**О‘ZBEKISTON RESPUBLIKASI**

**RAQAMLI TEXNOLOGIYALAR VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**FARG‘ONA FILIALI**

**“TASDIQLAYMAN”**

*Muhammad al-Xorazmiy nomidagi*

*TATU Farg‘ona filiali*

*О‘IB direktor о‘rinbosari*

**\_\_\_\_\_\_\_\_\_ T.M.Abdullayev**

“27” yanvar 2024 yil

**Bitiruvchi kurs bakalavr talablari uchun ixtisoslik fanlaridan yakuniy davlat attestatsiya sinovlari**

**DASTURI**



*Ta’lim yо‘nalishi: 5330300– Axborot xavfsizligi (sohalar bo‘yicha)*

**Farg‘ona – 2024**

Ushbu dastur О‘zbekiston Respublikasi Oliy va о‘rta maxsusu ta’lim vazirining 2018 yil 12 dekabrdagi 1963-2sonli “О‘zbekiston Respublikasi Oliy ta’lim muassasalari bitiruvchilarining yakuniy davlat attestatsiyasi tо‘g‘risidagi nizomga о‘zgartirishlar kiritish haqida”gi buyrug‘i talablari asosida ishlab chiqildi.

Ushbu dasturda 5330300– Axborot xavfsizligi (sohalar bo‘yicha) bakalavr ta’lim yо‘nalishi bitiruvchi kurs uchun Ixtisoslik fanlaridan yakuniy davlat attestatsiyasini о‘tkazish tartibi, savollari, baholash mezonlari va о‘quv adabiyotlari hamda elektron ta’lim resurslari keltirilgan.

|  |  |  |
| --- | --- | --- |
| **Tuzuvchilar:** |  N.Ibroximov  | −Axborot xavfsizligi kafedrasi mudiri. |
|  |  M.Turdimatov  | −Axborot xavfsizligi kafedrasi dotsenti. |
| **Taqrizchilar:** | L.K.Mamadaliyeva | −Farg‘ona politexnika instituti, “Intellektual muhandislik tizimlari” kafedrasi professori, texnika fanlari doktori, DSc. |
|  |  F.Muxtarov  | −Axborot xavfsizligi kafedrasi dotsenti. |

Ushbu dastur Axborot xavfsizliggi kafedrasining 20 yanvar № 6 -sonli yig‘ilishida muhokama qilingan.

Axborot xavfsizligi

kafedrasi mudiri: \_\_\_\_\_\_\_\_\_\_\_\_\_ N.Ibroximov

**Kelishildi:**

О‘quv-uslubiy bо‘lim boshlig‘i: \_\_\_\_\_\_\_\_\_\_\_\_\_ Sh.Umarov.

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali Uslubiy Kengashining 2024 yil 27 yanvar 6 - sonli yig‘ilishida tasdiqlangan.

**5330300– Axborot xavfsizligi (sohalar bo‘yicha) bakalavr ta’lim yо‘nalishi bitiruvchi kurs uchun ixtisoslik fanlaridan о‘tkaziladigan yakuniy davlat attestatsiyasi**

**DASTURI**

5330300– Axborot xavfsizligi (sohalar bo‘yicha) ta’lim yо‘nalishi bitiruvchi kurs talabalari uchun ixtisoslik fanlaridan о‘tkaziladigan yakuniy davlat attestatsiyasi “**Tarmoq xavfsizligi**”, “**Kriptografiya**”, “**Kiberxavfsizlik siyosati**”, “**Kiber-huquq va kiber-etika** ”, “**Axborot xavfsizligi xavflarini boshqarishga kirish**” fanlaridan yozma ravishda о‘tkazilishi belgilandi.

**“Tarmoq xavfsizligi” fani bо‘yicha**

Oliy ta’lim Davlat standartiga kо‘ra “Axborot xavfsizligi” fanining qatoriga bir necha о‘zaro bog‘liq bо‘lgan fanlar kiradi. Bular qatorida **“Tarmoq xavfsizligi”** fani ham bor. Fanni o’zlashtirishda, talaba “Kompyuter tarmoqlari”, “Kiberxavfsizlik asoslari” kabi fanlardan yetarli bilim darajasiga ega bo’lish talab etiladi. Shuningdek, darslik, internet tarmoqlari, o’quv va o’quv-uslubiy qo’llanmalar, ma’ruza matnlari, videoma’ruzalar, tarqatma materiallar, elektron ma’ruzalar, elektron qo’llanmalardan foydalaniladi. Fanni vazifasi – talabalarga tarmoq xavfsizligini ta’minlash sohasidagi xalqaro va milliy me’yoriy hujjatlarni bilish bilan bir qatorda tarmoq xavfsizligini ta’minlashda foydalaniladigan usullar hamda apparat va dasturiy vositalarini qо‘llashga doir bilimlar va uquvlar hosil qilishdan iborat.

O’quv fanini talab darajasida o’zlashtirish uchun uni o’qitish jarayonida o’qitishning interfaol usullaridan, kichik guruhlarlarda ishlash, aqliy xujum, muammoli o’qitish hamda turli innovatsion metodlardan foydalanib talabalarning erkin va mustaqil ishlashini samarali tashkil etish maqsadida qo’yilgan o’quv vazifalarini mustaqil bajarishni tashkil etish maqsadida axborot taxnologiyalari hamda axborot ta’lim muhitidan foydalanish ko’zda tutiladi.

