**باسمه تعالی**

****

**رمزنگاری پیشرفته**

**دکتر سلماسی‌زاده - دکتر احمدی**

**تمرین سری اول – بخش اول**

**نحوه عملکرد سامانه تدارکات الکترونیکی دولت (ستاد)**

**پوریا دادخواه**

**401201381**

* **معرفی**

ﺳﺎﻣﺎﻧﻪي ﺗﺪارﮐﺎت اﻟﮑﺘﺮوﻧﯿﮏ دوﻟﺖ (ﺑﻪ اﺧﺘﺼﺎر: ﺳﺘﺎد)، ﺳﺎﻣﺎﻧﻪاي دوﻟﺘﯽ-ﺣﺎﮐﻤﯿﺘﯽ اﺳﺖ ﮐﻪ وﻇﯿﻔﻪ ﺗﺠﻤﯿﻊ و ﺑﻬﺮهورﺳﺎزي ﺑﺨﺸﯽ از ﻣﻌﺎﻣﻼت ﺗﺠﺎري دوﻟﺖ را ﺑﺮﻋﻬﺪه دارد. اﯾﻦ ﺳﺎﻣﺎﻧﻪ ﺑﺮ ﻣﺤﻮر دﺳﺘﺮﺳﯽ آزاد ﺑﻪ اﻃﻼﻋﺎت و ﺣﻖ ﺑﺮاﺑﺮ ﺑﺮاي ﺷﻬﺮوﻧﺪان اﯾﺠﺎد ﺷﺪه و ﺳﺎزﻣﺎن ﻫﺎ و ﻧﻬﺎدﻫﺎي ﻣﺮﺑﻮﻃﻪ را ﻗﺎدر ﻣﯽﮐﻨﺪ ﻣﻌﺎﻣﻼت ﺧﻮد را در ﺑﺴﺘﺮي اﻣﻦ و ﺷﻔﺎف اﻧﺠﺎم دﻫﻨﺪ.

اﻫﺪاف اﺻﻠﯽ اﯾﺠﺎد اﯾﻦ ﺳﺎﻣﺎﻧﻪ و ﺧﻮاص آن را را ﻣﯽ ﺗﻮان در ﮐﻠﯿﺎت زﯾﺮ ﺑﺮﺷﻤﺮد.

1 ﺷﻔﺎف ﺷﺪن ﻣﻌﺎﻣﻼت: ﺑﻮاﺳﻄﻪ اﻟﺘﺰام ﻧﻬﺎدﻫﺎ در اﺳﺘﻔﺎده از اﯾﻦ ﺳﺎﻣﺎﻧﻪ، اﻣﮑﺎن ﻓﺴﺎد اﻋﻢ از واﮔﺬاري ﺧﺎرج از ﺿﻮاﺑﻂ، زد و ﺑﻨﺪ، دﻻﻟﯽ و ... ﺣﺪاﻗﻞ ﺷﺪه و ﻋﻼوه ﺑﺮ ﻧﻬﺎدﻫﺎي ﻧﻈﺎرﺗﯽ ﻣﺜﻞ ﺳﺎزﻣﺎن ﺑﺎزرﺳﯽ و ﺗﻌﺰﯾﺮات ، اﻣﮑﺎن رﺻﺪ ﻋﻤﻮﻣﯽ ﻧﯿﺰ ﻓﺮاﻫﻢ اﺳﺖ.

2 اﯾﻤﻨﯽ ﻣﻌﺎﻣﻠﻪ: ﺑﻮاﺳﻄﻪ رﻋﺎﯾﺖ ﭘﺮﺗﮑﻞ اﯾﻤﻦ در ﮐﻞ ﻓﺮاﯾﻨﺪ ﻣﻌﺎﻣﻠﻪ، اﻣﮑﺎن اﺳﺘﻔﺎده از ﺧﻼﻫﺎي ﻗﺎﻧﻮﻧﯽ، ﮐﻼﻫﺒﺮداري و... ﮐﺎﻫﺶ دارد.

