УДК 004.43 **DOI: 10.18413/2518-1092-2019-4-4-0-5**

Какаев Д.В.
Маслова М.А.

АВТОМАТИЗАЦИЯ РАСЧЕТОВ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕТОДОМ ЭКСПЕРТНЫХ ОЦЕНОК НА PYTHON

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: 619deniss61999@gmail.com, mashechka-81@mail.ru

Аннотация
Анализ рисков позволяет принимать правильные решения по управлению компанией и ведения бизнеса. Риски, связанные с информационной безопасностью информации, являются одними из основных и рассматриваются в международных стандартах серии ISO/IEC 27000, и, в частности, национальные стандарты Российской Федерации серии ГОСТ Р ИСО/МЭК 27000. Для расчета рисков информационной безопасности выделяют две группы методов. Первая группа включает в себя методы позволяющие определить уровень риска с помощью уровню его соответствия выбранному набору требований. Вторая группа основывается на расчете вероятности реализации угроз, а также уровень ущерба от их реализации. При расчете могут использоваться статистические методы, методы экспертных оценок или элементы теории принятия решений. Статистические методы основываются на анализе уже имеющихся инцидентов в области информационной безопасности. На основе уже зарегистрированных событий рассчитывается вероятность реализации угрозы и уровень ущерба от ее реализации. В данной работе приводится пример автоматизации расчетов рисков информационной безопасности методом экспертных оценок.
Ключевые слова: риски; метод экспертных оценок; автоматизация; Python.

UDC 004.43

Kakaev D.V.
Maslova M.A.

AUTOMATION OF CALCULATIONS OF INFORMATION SECURITY RISKS BY EXPERT ASSESSMENTS ON PYTHON

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: 619deniss61999@gmail.com, mashechka-81@mail.ru

Abstract
Risk analysis allows you to make the right decisions on managing the company and doing business. Risks associated with information security of information are one of the main ones and are considered in international standards of the ISO / IEC 27000 series, and, in particular, national standards of the Russian Federation of the GOST R ISO/IEC 27000 series. Two groups of methods are distinguished for calculating in-formation security risks. The first group includes methods to determine the level of risk using the level of compliance with the selected set of requirements. The second group is based on the calculation of the probability of the implementation of threats, as well as the level of damage from their implementation. In the calculation, statistical methods, expert judgment methods or elements of decision theory can be used. Statistical methods are based on the analysis of already existing incidents in the field of in-formation security. Based on the events already recorded, the probability of the threat and the level of damage from its implementation is calculated. This paper gives an ex-ample of the automation of information security risk calculations using expert assessments.
Keywords: risks; expert assessment method; automation; Python.

ВВЕДЕНИЕ

Работа с рисками является неотъемлемой частью современного бизнеса. Анализ рисков позволяет принимать правильные решения по управлению компанией и ведения бизнеса. Риски, связанные с информационной безопасностью информации, являются одними из основных и рассматриваются в международных стандартах серии ISO/IEC 27000, и, в частности,

национальные стандарты Российской Федерации серии ГОСТ Р ИСО/МЭК 27000 [1]. Для обеспечения информационной безопасности в организациях, где обрабатывается государственная тайна имеется ряд нормативно-правовых актов и требований, в соответствии с которыми строится система защиты информации [2]. Для коммерческих организаций, где циркулирует коммерческая тайна, персональные данные и иная информация, утечка которой может нанести ущерб организации, нет строгих требований для построения системы защиты информации. Поэтому коммерческие организации основываются на анализе рисков информационной безопасности [3].

Риск информационной безопасности- возможность того, что некоторая угроза сможет воспользоваться уязвимостью актива и нанесет ущерб организации. Фактически риск представляет собой оценку, показывающая насколько эффективно система защиты информации противодействует реализации информационных угроз на данный момент [4].