**“Kriptografiya 1 va 2” fani bо‘yicha**

**Fanni o‘qitishdan maqsad** – talablarga kriptografiyaning matematik asoslarini tushinishini uchun zarur bo’lgan bilim va ko’nikmalarni shakllantirishdan iborat. Sonlar nazariyasi matematikaning alohida bo’limi sifatida butun sonlarga xos bo‘lgan xususiyatlarini tekshirish va tahlil qilish bilan shug’illanadi.Kriptografiya sohasida ushbu soha xavfsizlik va maxfiylikni ta’minlashga qaratilgan mustahkam kriptografik tizimlarini yaratishda muhim rol o‘ynaydi.

**“Kiberxavfsizlik siyosati” fani bо‘yicha**

**Fanni o‘qitishdan maqsad** – talablarga kiberxavfsizlikni ta’minlash sohasidagi xalqaro va milliy me’yoriy, nazariy va amaliy izlanishlar natijalari bilan tanishtirish bilan bir qatorda kiberxavfsizlik siyosatini tashkil etishda foydalanilgan turli zamonaviy yondashuvlar, tashkiliy va huquqiy me’yorlarini qo‘llashga doir bilimlar va ko‘nikmalar xosil qilishdan iborat.

**Fanning vazifasi** – modulyar arifmetika, chekli maydonlar ustida amallar, tub sonlarni generatsiya qilish, Evkilid va kengaytirilgan Evkilidning algoritmlari, qoldiqlar haqidagi xitoy teoremalari, kvadrat chegirma, faktorizatsiyalash va diskret logarifmlash masalalarini yechish, birlamchi ildiz, elliptik egri chiziqlarning matematik asoslari kabi bilimlarni o‘rgatishdan iborat.

**Fanni o‘qitishdan maqsad-** talablarga axborotlarni kriptografik himoyalash vositalari maxfiy kalitli va ochiq kalitli kriptotizimlardan foydalanish bo’yicha bilim, ko‘nikma hamda malakalarini shakllantirishdan iborat.

 **Fanning vazifalari-**talablardan kriptografiyaning asosiy tushunchalari, klassik kriptotizimlar va ularning kriptotahlili, oqimli va blokli simmetrik shifrlash algoritmlari, xesh funksiyalar va ma’lumotlarni autentifikatsiyalash kodlari, ochiq kalitli shifrlash algoritmlari va ularga asoslangan elektron raqamli imzo algortimlari kabi bilimlarni shakllantirishdan iborat.

**Fanning vazifasi -** talabalarga nazariy bilimlar, amaliy ko‘nikmalar berish, hamda kiberxavfsizlik siyosatining asosiy tushunchalari, xavfsizlikni ta’minlashga qaratilgan milliy va rivojlangan davlatlar tajribasi va mazmuni bilan tanishtirish hamda kiberxavfsizlikka zamonaviy tahdidlar, tarmoq xavfsizligi standartlari, kiberxavfsizlikni ta’minlashda foydalaniladigan vositalarning ahamiyatini ochib berish.

**“Kiber-huquq va kiber-etika” fani bо‘yicha**

**Fanni o‘qitishdan maqsad** – talabalarga kiberxavfsizlikni ta’minlash soxasidagi xalqaro va milliy me’yoriy, nazariy va amaliy izlanishlar natijalari bilan tanishtirish bilan bir qatorda axborot tizimlarini, resurslarini himoyalangan axborotga nisbatan bo‘ladigan tahdidlarga zamonaviy yondashuvga asoslangan xolda xuquqiy tahlil qilishga doir bilimlar va o‘quvlar xosil qilishdan iborat.

**Fanning vazifasi** – talablarga nazariy bilimlar, amaliy ko‘nikmlar, hamda kibermakonda huquqiy normalariga va kiberetikaning qoidalariga rioya qilgan holda axborotni ximoyalashning ahamiyatini ochib berish.

**“Axborot xavfsizligi xavflarini boshqarishga kirish” fani bо‘yicha**

**Fanni o‘qitishdan maqsad** – Axborot risklarini (xavflarini)boshqarishga kirish tizimini, axborot xavfsizligi risklarini aniqlash, qayta ishlash bartaraf etish usullari va vositalarini qo‘llash, risklarini tahlil qilishga doir bilim va o‘quvlar xosil qilishdan iborat.

**Fanning vazifasi** –talabalarga axborot xavfsizligi risklari bo‘yicha nazariy bilimlar, amaliy ko‘nikmalar, hamda axborotni himoyalashda risklarni baholash ahamiyatini ochib berish.