3 ﺟﻠﻮﮔﯿﺮي از ﻗﺎﭼﺎق: ﺑﻮاﺳﻄﻪ اﺳﺘﻔﺎده از اﯾﺮان ﮐﺪ" ﺳﻼﻣﺖ ﮐﺎﻻ ﺗﻀﻤﯿﻦ ﺷﺪه و ﻣﮑﺎن ورود ﮐﺎﻻي ﻗﺎﭼﺎق ﺑﻪ ﻣﺼﺎرف دوﻟﺖ ﮐﺎﻫﺶ ﻣﯿﺎﺑﺪ.

4 ﮐﺎﻫﺶ ﻫﺰﯾﻨﻪ ﻫﺎي دوﻟﺖ: ﺑﺎ ﻋﻤﻮﻣﯽ ﺷﺪن ﻓﺮاﯾﻨﺪﻫﺎ و رﻗﺎﺑﺖ ﺑﯿﻦ اﺷﺨﺎص ﺑﺮاي اﻧﺘﺨﺎب ﺑﻪ ﻋﻨﻮان ﻃﺮف ﻣﻌﺎﻣﻠﻪ، ﻣﻨﺎﻓﻊ دوﻟﺖ ﺑﯿﺸﯿﻨﻪ ﻣﯽ ﮔﺮدد.

5 دﺳﺘﺮﺳﯽ ﺑﺮاﺑﺮ: ﺑﺎ اﯾﻦ ﺳﺎﻣﺎﻧﻪ اﻣﮑﺎن و ﻓﺮﺻﺖ ﺑﺮاي ﻫﻤﻪ ﺷﻬﺮوﻧﺪان ﺑﺮاﺑﺮ ﻣﯽ ﺷﻮد و راﻧﺖ اﻃﻼﻋﺎﺗﯽ از ﺑﯿﻦ ﻣﯽ رود.

* **ساختار سایت**

ﺳﺎﯾﺖ ﺷﺎﻣﻞ ﺳﻪ ﺑﺨﺶ اﺻﻠﯽ اﺳﺖ. ﺧﺮﯾﺪ ﺟﺰﯾﯽ و ﻣﺘﻮﺳﻂ، ﻣﻨﺎﻗﺼﻪ و ﻣﺰاﯾﺪه. ﻫﺮ ﮐﺪام از اﯾﻦ ﻣﻮارد ﺑﻪ زﯾﺮ ﺑﺨﺶ ﻫﺎﯾﯽ ﺗﻘﺴﯿﻢ ﻣﯽ ﺷﻮﻧﺪ.



ﺷﮑﻞ1: ﺑﺨﺶ ﻫﺎي اﺻﻠﯽ

ﺧﺮﯾﺪ ﺟﺰﯾﯽ و ﻣﺘﻮﺳﻂ: اﯾﻦ ﺑﺨﺶ ﻣﺮﺑﻮط ﺑﻪ ﮐﺎﻻﻫﺎﯾﯽ اﺳﺖ ﮐﻪ ﺳﺎزﻣﺎن ﻣﺮﺑﻮﻃﻪ ﻗﺼﺪ واﮔﺬاري آن را داﺷﺘﻪ و ﻫﻤﭽﻨﯿﻦ ﮐﺎﻻ ﯾﺎ ﺧﺪﻣﺘﯽ ﮐﻪ ﻣﺘﻘﺎﺿﯽ ﺑﮑﺎرﮔﯿﺮي اﺳﺖ. در اﯾﻦ ﺑﺨﺶ ﺑﺎ ﻋﻨﻮان ﺗﺎﻣﯿﻦ ﮐﻨﻨﺪه ﯾﺎ ﺧﺮﯾﺪار ﻣﯽ ﺗﻮان اﻗﺪام ﮐﺮد.

ﺑﻪ ﻃﻮر ﻣﻌﻤﻮل ﺗﻘﺎﺿﺎﻫﺎ روزﻫﺎي ﻣﻌﯿﻨﯽ در ﺳﺎﻣﺎﻧﻪ ﺑﺎﻗﯽ ﻣﺎﻧﺪه و در ﻧﻬﺎﯾﺖ از ﺑﯿﻦ ﻣﺘﻘﺎﺿﯿﺎن، ﻃﺮف ﻗﺮارداد اﻧﺘﺨﺎب ﻣﯽ ﺷﻮد.