Таким образом, на основе выявленных уязвимостей системы защиты, возможных угрозы и вероятности их реализации можно найти баланс между финансовыми затратами на модернизацию системы защиты и затратами при утечки защищаемой информации. Результат анализа рисков является наглядным представлением возможных уязвимостей и вероятности их реализации, ущерба от их реализации. Эти результаты в дальнейшем могут быть использованы для представления директору организации для принятия им решения по выделению средств на систему защиты и при построения этой системы защиты.[5]

ОСНОВНАЯ ЧАСТЬ

Для расчета рисков информационной безопасности выделяют две группы методов. Первая группа включает в себя методы позволяющие определить уровень риска с помощью уровня его соответствия выбранному набору требований. Этими требованиями могут быть: международные стандарты информационной безопасности, нормативно-правовые акты Российской Федерации в области зашиты информации, рекомендации к защите информации от крупных компаний, работающих в этой области и др. Зачастую требования выдвигаемые нормативными документами к организациям, в которых обрабатывается государственная тайна, для коммерческой организации будут немного преувеличены. Но тем не менее они могут использоваться как ориентир или использоваться с небольшими изменениями на усмотрение коммерческой организации. [6]

Вторая группа основывается на расчете вероятности реализации угроз, а также уровень ущерба от их реализации. Значение риска вычисляется отдельно для каждой атаки. И представляется как произведение вероятности проведения атаки на величину возможного ущерба от этой атаки. Владелец информации дает оценку ущербу, а группа экспертов выдвигает предположения и вычисляет вероятность атаки [7].

При расчете могут использоваться статистические методы, методы экспертных оценок или элементы теории принятия решений. Статистические методы основываются на анализе уже имеющихся инцидентов в области информационной безопасности. На основе уже зарегистрированных событий рассчитывается вероятность реализации угрозы и уровень ущерба от ее реализации. Но статистической информации об инцидентах не так много и часть умалчивается. Ведь организации выгоднее умолчать о какой-либо утечке чтобы избежать репутационных потерь [8].

При использовании метода экспертных оценок анализ результатов работы проводится группой экспертов, компетентных в области информационной безопасности. Эксперты определяют количественные или качественные уровни риска, основываясь на своем профессиональном опыте. Для вычисления значения риска безопасности более сложные алгоритмы обработки результатов работы группы экспертов применяются элементы теории принятия решений [9].

РЕЗУЛЬТАТЫ

Рассмотрим программную реализацию одного из методов расчета рисков с помощью Python.

Формируется группа компетентных экспертов, которые будут проводить оценку рисков. Каждому эксперту предлагается ввести свой критерий оценки значимости мнений экспертов и шкалу для него. Далее каждому эксперту предлагается оценить каждый из предложенных критериев, где 1 – самый важный, по их мнению, критерий, а последний – наименее важный. После этого начинает формироваться таблица: строки с оценками экспертов (Листинг 1, 01-07), строка сумма рангов (Листинг 1, 08-016), строка вес критериев (Листинг 1, 017-024). Полученные веса критериев будут использованы в дальнейших расчетах. Программа выводит результат в удобном для восприятия виде (Рис.1).

Листинг 1

```
01:    for i in range(usersAmount):
02:        data=[globals()['user_%s' % (i+1)]]
03:        for j in range(usersAmount):
04:            data.append(globals() ['user_%s_kriteriy_%s_rang' % (i+1,j+1)])
05:        data.append('')
06:        culc_rang_kriteriy.append(data)
07:    rangsumall=0
08:    data=['Сумма рангов']
09:    for i in range(usersAmount):
010:       globals()['rangsumkriteriy_%s' % (i+1)]=0
011:       for j in range(usersAmount):
012:           globals()['rangsumkriteriy_%s'                                    %
       (i+1)]+=float(globals()['user_%s_kriteriy_%s_rang' % (j+1,i+1)])
013:       data.append(globals()['rangsumkriteriy_%s' % (i+1)])
014:       rangsumall+=globals()['rangsumkriteriy_%s' % (i+1)]
015:   data.append(rangsumall)
016:   culc_rang_kriteriy.append(data)
017:   data=['Вес критерия']
018:   helpculcsum=0
019:   for i in range(usersAmount):
020:       helpculcsum+=rangsumall/globals()['rangsumkriteriy_%s' % (i+1)]
021:   for i in range(usersAmount):
022:       globals()['weight_%s'                                             %
       (i+1)]=round(rangsumall/globals()['rangsumkriteriy_%s'                %
       (i+1)]/helpculcsum,2)
023:       data.append(globals()['weight_%s' % (i+1)])
024:   culc_rang_kriteriy.append(data)
```