5330300– Axborot xavfsizligi (sohalar bo‘yicha) ta’lim yо‘nalishi bitiruvchi kurs talabalari uchun ixtisoslik fanlaridan о‘tkaziladigan yakuniy davlat attestatsiyasi “**Tarmoq xavfsizligi**”, “**Kriptografiya**”, “**Kiberxavfsizlik siyosati**”, “**Kiber-huquq va kiber-etika** ”, “**Axborot xavfsizligi xavflarini boshqarishga kirish**” fanlaridan о‘tkaziladigan yakuniy davlat attestatsiyasi sinovlarinig asosiy

**SAVOLLARI**

1. Kriptografiyaning asosiy tushunchalari va atamalari

2. Kriptotizmlarga qo‘yiladigan talablar. Kirxgof prinsipi.

3. Simmetrik kalitli shifrlash algoritmlari va xesh funksiyalar

4. Kriptografik algoritmlarga qaratilgan hujumlar

5. Kriptografik tizimlarda bardoshlilik tushunchasi. Nazariy, amaliy bardoshlilik.

6. Modul arifmetikasi va uning xususiyatlari.

7. Shifrlash usullarining klassifikatsiyasi.

8. Klassik shifrlash usullari va ularda foydalanilgan akslantirishlar.

9. Klassik shifrlash usullari (Sezer, Affin tizimidagi Sezer, Sehrli kvadrat, Vijiner, Ikki tomonlama o‘rin almashtirish, Gamilton marshruti).

10. Klassik shifrlash algoritmlarining kriptotahlili

11. Simmetrik shifrlash usullari. Blokli va oqimli simmetrik shifrlash usullari

12. Oqimli shifrlash algoritmlarning mohiyati. Psevdotasodifiy va tasodifiy sonlar generatori.

13. A5/1 shifri va uning GSM tarmoqda foydalanish tahlili.

14. RC4 shifri va uning WEP protokolda foydalanish tahlili.

15. Simmetrik blokli shifrlar va ularni qurish usullari.

16. DES simmetrik blokli shifrlash algoritmi.

17. AES simmetrik blokli shifrlash standarti.

18. ГОСТ 28147-89 simmetrik blokli shifrlash standarti

19. O‘z Dst 1105:2009 simmetrik blokli shifrlash standarti

20. Simmetrik blokli shifrlash rejimlari

21. Xesh funksiyalar va ularni qurish usullari

22. MD5 xesh funksiyasi

23. Ma’lumotlarni autentifikatsiyalash kodlari. HMAC algoritmi

24. Ochiq kalitli shifrlash algoritmlari va ularni yaratishda foydalanilgan matematik muammolar.

25. Simmetrik va ochiq kalitli shifrlash tizimlarining qiyosiy tahlili.

26. RSA ochiq kalitli shifrlash algoritmi

27. Faktorlash muammosi va uni hisoblash

28. RSA ochiq kalitli shifrlash algoritmining kriptotahlili

29. El-Gamal ochiq kalitli shifrlash algoritmi

30. Diffi-Xelman kalitlarni ochiq taqsimlash protokoli va uning xavfsizlik tahlili.

31. Elliptik egri chiziqlarga asoslangan ochiq kalitli shifrlash algoritmlari

32. Chekli maydonda elliptic egri chiziqlar ustida amallar bajarish

33. Elektron raqamli imzo tizimlari va ularning asosiy vazifalari.

34. RSA shifrlash algoritmiga asoslangan ERI algoritmlari.

35. El-Gamal shifrlash algoritmiga asoslangan ERI algoritmlari.

36. Ochiq kalitli shifrlardan ma’lumot konfidensialligini ta’minlashda foydalanish afzallik va kamchiligi

37. Kriptografik protokollar

38. Ochiq kalitli shifrlash algoritmlariga asoslangan autentifikatsiyalash protokollari.

39. Ochiq kalitli kriptografik algoritmlardan bulutli hisoblash tizimlarida foydalanish.

40. Gibrid shifrlash usullari va ularni qurish

41.Risk tushunchasi. Risklarni klassifikatsiyasi. Riskni tashkil etuvchilari. Risklarni boshqarish.

42. Risklarni taxlil qilish metodlari. Metodlarning avzalliklari va kamchiliklari.

43. Risklarni boshqarishda kontekst tushunchasi. Axborot xavfsizligi risklarini boshqarish asosiy mezonlari, risklarni ko‘lami va chegaralari.

44. Risklarni boshqarishda ichki va tashqi kontekst. Risk mezoni. Riskni baholash.

45. Aktivlarni identifikatsiya qilish. Asosiy aktiv, biznes jarayonlar va faoliyat, qo‘shimcha aktiv, apparat vositalar, dasturiy ta’minot, operatsion tizim.

46. Risklarni tahlil qilish bosqichlari. Umumiy qoidalar. Boshqarish metodlarini baholash.

47. Risk tahlili va extimolligini baholash. Dastlabki tahlil. Riskni qiyosiy baholash. Ruyhatga olish, xujjatlashtirish.

48. Riskni sifat va miqdor ko‘rsatkichlarini baholash. Riskni identifikatsiyalash, aktivni, taxdidni, zaiflikni, nazorat vositalarini baholash.

49. Riskni sifat va miqdor ko‘rsatkichlarini baholash. Oqibatlarni identifikatsiyalash, tahlil qilish, baholash. Sifat va miqdor o‘lchovi, risk darajasini o‘lchash.