ﺷﮑﻞ2: ﺑﺨﺶ ﺧﺮﯾﺪ ﺟﺰﯾﯽ و ﻣﺘﻮﺳﻂ

ﻣﻨﺎﻗﺼﻪ: اﯾﻦ ﺑﺨﺶ از ﺳﺎﻣﺎﻧﻪ ﺳﺘﺎد ﺧﺮﯾﺪﻫﺎي ﻋﻤﺪه دﺳﺘﮕﺎه ﻫﺎي اﺟﺮاﯾﯽ را ﺑﺎ اﺳﺘﻔﺎده از ﺑﺮﮔﺰاري اﻧﻮاع ﻣﻨﺎﻗﺼﻪ ﻫﺎ ﻃﺒﻖ ﻗﺎﻧﻮن ﺑﺮﮔﺰاري ﻣﻨﺎﻗﺼﺎت اﻣﮑﺎن ﭘﺬﯾﺮ ﻣﯿﮑﻨﺪ. ﻣﺪﯾﺮان و ﻣﺴﺌﻮﻻن روي ﺑﺮﮔﺰاري اﯾﻦ ﻣﻨﺎﻗﺼﻪ ﻫﺎ در ﺳﺎﯾﺖ ﺳﺘﺎد ﻧﻈﺎرت دارﻧﺪ ﮐﻪ ﺗﺎﺧﯿﺮي در روﻧﺪ اﺟﺮاي آن ﻫﺎ اﯾﺠﺎد ﻧﺸﻮد. ﻫﻤﭽﻨﯿﻦ ﻧﻬﺎدﻫﺎي ﻧﻈﺎرﺗﯽ ﺑﺮ ﻣﻨﺎﻗﺼﻪ ﻫﺎ و ﻣﻌﺎﻣﻼت ﻧﻈﺎرت دﻗﯿﻖ دارﻧﺪ ﮐﻪ از ﺗﺨﻠﻔﺎت آﮔﺎه ﺷﻮﻧﺪ.

ﻣﺮاﺣﻞ ﺑﺮﮔﺰاري ﻣﻨﺎﻗﺼﻪ ﻫﺎ در ﺳﺎﯾﺖ ﺳﺘﺎد اﯾﺮان ﺑﻪ ﺷﮑﻞ زﯾﺮ اﻧﺠﺎم ﻣﯿﮕﯿﺮد.

1. اﻧﻮاع ﻣﻨﺎﻗﺼﻪ ﻫﺎي ﻋﻤﻮﻣﯽ و ﻣﺤﺪود ﮐﺎﻻ/ ﺧﺪﻣﺎت ﺑﺎ ﻓﻬﺮﺳﺖ ﺑﻬﺎ و ﺑﺪون ﻓﻬﺮﺳﺖ ﺑﻬﺎ ﺛﺒﺖ و ﻣﻨﺘﺸﺮ ﻣﯿﺸﻮﻧﺪ

2. ﻓﺮاﺧﻮان ﻫﺎي ارزﯾﺎﺑﯽ ﮐﯿﻔﯽ ﻧﯿﺰ ﺛﺒﺖ و ﻣﻨﺘﺸﺮ ﻣﯿﺸﻮﻧﺪ 3. اﺳﻨﺎد ﻣﺸﺎﻫﺪه و داﻧﻠﻮد ﻣﯿﺸﻮﻧﺪ