Эксперт\Критерий->	1	2	3	
Аня	1	2	3	
Саша	3	2	1	
Влад	2	3	1	
Сумма рангов	6	7	5	18.0
Вес критерия	0.33	0.28	0.39	

Рис. 1. Таблица расчет рангов критериев
Fig. 1. Table calculation of the ranks of the criteria

Каждому эксперту предлагается оценить всех экспертов, в том числе и себя, по ранее указанным критериям. Далее идут расчеты для таблицы расчета рангов экспертов: суммарные оценки каждого эксперта (Листинг 2, 01-013), расчет рангов экспертов путем умножения суммарной оценки эксперта по критерию на вес этого критерия (Листинг 2, 014-018), расчет веса экспертного мнения путем деления ранга эксперта на суммарное значение рангов (Листинг 2, 019-027). После этого формируется таблица расчета рангов экспертов (рис. 2) [10].

Листинг 2

```
01:   outer=[]
02:   for i in range(usersAmount):
03:       inner=[]
04:       inner.append(globals()['user_%s' % (i+1)])
05:       for j in range(usersAmount):
06:           inner.append (generalTable(i,j+1,usersAmount))
07:       inner.append('')
08:       inner.append('')
09:       outer.append(inner)
010:  inner=['Итого']
011:  for i in range(usersAmount+2):
012:      inner.append('')
013:  outer.append(inner)
014:  for i in range(usersAmount):
015:      buf=0
016:      for j in range(usersAmount):
017:          buf+=globals()['weight_%s' % (j+1)]*outer[i][j+1]
018:      outer[i][usersAmount+1]=round(buf,2)
019:  buf=0
020:  for i in range(usersAmount):
021:      buf+=outer[i][usersAmount+1]
022:  outer[usersAmount][usersAmount+1]=buf
023:  for i in range(usersAmount):
024:      globals()['user_%s_weight'                                          %
      (i+1)]=float(outer[i][usersAmount+1])/float(outer[usersAmount][usersAmou
      nt+1])
025:      outer[i][usersAmount+2]=      round(globals()['user_%s_weight'      %
      (i+1)],2)
026:  for i in range(usersAmount):
027:      outer[usersAmount][usersAmount+2]
```

Эксперт\Критерий	[1, 0.33]	[2, 0.28]	[3, 0.39]	Ранг эксперта	Вес. эксп. мнения
Аня	6	6	8	6.78	0.32
Саша	12	5	7	8.09	0.39
Влад	6	9	4	6.06	0.29
Итого				20.93	

Рис. 2. Таблица расчета рангов экспертов
Fig. 2. Expert rank calculation table

В итоге были рассчитаны все ранги экспертного мнения каждого участника, которые будут использоваться дальше для определения актуальных угроз. Данный расчет является универсальным для метода экспертных оценок и может использоваться в любых других случаях, с использованием метода экспертных оценок.

На этом этапе перед экспертами стоит задача формирования списка возможных рисков в оцениваемой области. Для этого каждый эксперт предлагает 5-7 рисков, которым следовало бы уделить внимание в данной ситуации, затем риски обсуждаются, несущественные риски отбрасываются, формулируется общий список. Для анализа должен быть составлен список из 15 – 20 рисков. Каждому риску присваивается свой единый для всех экспертов код. Этот список вводится в программу для дальнейшей оценки.

В пункте оценки критериев значимости рисков каждый эксперт предлагает один критерий важности. Полученным критериям назначается номер для удобства и формируется таблица.

Далее происходит ранжирование критериев важности. Каждому эксперту предлагается оценить выбранный на предыдущем этапе критерии в порядке значимости, где 1 – самый важный критерий, последний – наименее важный (Листинг 3). Оценки экспертов заносятся в таблицу и выводятся на экран индивидуально для каждого эксперта.