50. Axborot xavfsizligi risklarini qayta ishlash. Risklarni qayta ishlash.Riskni kamaytirish. Riskni qoldirish.

51. Axborot xavfsizligi risklarini qayta ishlash. Riskni oldini olish. Riskni ko’chirish. Riskni qabul qilish.

52. Risk bo‘yicha shartnomalar va axborot almashish. Risk menejmenti ma’lumotlari. Risk bo‘yicha axborot almashinuvi rejalari. Qaror qabul qilishni rejalashtirish.

53. Axborot xavfsizligini monitoringi va risk faktorlarini qayta ko‘rib chiqish. Riskning hayotiy davri.

54. Riskning hayotiy davrining turli bosqichlarida baholash usullari.

55. Tashkilot uzluksiz ishlashini ta’minlanishini boshqarish usullari.

56. Zamonaviy jamiyatda axborot xavfsizligi risklari.

57. Axborot xavfsizligi risklarini boshqarishdagi yondashuvlar. CRAMM (Risk Analysis and Management Method).

58. Axborot xavfsizligi risklarini boshqarishdagi yondashuvlar. COBIT for Risk usuli.

59. Riskni boshqarish sohasiga oid halqaro va milliy standartlar. ISO / IEC 27005:2011 “Axborot texnologiyalari.

60. Xavfsizlikni ta’minlash metodlari va vositalari. Axborot xavfsizligini risklarini boshqarish”.

61. Axborot xavfsizligi risklarini taxlil qilishning graf modeli.

62. Graf tushunchasi. Graf turlari. To‘liq graflar.

63. To‘liq kesishuvli xavfsizlik modeli. Himoyalanadigan kichik ob’ekt struktur sxemasi. Taxdidlar to‘plami.

64. Biznesning uzluksizligini boshqarish. Biznesning uzluksizligini ta’minlanishini boshqarishda axborot xavfsizligi masalalari.

65. Biznesning uzluksizligi va risklar.

66. Axborot xavfsizligi riskining modeli.

67. Axborot xavfsizligi riskini "galstuk - kapalak" usuli yordamida tahlili.

68.Axborot xavfsizligi riskini "sabab - oqibat" usuli yordamida tahlil.

69. Axborot xavfsizligi riskini "nosozliklar-daraxti" usuli yordamida tahlil.

70. Axborot xavfsizligi riskini "vaziyatlar - daraxti" usuli yordamida tahlil.

71.Axborot xavfsizligi risklarini identifikatsiyalash.

72.Axborot aktivlarini xayotiy davrini boshqarish.