4. ارﺳﺎل ﭘﯿﺸﻨﻬﺎدﻫﺎ ﺑﻪ وﺳﯿﻠﻪ ﭘﺎﮐﺖ ﻫﺎي اﻟﻒ، ب و ج 5. ارﺳﺎل ﭘﺎﺳﺦ اﺳﺘﻌﻼم

6. اﺻﻼح ﻣﻨﺎﻗﺼﻪ ﻫﺎي ﻣﻨﺘﺸﺮ ﺷﺪه 7. ﺑﺎزﭘﺲ ﮔﯿﺮي ﭘﯿﺸﻨﻬﺎدﻫﺎ و ارﺳﺎل ﻣﺠﺪد

8. ﺑﺎزﮔﺸﺎﯾﯽ ﭘﺎﮐﺖ ﻫﺎ ﺑﺎ اﻣﻀﺎي اﻟﮑﺘﺮوﻧﯿﮑﯽ ﺗﻤﺎﻣﯽ اﻋﻀﺎي ﮐﻤﯿﺴﯿﻮن ﻣﻨﺎﻗﺼﻪ

9. ﺑﺮرﺳﯽ ﭘﺎﮐﺖ ﻫﺎ ﺗﻮﺳﻂ ﮐﻤﯿﺘﻪ ﻓﻨﯽ در ﻣﺮاﺣﻞ ﻣﺨﺘﻠﻒ 10. ﺗﻬﯿﻪ ﻟﯿﺴﺖ ﮐﻮﺗﺎه

11. اﻋﻼم ﺑﻪ ﺑﺮﻧﺪه 12. ﭘﺬﯾﺮش ﺑﺮﻧﺪه

13. اﻧﻌﻘﺎد ﻗﺮارداد ﺑﺎ اﻣﻀﺎي اﻟﮑﺘﺮوﻧﯿﮑﯽ ﻣﺴﺌﻮﻟﯿﻦ دﺳﺘﮕﺎه و ﺗﺎﻣﯿﻦ ﮐﻨﻨﺪه

14. ارﺳﺎل و درﯾﺎﻓﺖ ﮐﺎﻻ/ ﺻﻮرت وﺿﻌﯿﺖ ﺧﺪﻣﺎت

15. اﻧﺠﺎم اﻧﻮاع ﭘﺮداﺧﺖ در ﻗﺎﻟﺐ ﭘﯿﺶ ﭘﺮداﺧﺖ، ﻋﻠﯽ اﻟﺤﺴﺎب و ﻗﻄﻌﯽ )ﺑﻪ ﺻﻮرت اﻟﮑﺘﺮوﻧﯿﮑﯽ/ﻏﯿﺮ اﻟﮑﺘﺮوﻧﯿﮑﯽ( ﺑﺎ اﻣﻀﺎي اﻟﮑﺘﺮوﻧﯿﮑﯽ ﺻﺎﺣﺒﺎن اﻣﻀﺎء از ﻃﺮﯾﻖ ﺳﺎﻣﺎﻧﻪ ﻣﻨﺎﻗﺼﻪ

در اﯾﻦ ﺑﺨﺶ ﻧﯿﺰ اﻣﮑﺎن اﻗﺪام ﺑﻪ ﻋﻨﻮان ﻣﻨﺎﻗﺼﻪﮔﺬار و ﻣﻨﺎﻗﺼﻪﮔﺮ وﺟﻮد دارد.



ﺷﮑﻞ3: دو ﺣﺎﻟﺖ ﺷﺮﮐﺖ در ﻣﻨﺎﻗﺼﻪ

ﻣﺰاﯾﺪه: ﻓﺮاﯾﻨﺪ ﻣﺰاﯾﺪه ﺑﻪ اﯾﻦ ﺷﮑﻞ اﺳﺖ ﮐﻪ اﺑﺘﺪا ﻓﺮوﺷﻨﺪه ﺣﺪاﻗﻞ ﻗﯿﻤﺖ اﻣﻮال ﺧﻮد را ﺑﺮاي ﻓﺮوش ﻣﺸﺨﺺ ﻣﯿﮑﻨﺪ، ﺑﻌﺪ از آن ﺧﺮﯾﺪاران ﻗﯿﻤﺖ ﻫﺎي ﭘﯿﺸﻨﻬﺎدي ﺧﻮد را ﺑﺮاي ﺧﺮﯾﺪ آن اﻣﻮال ﻣﯿﺪﻫﻨﺪ. ﻗﯿﻤﺘﯽ ﮐﻪ ﭘﯿﺸﻨﻬﺎد ﻣﯿﺸﻮد ﺑﺎﯾﺪ ﺑﺮاﺑﺮ ﯾﺎ ﺑﯿﺸﺘﺮ از ﻗﯿﻤﺖ ﻣﺸﺨﺺ ﺷﺪه ﺗﻮﺳﻂ ﻓﺮوﺷﻨﺪه ﺑﺎﺷﺪ. در ﻧﻬﺎﯾﺖ ﮐﺎﻻ ﺑﺎ ﺑﺎﻻﺗﺮﯾﻦ ﻗﯿﻤﺘﯽ ﮐﻪ ﭘﯿﺸﻨﻬﺎد ﺷﺪه اﺳﺖ ﺧﺮﯾﺪاري ﺧﻮاﻫﺪ ﺷﺪ.