Листинг 3

```
01:   for i in range( usersAmount):
02:       globals()['users_%s_table(kriteriy-rang)' % (i+1)]=[]
03:       for j in range(len(risk_kriteriy_matrix)):
04:           buffer=[]
05:           buffer.append(globals()['risk_kriteriy_%s' % (j+1)])
06:           globals()['users_%s_kriteriy_%s_rang'                    %
      (i+1,j+1)]=input(str(globals()['user_%s'   %   (i+1)])+',   введите   ранг
      критерия '+str(globals()['risk_kriteriy_%s' % (j+1)]))
07:           buffer.append      (globals()['users_%s_kriteriy_%s_rang'      %
      (i+1,j+1)])
08:           globals()['users_%s_table(kriteriy-rang)'                    %
      (i+1)].append(buffer)
09:       tableHeaders=['Критерий','Ранг']
010:      print(tabulate  (globals()['users_%s_table(kriteriy-rang)'  %  (i+1)],
      headers=tableHeaders, tablefmt="grid"))
```

На этапе расчета рангов и весов критериев важности рисков производятся расчеты и формируются в таблицу. Происходит расчет рангов каждого критерия путем суммирования для всех экспертов произведений веса экспертного мнения и его оценки соответствующего критерия важности (Листинг 6, 011-017). Расчет весов критериев важности рассчитывается как частное от вспомогательного расчета соответствующего критерия и суммарному значению вспомогательных расчетов всех рангов (Листинг 6, 025-030).

Листинг 4

```
01:   calculation_rang_tabel=[]
02:   for i in range(usersAmount):
03:       buffer=[]
04:       buffer.append(globals()['user_%s' % (i+1)])
05:       buffer.append(globals()['user_%s_weight' % (i+1)])
06:       for j in range(usersAmount):
07:           buffer.append(globals()['users_%s_kriteriy_%s_rang'            %
      (i+1,j+1)])
08:       buffer.append('')
09:       calculation_rang_tabel.append(buffer)
010:  buffer=['Ранг', '']
011:  for i in range(usersAmount):
012:      globals()['kriteriy_%s_rang' % (i+1)]=0
013:      for j in range(usersAmount):
014:          globals()['kriteriy_%s_rang'                                  %
      (i+1)]+=float(globals()['user_%s_weight'                              %
      (j+1)])*float(globals()['users_%s_kriteriy_%s_rang' % (j+1,i+1)])
015:      buffer.append(globals()['kriteriy_%s_rang' % (i+1)])
016:  buffer.append('')
017:  calculation_rang_tabel.append(buffer)
018:  res=0
019:  for i in range(usersAmount):
020:      res+=globals()['kriteriy_%s_rang' % (i+1)]
021:  calculation_rang_tabel[usersAmount][usersAmount+2]=round(res,2)
022:  helpcalc=0
023:  for i in range(usersAmount):
024:
      helpcalc+=calculation_rang_tabel[usersAmount][usersAmount+2]/globals()['
      kriteriy_%s_rang' % (i+1)]
```

```
025:  buffer=['Вес критерия','']
026:  for i in range(usersAmount):
027:      globals()['kriteriy_%s_weight'                                    %
      (i+1)]=calculation_rang_tabel[usersAmount][usersAmount+2]/globals()['kri
      teriy_%s_rang' % (i+1)]/helpcalc
028:      buffer.append(globals()['kriteriy_%s_weight' % (i+1)])
029:  buffer.append('')
030:  calculation_rang_tabel.append(buffer)
```

В этом пункте экспертам необходимо оценить выбранные риски по всем критериям в порядке значимости, где 1 – самый важный риск, последний – наименее важный.

Для каждого эксперта формируется таблица, которая состоит из рисков и соответствующих им оценок по каждому критерию (Листинг 5, 01-09), расчет рангов каждого критерия путем суммы произведений веса критерия на соответствующую ему оценку (Листинг 5, 010-015). На основе рассчитанных рангов каждому критерию назначается приоритет: с возрастанием ранга возрастает приоритет (Листинг 5, 015-023).