73. Axborot xavfsizligi risklari tahlili.

74. Axborot xavfsizligi risklari tahliliy vositalari.

75. Tipik tahdidlar va tahdidlarning manbalari.

76. Axborot xavfsizligida risklarini boshqarishning tashkiliy strukturasi.

77. Ob’ektning dastlabki himoyalanganlik darajasini baholash.

78. Ob’ektga yetkaziladigan zararni baholash usullari.

79. Axborot xavfsizligi riskini baholash usullari.

80. Axborot xavfsizligi riskini baholash metodikasi.

81. ISO/IEC 27005:2013. Xavfsizlikni ta’minlash usullari.

22. Ob’ektning axborot xavfsizligi darajasini aniqlash va baholash.

83. Tashkilotda ehtimoliy havflarni boshqarish usullari.

84. Axborot xavfsizligi riskni qayta ishlash usullari.

85. Axborot xavfsizligi riskni qabul qilish.

86. Tashkilot risklarini baholash va tahlil qilish.

87. Tashkilot risklarini amaliy tahlili va monitoringi.

88. O'z DSt ISO/IEC 13335-1:2009 standarti. Axborot kommunikastiya texnologiyalari havfsizligini boshqarish modellari.

89. Axborot xavfsizligi risklarini aniqlashga yondashuv. Foydalanishni boshqarish siyosati.

90. Axborot xavfsizligi boshqarish tizimini takomillashtirish usullari. Risk monitoringi.

91. Milliy xavfsizlikning turlari va kiberxavfsizlik siyosatida tutgan oʻrni

92. Kiberxavfsizlik siyosatini aniqlashda qanday ishlar amalga oshirilishi lozim

93. Kiberxavfsizlik siyosati domenlari

94. Korxona arxitekturasini tuzishda kiberxavfsizlik strategiyasi va arxitekturasining oʻrni.

95. Kiberxavfsizlik siyosatida inson omilining roli qanday?

96. Kiberjinoyatchilikni oldini olish usullari va kiberqonunlar haqida maʻlumot bering.

97. Kiberxavfsizlik siyosatining irarxiyasi deganda nimani tushunasiz?

98. Axborot texnologiyalari sohasida korxonalarda qanday xavfsizlik siyosati qoʻllaniladi?

99. Internetdan foydalanish siyosatining 4 ta kategoriyalari tavfsiflab bering?

100. Foydalanishni boshqarishning DAC usuli va uning xususiyatlari qanday?

101. Bell-La Padul modeli va uning kiberxavfsizlik siyosatidagi oʻrni qanday?

102. Kiberxavfsizlik sohasiga oid xalqaro standartlar haqida ma’lumot bering.

103. Kiberxavfsizlik siyosatida axborotni himoyalashda tarmoqlararo ekranlarning oʻrni qanday?

104. Axborot tizimlari tashkilotiga ishga qabul qilish va tugatish tartiblari?

105. Korporativ tizimlarni zararkunanda dasturlar va viruslar taʻsiridan himoya qilish.

106. Tarmoqlararo ekran yordamida kiberhujumlarga qarshi himoyani taʼminlash

107. Kiberxavfsizlik vositalariga nimalar kiradi?

108. Kiberxavfsizlik siyosatida xodimlarni xavfsizlik boʻyicha oʻqitish qanday ahamiyatga ega?

109. Kiberxavfsizlik siyosatini amalga oshirish va rivojlantirishda qanday uslublar mavjud?

110. Kiberxavfsizlik siyoatida Geopolitikaning oʻrni qanday?

111. Korporativ axborot tizimlari xavfsizlik monitoring va auditi deganda nimani tushunasiz?

112. Raqamli kriminalistikaga taʻrif bering.

113. Kiberjinoyatlar turlari va ularga taʻrif bering.

114. Rossiyaning kiberxavfsizlik siyosati boʻyicha yondashuvi qanday?

115. AQSHning kiberxavfsizlik siyosati boʻyicha yondashuvi qanday?

116. Kiberhujumlarni oldini olishda huquqni muhofaza qiluvchi organlarning oʻrni.

117. Oʻzbekistondagi kiberxavfsizlik taʻminlangan tashkilotlar 2023-yilgi reytingi haqida ma’lumot bering.

118. Oʻzbekistonning kiberxavfsizlik siyosati boʻyicha yondashuvi qanday?

119. Xavfsizlik siyosatini ishlab chiqish bosqichlarini sanab bering.

120. Axborot xavfsizligi siyosatini ishlab chiqishda nimalarga e’tibor berish kerak?

121. Oʻzbekiston Respublikasining Kiberxavfsizlik to’g’risidagi qonuni haqida ma’lumot bering.

122. Osiyo yetakchi davlatlarda kiberxavfsizlik qaysi bosqichda rivojlangan?

123. Kiberxavfsizlik markazi qanday xizmatlarni taqdim etadi ?

124. Oʻzbekiston Respublikasining “Kiberxavfsizlik toʻgʻrisida”gi qonuni qachon qabul qilindi va bu qonuning maqsadlarini sanab oʻting.

125. Zaifliklarni skanerlash vositalari

126. Suqilib kirish testlari (penetrating testing).

127. Simsiz tarmoqdan foydalanish siyosati

128. Mobil qurilmalardan foydalanish siyosati.

129. Bulutli xizmatlarga oid siyosat.

130. Elektron pochtadan foydalanish siyosati.

131. Monitoringlash siyosati. Audit siyosati

132. Fizik xavfsizlik siyosati.

133. Tizimlardan foydalanishdagi siyosatlar

134. Zaxiralash va qayta tiklash siyosati

135. Korporatsiyalarning kiberjinoyatga munosabati. 1. Tarmoqda autentifikatsiya, avtorizatsiya va qayd etish tushunchalari.

136. RADIUS AAA protokoli uchun IETF-standarti. TACACS+ va uning qo‘llanilishi. RADIUS va TACACS+ protokollarining asosiy imkoniyatlari

137. Bulutli hisoblash tizimlari xizmatlaridan foydalanishda axborot xavfsizligi muammolari, bulutli hisoblash tizimi platformalari turlari, bulutli tizimlarda foydalanuvchilar ma’lumotlarining xavfsizligini ta’minlash.

138. Hujumlarni aniqlash tizimi. IDS/IPS texnologiyalari. IPS signaturasi. IPSNI qo‘llash.

139. Foydalanishlarga ruxsat berish ro‘yxati (ACL).

140. Tarmoqlararo ekran texnologiyalari. Tarmoqlararo ekranlarning qo‘shimcha imkoniyatlari.

141. ASA (Adaptive Security Appliance) ga kirish. ASA tarmoqlararo ekranning konfiguratsiyasi.

142. Himoyalangan virtual tarmoq texnologiyalari. IPSec VPN komponentalari.

143. Virtual xususiy tarmoqlarni qо‘llagan xolda tarmoqlararo xavfsizlikni ta’minlash kommunikatsiyalari

144. Tarmoq trafigini tahlillash. Qalbaki ARP-server va DNS-serverlar.

145. Masofaviy hujum tushunchasi. Masofaviy hujumlarni tasniflash va ularni amalga oshirish mexanizmlari

146. Axborotni himoyalashning tashkiliy-texnik usullari.

147. IKE kriptokalitlarini boshqarish protokoli.

148. AH va ESP protokollari yordamida uzatilayotgan ma’lumotlarni himoyalash.

149. IPSec xavfsizlik vositasi arxitekturasi.

150. OSI modelining transport sathi imkoniyatlari va xususiyatlari. Transport sathi xavfsizlik protokollari.

151. SSL/TLS va SOCKS protokollari va ularni tarmoq xavfsizligini ta’minlashdagi o‘rni.

152. Kanal sathida himoyalangan kanallarni shakllantirish protokollari. PPTP, L2F va L2TP protokollari

153. Identifikatsiya va foydalanishlarini boshqarish. Himoyalangan masofaviy foydalanishlarni tashkil etish

154. Tarmoq xavfsizligi tashkil etish va vazifalarining asosiy tamoyillari

155. Ochiq tizimlar o‘zaro ishlashining etalon modeli.

156. OSI va TCP/IP modellarining imkoniyatlari va protokollari

157. Xavfsizlik shlyuzlarini qо‘llagan holda tarmoqlararo xavfsizlikni ta’minlash kommunikatsiyalari (О‘z DSt ISO/IEC 27033).

