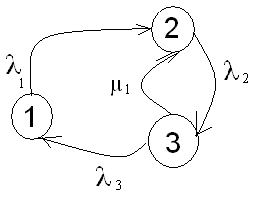
**Контрольные вопросы**

1. Как могут быть реализованы угрозы безопасности ПДн?
2. Что понимается под угрозами безопасности ПДн при их обработке в ИСПДн?
3. Какая градация исходной степени защищенности используются в соответствии с «Методикой определения актуальных угроз безопасности персональных данных…»?
4. Какая градация принята для характеристики вероятности реализации угрозы ПДн?
5. Сформулируйте правила составления СДУ Колмогорова.

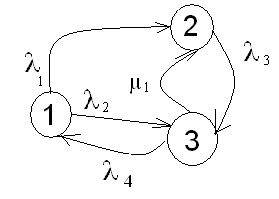
**ПРИЛОЖЕНИЕ А**

**Варианты заданий**

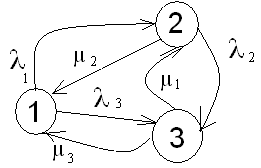
Вариант 1. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 0.1 λ1 = 0.2 λ2 = 0.6 λ3 = 0.7.



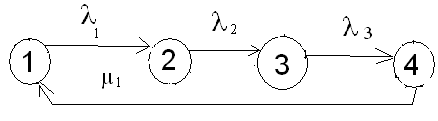
Вариант 2. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 0.5 λ1 = 0.2 λ2 = 0.6 λ3 = 0.7. λ4 = 0.75.



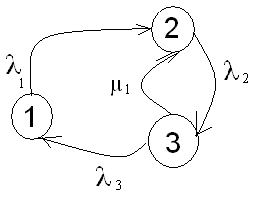
Вариант 3 Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 1 µ2 =3 µ3 =5 λ1 = 2 λ2 = 6 λ3 =7.



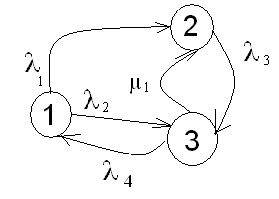
Вариант 4. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 10 λ1 =20 λ2 = 60 λ3 = 70.



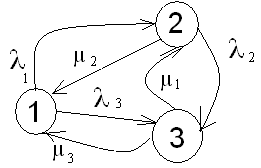
Вариант 5. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 0.2 λ1 = 0.37 λ2 = 0.16 λ3 = 0.12.



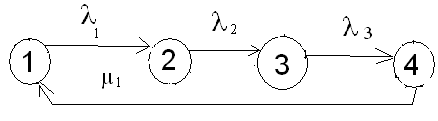
Вариант 6. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 0.33 λ1 = 0.75 λ2 = 0.6 λ3 = 0.7. λ4 = 0.75



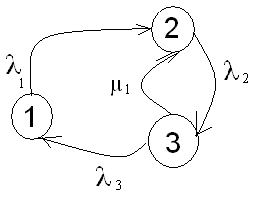
Вариант 7. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 2.2 µ2 =4 µ3 =5.2 λ1 = 2 λ2 = 6 λ3 =7.



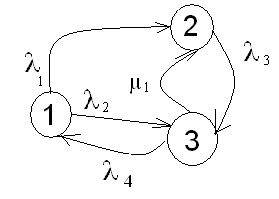
Вариант 8. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 22 λ1 =20 λ2 = 49 λ3 = 35.



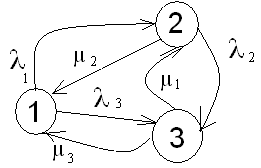
Вариант 9. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 0.29 λ1 = 0.21 λ2 = 0.91 λ3 = 0.67.



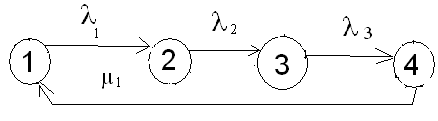
Вариант 10. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 0.32 λ1 = 0.18 λ2 = 0.47 λ3 = 0.17 λ4 = 0.29.



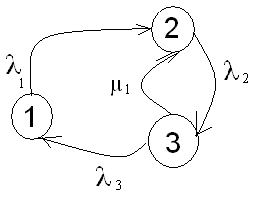
Вариант 11. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 5 µ2 =4 µ3 =8 λ1 = 6 λ2 = 6 λ3 =6.



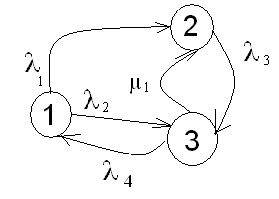
Вариант 12. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 112 λ1 =189 λ2 = 390 λ3 = 460.



Вариант 13. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 0.25 λ1 = 0.25 λ2 = 0.25 λ3 = 0.25.



Вариант 14. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 0.33 λ1 = 0.26 λ2 = 0.36 λ3 = 0.59. λ4 = 0.75



Вариант 15. Граф переходов состояний показан на рисунке. Интенсивности переходов (1/час): µ1 = 2 µ2 =3 µ3 =4 λ1 = 5 λ2 = 6 λ3 =7.