Листинг 5

```
01:    for i in range(usersAmount):
02:        table_marking=[]
03:        mas=[]
04:        for j in range(len(risk_tabel)):
05:            buffer=[]
06:            globals()['user_%s_risk_%ssumrang' % (i+1,j+1)]=0
07:            buffer.append(j+1)
08:            for g in range(usersAmount):
09:                buffer.append(globals()  ['user_%s_risk_%s_kriteriy_%s_mark'  %
      (i+1,j+1,g+1)])
010:           for jj in range(usersAmount):
011:               globals()['user_%s_risk_%ssumrang'                          %
      (i+1,j+1)]+=float(globals()['user_%s_risk_%s_kriteriy_%s_mark'            %
      (i+1,j+1,jj+1)])*float(globals()['kriteriy_%s_weight' % (jj+1)])
012:           mas.append(globals()['user_%s_risk_%ssumrang' % (i+1,j+1)])
013:           buffer.append(globals()['user_%s_risk_%ssumrang' % (i+1,j+1)])
014:           buffer.append('')
015:           table_marking.append(buffer)
016:       sortedmas=sorted(mas)
017:       for i1 in range(len(mas)):
018:           for i2 in range(len(mas)):
019:               if mas[i1]==sortedmas[i2]:
020:                   globals()['user_%s_risk_%s_mark'                        %
      (i+1,i1+1)]=sortedmas.index(mas[i1])+1
021:                   table_marking[i1][usersAmount+2]=
      sortedmas.index(mas[i1])+1
022:                   sortedmas[i2]=0
023:                   break
```

Далее необходимо объединить оценки всех экспертов и на их основе выделить актуальные риски. Для этого формируется таблица, в которой суммируются приоритеты по каждому риску для всех экспертов (Листинг 6, 01-06). Далее происходит расчет рангов путем умножения соответствующего значения приоритета на вес мнения эксперта (Листинг 6, 07-013). На основе рассчитанных рангов каждому критерию назначается приоритет: с возрастанием ранга возрастает приоритет (Листинг 6, 014-019).

Листинг 6

```
01:   table_marking_general=[]
02:   mas=[]
03:   for i in range(len(risk_tabel)):
```

```
04:         buffer=[]
05:         buffer.append(globals()['risk_%s' % (i+1)])
06:         globals()['rangsum_risk_%s' % (i+1)]=0
07:         for j in range(usersAmount):
08:             buffer.append(globals()['user_%s_risk_%s_mark' % (j+1,i+1)])
09:             globals()['rangsum_risk_%s' % (i+1)]+=globals()['user_%s_weight'
      % (j+1)]*globals()['user_%s_risk_%s_mark' % (j+1,i+1)]
010:        buffer.append(globals()['rangsum_risk_%s' % (i+1)])
011:        mas.append(globals()['rangsum_risk_%s' % (i+1)])
012:        buffer.append('')
013:        table_marking_general.append(buffer)
014:        for i1 in range(len(mas)):
015:            for i2 in range(len(mas)):
016:                if mas[i1]==sorted(mas)[i2]:
017:                    table_marking_general[i1][usersAmount+2]=
      sorted(mas).index(mas[i1])+1
018:                    sortedmas[i2]=0
019:                    break
```

4.2 Оценка рисков по критериям (коллективное мнение)

Риск	Аня (0.32)	Саша (0.39)	Влад (0.29)	Расчет рангов	Приоритеты
риск 1	8	6	13	8.67	11
риск 2	9	5	5	6.28	4
риск 3	4	12	6	7.7	6
риск 4	13	9	12	11.15	13
риск 5	12	3	11	8.2	10
риск 6	10	11	2	8.07	9
риск 7	14	1	14	8.93	12
риск 8	6	8	4	6.2	3
риск 9	7	14	1	7.99	8
риск 10	3	2	7	3.77	1
риск 11	15	13	9	12.48	15
риск 12	1	4	8	4.2	2
риск 13	5	10	3	6.37	5
риск 14	11	15	10	12.27	14
риск 15	2	7	15	7.72	7

Рис. 3. Таблица оценок рисков
Fig. 3. Risk Assessment Table

Из полученной таблицы рисков необходимо выбрать 10 с наименьшим рангом. Это и будет перечень наиболее важных рисков по исследуемому вопросу.

ЗАКЛЮЧЕНИЕ

В итоге работы написана программа для автоматизации расчетов рисков при оценке их методом экспертных оценок. Представленные элементы кода, который можно модернизировать под свои индивидуальные нужды при расчетах. Таким образом, программа не только упрощает однотипную и необходимую работу, но может быть подстроена для работы в других расчетах, что увеличивает ее область применения. Правильность самих результатов будет зависеть от компетентности выбранных для проведения оценок экспертов.