158. Etalon tarmoq ssenariylari, tahdidlar, loyihalashtirish usullari va boshqaruv masalalari (О‘z DSt ISO/IEC 27033).

159. Tarmoq xavfsizligini loyihalashtirish va joriy etish bо‘yicha rahbariy kо‘rsatmalar (О‘z DSt ISO/IEC 27033).

160. Tarmoq xavfsizligi. Sharh va konsepsiyalar (О‘z DSt ISO/IEC 27033).

161. Kompyuter tizimlari va tarmoqlarida xavfsizlik siyosati modellari tushunchasi.

162. Tarmoq tahdidlarining zamonaviy shakllari va ulardan himoyalanish usullari va tarmoq xavfsizligi tahdidlari klassifikatsiyasi.

163. Kompyuter tarmoqlarida xavfsizlik tushunchasi va tarmoqlarni qurishda tarmoq xavfsizligining mohiyati.

164. OSI modelining fizik sathida ma’lumotlarni himoyalash.

165. OSI modelining kanal sathida ma’lumotlarni himoyalash.

166. OSI modelining tarmoq sathida ma’lumotlarni himoyalash.

167. OSI modelining transport sathida ma’lumotlarni himoyalash.

168. OSI modelining seans sathida ma’lumotlarni himoyalash.

169. OSI modelining taqdimot sathida ma’lumotlarni himoyalash.

170. OSI modelining ilova sathida ma’lumotlarni himoyalash.

171. Tarmoq qurilmalari: kommutatorlarda xavfsizlik sozlamalari.

172. Tarmoq qurilmalari: marshrituzator xavfsizlik sozlamalari.

173. Tarmoq qurilmalari: Tarmoqlararo ekranlar va ularni xavfsizlik sozlamalari.

174. WIFI qurilmalarida simsiz tarmoq xavfsizligi sozlamalari.

175. Transmission Control Protocol (TCP) va Internet Protocol (IP) (TCP/IP protokollari) vazifasi va xavfsizligi.

176. Ilova darajasida axborot xavfsizligi protokoli - PGP protokoli (Pretty Good Privacy) xususiyatlari.

177. BS 7799-1:2005 - Britaniya standarti (Axborot xavfsizligini boshqarish amaliyoti) tavsifi

178. Simsiz tarmoqlar xavfsizligi uchun SNAP (Subnetwork Address Protocol) ning o‘ziga xos xususiyatlari

179. Simsiz tarmoqlar xavfsizligini ta’minlashda EAP (Extensible Authentication Protocol) protokolining qo’llanilishi.

180. Kompyuter tarmoqlariga bo‘ladigan zamonaviy hujumlar va ularni klassifikatsiyasi.

181. Tarmoq xavfsizligi bilan shug‘illanadigan xalqaro tashkilotlar.

182. Tarmoq xavfsizligini ta’minlashda foydalaniladigan apparat-dasturiy vositalar.

183. OSI modeli va TC/IP modeli farqlanishi va ularda xavfsizlik muammolari.

184. Tarmoq xavfsizligi standartlari (О‘z DSt ISO/IEC 27033).

185. Kiberinfrastruktura muammolari

186. Kiberfoydalanuvchilar muammolari: zararli reklamalar, obro‘sizlantirish, tegishli foydalanish, kiberjinoyatlar, geojoylashuv, shaxsiylik

187. Kiberxavfsizlik siyosati katalogi

188. Xavfsizlik freymvorklari

189. Kiberxavfsizlik tushunchasi. Konfidensiallik, yaxlitlik va foydalanuvchanlik

190. Kiberjinoyatchilik tushunchasi, kiberjinoyatchilik turlari

191. Axborotdan oqilona foydalanish kodeksi

192. O'zbekistonda kiberxavfsizlikni ta'minlashning asosiy yo'nalishlari

193. Kiberxavfsizlikni ta'minlash sohasidagi davlat siyosati

194. Axborotni himoyalash usullari

195. Kiberhuquq tushunchasi, kiberhuquq rivojlanish bosqichi

196. Kiberxavfsizlik muammolari

197. O'zbekiston AKT sohasidagi siyosatni belgilovchi qonunlar.

198. Axborot xavfsizligi sohasidagi subyektlar va obyektlar o'rtasidagi munosabatlarni tartibga soluvchi me'yoriy hujjatlar.