اﯾﻨﺠﺎ ﯾﮏ دﺳﺘﻪ ﺑﻨﺪي روي ﻣﺰاﯾﺪه اﻣﻮال ﺗﻤﻠﯿﮑﯽ و ﻣﺰاﯾﺪه دﺳﺘﮕﺎه اﺟﺮاﯾﯽ وﺟﻮد دارد و ﭘﺲ از اﻧﺘﺨﺎب، اﻧﺘﺨﺎب ﻧﻘﺶ ﻫﺎي ﻣﺰاﯾﺪهﮔﺮ و ﻣﺰاﯾﺪهﮔﺰار در دﺳﺘﺮس اﺳﺖ.



ﺷﮑﻞ4: ﺗﻀﻤﯿﻦ اﻣﻨﯿﺖ ﭘﺎﮐﺖ ﻫﺎي ﻣﻨﺎﻗﺼﻪ

* **امنیت**

در ﺑﺤﺚ ﺗﺎﻣﯿﻦ اﻣﻨﯿﺖ ﻣﻌﺎﻣﻠﻪ ﻋﻮاﻣﻞ ﻣﺘﻌﺪدي اﺛﺮﮔﺬارﻧﺪ. در اﯾﻨﺠﺎ ﺑﻪ ﺑﺮرﺳﯽ دو ﻣﻮرد اﮐﺘﻔﺎ ﻣﯽ ﺷﻮد.

* رﻣﺰﮔﺬاري ﭘﺎﮐﺖﻫﺎ: ﺑﺮاي ﺗﻀﻤﯿﻦ ﺳﻼﻣﺖ ﻣﻨﺎﻗﺼﻪ ﻻزم اﺳﺖ ﮐﻪ ﮐﻪ ﻣﺤﺘﻮاي ﭘﺎﮐﺖﻫﺎ ﻗﺒﻞ از ﻣﻮﻋﺪ ﺑﺎزﮔﺸﺎﯾﯽ اﻓﺸﺎ ﻧﺸﻮد ﮐﻪ ﺑﺤﺚ رﻣﺰﻧﮕﺎري اﯾﻦ ﺑﺨﺶ ﺑﺮ ﻋﻬﺪه اﺳﺘﺎﻧﺪارد FIPS 140-2 (Federal Information Processing Standards) می‌باشد.
* اﻣﻀﺎ دﯾﺠﯿﺘﺎل: اﺣﺮاز اﺻﺎﻟﺖ اﻓﺮاد ﻃﺮف ﻗﺮارداد ﺑﻮﺳﯿﻠﻪ اﻣﻀﺎ دﯾﺠﯿﺘﺎل ﻣﺒﺘﻨﯽ ﺑﺮ رﻣﺰﻧﮕﺎري ﮐﻠﯿﺪ ﻋﻤﻮﻣﯽ اﻧﺠﺎم ﻣﯽ ﺷﻮد. در اﯾﻦ ﻓﺮاﯾﻨﺪ ﻓﺮد ﻣﺘﻘﺎﺿﯽ ﺑﻮﺳﯿﻠﻪي ﮐﻠﯿﺪ ﺧﺼﻮﺻﯽ ﺧﻮد، ﻣﺘﻌﻬﺪ ﻣﯽ ﮔﺮدد.

ﻻزم ﺑﻪ ذﮐﺮ اﺳﺖ در اﯾﻦ روش از ﺗﻮﮐﻦﻫﺎ اﺳﺘﻔﺎده ﻣﯽ ﺷﻮد.



ﺷﮑﻞ 5: ﺗﻮﮐﻦ ﺑﻪ ﻋﻨﻮان ﮐﻠﯿﺪ ﺧﺼﻮﺻﯽ