Список литературы

1. ГОСТ Р ИСО/МЭК 27000, 2012 г. URL: http://docs.cntd.ru/document/1200102762 (дата обращения 10.12.2019)

2. Приказ об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, 2013 г. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 10.12.2019)

3. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов 3-е изд., стер. – М.: Флинта, 2011. – 224 с. URL: http://www.biblioclub.ru/book/93351/(дата обращения 10.12.2019)

4. Варфоломеев А.А. Управление информационными рисками: Учеб. пособие. – М.: РУДН, 2008. – 158 с. (дата обращения 10.12.2019)

5. Милославская, Н.Г. Управление рисками информационной безопасности: учеб. пособие / М.Ю. Сенаторов, А.И. Толстой, Н.Г. Милославская. – М.: Горячая линия – Телеком, 2013. – 131 с. – (дата обращения 10.12.2019)

6. Киселева И.А., Искаджян С.О. Информационные риски: методы оценки и анализа // ИТ-портал, 2017. №2(14). URL: http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/ (дата обращения 10.12.2019)

7. Набатова, Д.С. Математические и инструментальные методы поддержки принятия решений: учебник и практикум для бакалавриата и магистратуры / Д. С. Набатова, 2017. – 292 с. – URL: https://www.biblio-online.ru/book/0AB93023-5D55-4432-B8F1-34FE55F7BE10(дата обращения 10.12.2019)

8. Калинин М.О. Теория и системы управления информационной безопасностью. Анализ рисков информационной безопасности. Лабораторный практикум. – СПб.: Издательство Политехнического университета, 2010. (дата обращения 10.12.2019)

9. Баранова Е.К., Барабаш А.В. Моделирование системы защиты информации. – М.: РИОР ИНФРА-М, 2014. – 120 с. (дата обращения 10.12.2019)

10. Документация Python для сетевых инженеров. URL: https://pyneng.readthedocs.io/ru/latest/book/12_useful_modules/tabulate.html(дата обращения 10.12.2019)

References

1. GOST R ISO / IEC 27000, 2012. URL: http://docs.cntd.ru/document/1200102762 (data accessed 10.12.2019)

2. Order on the approval of requirements for the protection of information not constituting state secrets contained in state information systems, 2013 URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (data accessed 10.12.2019)

3. Averchenkov V.I., Rytov M.Yu., Kondrashin G.V., Rudanovsky M.V. Information Security Systems in Leading Foreign Countries: A Textbook for High Schools 3rd ed., Sr. – M.: Flint, 2011. – 224 p. URL: http://www.biblioclub.ru/book/93351/ (data accessed 10.12.2019)

4. Varfolomeev A.A. Information Risk Management: Textbook. allowance. – M.: RUDN University, 2008. -158 p. (data accessed 10.12.2019)

5. Miloslavskaya, N.G. Information Security Risk Management: Textbook. allowance / M.Yu. Senators, A.I. Tolstoy, N.G. Miloslavskaya. – M.: Hot line – Telecom, 2013. – 131 p. – (data accessed 10.12.2019)

6. Kiseleva I.A., Iskadzhyan S.O. Information risks: assessment and analysis methods // IT portal, 2017. No. 2 (14). URL: http://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/ (data accessed 10.12.2019)

7. Nabatova, D.S. Mathematical and instrumental methods of decision support: a textbook and a workshop for undergraduate and graduate programs / D.S. Nabatova. – M.: Yurayt Publishing House, 2017. – 292 p. – URL: https://www.biblio-online.ru/book/0AB93023-5D55-4432-B8F1-34FE55F7BE10 (data accessed 10.12.2019)

8. Kalinin M.O. Theory and information security management systems. Risk analysis of information security. Laboratory workshop. – St. Petersburg: Publishing House of the Polytechnic University, 2010. (data accessed 10.12.2019)

9. Baranova E.K., Barabash A.V. Modeling information security system. – M.: RIOR INFRA-M, 2014. – 120 p. (data accessed 10.12.2019)

10. Python documentation for network engineers. URL: https://pyneng.readthedocs.io/ru/latest/book/12_useful_modules/tabulate.html (data accessed 10.12.2019)

Какаев Денис Валерьевич, студент 4 курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, аспирант, старший преподаватель кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Kakaev Denis Valerievich, 4th year student of the Department Information security, Institute of Radioelectronics and information security
Maslova Maria Aleksandrovna, postgraduate student, senior lecturer of the Department Information security, Institute of Radioelectronics and information security