199. Kiberxavfsizlikni ta'minlashning davlat tizimi

200. Kiberhuquqni ta'minlashda tashkilotlat faoliyatini litsenziyalash tizimi.

201. Axborotni himoya qilish vositalarini sertifikatsiyasi

202. Intelektual mulh tushunchasi, intelektual mulkni himoyalash

203. Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma'lumotlar bazalarining huquqiy himoyasi to'g'risidagi qonuning mohiyati

204. Kompyuter dasturlariga mualliflik huquqlari. Kompyuter dasturlarii ro'yxatga olish.

205. Kiberxavfsizlikning ijtimoiy va etik jihatlari

206. Kiberjmakonda axborot xavfsizligini ta'minlashda risk tushunchasi.

207. "Konfidensial axborotning turlari va darajalari bo'yicha klassifikatsiyasi"

208. Elektron resurs tushunchasi. Elektron resurslari kategoriyalari

209. Elektron resurslar va tizimlarini muxofaza qilish tartiblari

210. Davlat sirlari, tijorat silari, xizmat sirlar, kasbiy, shaxsiy sirlar muxofazasi

211. xujjatlarni maxfiylik darajasini belgilash va yuritish qoidalari

212. Kiberxavfsizlik buzg'unchisining gipotetik modeli.

213. Himoyalangan axborotga nisbatan bo'ladigan tahdidlarga zamonaviy yondashuv

214. Himoyalangan kibermakon tushunchasi va tahdidlar strukturasi

215. Kibermakonda elektron resursni xavfsizligini ta'minlashda tizimli yondashuv

216. Kiberxavfsizlik sohasiga oid milliy standartlar

217. Kiberxavfsizlik sohasiga oid xalqaro standartlar

218. Yevropa davlatlarining axborot xavfsizligini ta'minlashning uyg'unlashtirilgan mezonlari

219. Axborotni tadqiq qilish va nusxalashdan himoyalash tizimlari

220. Dasturni dizeccemberlardan himoyalash, shifrlash dasturlari.

221. Bulutli xizmatlarni ko'rsatishni huquqiy tartibga solish muammolari

222. Axborot urushining milliy xavfsizlikka tahdidi

223. Axborotlashtirish qoidalarini buzganlik uchun javobgarlik

224. Dasturiy ta'minot ishlab chiqaruvchilarning himoya turlari

225. Dasturiy ta'minot xavfsizligini ta'minlashda zaifliklar turlari

226. Elektron to'lovlarni amalga oshirishning huquqiy ahamiyati

227. Kiberxavfsizlik to'g'risida qonun mohiyati.

228. Kompyuter xavfsizligi bilan bog'liq ahloqiy muammolar: Hakerlik, haktivizm va konturhaking.

229. Kompyuter xavfsizligini ta'minlashda bilan axloqiy muammolar va ularning yechimlari.

230. Zamonaviy kiberjinoyatlarning ko'rinishlari va ularni kelib chiqish sabablari

231. Internet tarmog'ida siyosiy g'oyalarini tarqatish usullari

232. So'z erkinligi, internetdan foydalanishda inson huquqlari va axborot erkinligini himoya qilish

233. Ochiq kodli dasturiy vositalarning himoyalashning huquqiy asoslari.

234. Internet etikasining muhim masalalari.

235. Kibermajaro etikasining paydo bo'lishi va hozirda foydalanish omillari.

236. Yirik mamlakatlardagi mavjud kibermojarolar.

238. Suniy intelekt va undagi kiber etika masalalari.

239. Kiberbulling tushunchasi. Kiberbulling turlari.

240. Maxfiy xizmatlar doirasida etika masalalari.

**Davlat attestatsiya sinovlarida Ixtisoslik fanlari bо‘yicha bitiruvchilar bilimini baxolash**

**MEZONLARI**

О‘zbekiston Respublikasi Prezidentining 2018 yil 5 iyundagi PQ-3775-son «Oliy ta’lim muassasalarida ta’lim sifatini oshirish va ularning mamlakatda amalga oshirilayotgan keng qamrovli islohotlarda faol ishtirokini ta’minlash bо‘yicha qо‘shimcha chora-tadbirlar tо‘g‘risida»gi [qarori](http://lex.uz/docs/3765586) hamda О‘zbekiston Respublikasi Vazirlar Mahkamasining 2018-yil 24-iyuldagi 569-sonli “Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetida kadrlar tayyorlash tizimini tubdan takomillashtirish va samaradorligini oshirish chora-tadbirlari tо‘g‘risida”gi qarorlari asosan amalga oshiriladi.

1. Bitiruvchi kurslar uchun о‘tkaziladigan yakuniy davlat attestatsiyasi sinovlarini Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filialida о‘qiydigan tillar, ya’ni о‘zbek tilida topshiradilar.
2. Bitiruvchi kurslar uchun о‘tkaziladigan yakuniy davlat attestatsiyasi sinovlari tanlangan mutaxassislik fanlari bо‘yicha о‘tkaziladi.

Muhammad al-Xorazmiy nomidagi TATU va uning filiallarida 2018-2019 о‘quv yilidan boshlab о‘qitishning kredit tizimi joriy etilganini inobatga olgan holda ballar taqsimoti quyidagicha holatda amalga oshirildi:

“5” - “A’lo” –– 90 – 100;

“4” - “Yaxshi” –– 70 – 89;

“3”- “Qoniqarli” –– 60 – 69;

“2”- “Qoniqarsiz” –– 0 – 59;

0 – 59 oralig‘ida ball tо‘plagan talabalar yakuniy davlat attestatsiya sinovlaridan о‘ta olmagan hisoblanadi. Yakuniy davlat attestatsiyasi sinovidan о‘ta olmagan shaxs о‘qish muddati tugagandan sо‘ng, arizasiga muvofiq yakuniy davlat attestatsiyasi sinovini keyingi yillarda qayta topshirish huquqiga ega. Bunda oliy ta’lim muassasasi rektori (filial direktori) shaxsni yakuniy davlat attestatsiyasi sinovini qayta topshirishga qо‘yish bо‘yicha buyruq chiqarishi lozim bо‘ladi.

Bitiruvchi kurslar uchun о‘tkaziladigan yakuniy davlat attestatsiyasi tanlangan mutaxassislik bо‘yicha bilim darajasini belgilovchi maxsus fanlardan sinov о‘tkaziladi, **baholash mezoni** **0 balldan 100 ballgachani** tashkil qiladi. Sinov maxsus yozma ish ravishda tashkil etilib, yakuniy davlat attestatsiyasini topshiruvchilar tanlangan mutaxassislik bо‘yicha nazariy bilimi aniqlanadi. Maxsus fanlar bо‘yicha savollar ushbu fanlar dasturlari asosida tuzilgan. Har bir variant **5 ta** savoldan iborat bо‘lib **100 ballni** tо‘plash mumkin.

Mutaxassislik bо‘yicha har bir savolga javob tо‘g‘ri va tо‘liq yoritilsa, savolning ahamiyati, amaliy jihatlari, natijalari mustaqil aniq fikrlar asosida muammolarga jiddiy yondashilgan holda yoritilsa, javobda mantiqiy yaxlitlikka erishilgan bо‘lsa, о‘zlashtirish kо‘rsatkichi **28-33 (29-34) ball** oralig‘ida baholanadi.

Berilgan savolga tо‘g‘ri javob yozilsa, javoblar ilmiy-amaliy jihatdan asosli, mantiqli yoritilgan bо‘lsa, biroq ta’lim islohatlarni bugungi yangilanishlar amaliyoti bilan bog‘lashda ayrim noaniqliklarga yо‘l qо‘yilgan bо‘lsa, о‘zlashtirish kо‘rsatkichi **23-27 ball** oralig‘ida baholanadi.

Savolga asosan tо‘g‘ri javob yozilsa, biroq qо‘yilgan masalaning mohiyati, mazmuni, natijalari yuzaki yoritilsa, fikr-mushohada bayonida tarqoqlik kuzatilsa о‘zlashtirish kо‘rsatkchi **18-22 ball** oralig‘ida baholanadi.

Savolga javob notо‘g‘ri yozilsa, о‘quv adabiyotidan sо‘zma-sо‘z kо‘chirilgan bо‘lsa, savollarga umuman javob yozilmagan bо‘lsa yoki savolni mohiyatini tushunmaydi, lekin atroflicha yondashsa о‘zlashtirish kо‘rsatkichi **0-17 ball** oralig‘ida baholanadi.

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Umumiy ball** | **Yakuniy davlat attestatsiyasini topshiruvchining bilim darajasi** | **Ball** |
| 1. | 28-33(29-34) | Qо‘yilgan savolga javob mazmunan aniq yoritilgan, uning mazmun va mohiyati tо‘liq ochib berilgan, javobda mantiqiy yaxlitlikka erishilgan. | 6-7(7-8) |
| Mamlakatimizda amalga oshirilayotgan ta’lim islohotlar tahlili, uning amaliy samaralari, natijalari bо‘yicha mustaqil, ijodiy fikrning mavjudligi. | 6-7 |
| Muammolarni aniq misollar bilan tahlil qilish qobiliyatiga ega. | 6-7 |
| Mantiqiy ketma-ketlikka erishilganlik, savol bо‘yicha umumiy xulosalar chiqarilganlik. | 5-6 |
| Imlo va stilistik xatolarga yо‘l qо‘yilmagan. | 5-6 |
| 2. | 23-27 | Berilgan savolga tо‘g‘ri javob yozilgan, ammo noaniqliklar va cheklanishlarga yо‘l qо‘yilgan. | 5-6 |
| Savolga javob yozishda bitiruvchining mustaqil fikrlash qobiliyati seziladi. | 5-6 |
| Amaliy masala kо‘rsatilgan. | 5-6 |
| Javoblarga ijodiy yondashuv mavjud. | 4-5 |
| Imlo va stilistik xatolarga yо‘l qо‘yilmagan. | 4-4 |
| 3. | 18-22 | Javobda masalaning mohiyati tushuntirilgan, biroq mazmun va natijalar yuzaki yoritilgan. | 4-5 |
| Javobda fikrlar tarqoq. | 4-5 |
| Mantiqiy ketma-ketlik mavjud emas. | 4-5 |
| Berilgan savol bо‘yicha umumiy tasavvurga ega, lekin tahlil etarli emas. | 3-4 |
| Imlo va stilistik xatolarga yо‘l qо‘yilmagan. | 3-4 |
| 4. | 0-17 | Notо‘g‘ri javob berilgan.Savol bо‘yicha aniq tasavvurga ega emas.О‘quv adabiyotlaridan sо‘zma-sо‘z kо‘chirilgan.Savolni mohiyatini tushunmaydi, lekin atroflicha yondashilgan. | 0-17 |

**ASOSIY ADABIYOTLAR RО‘YXATI**

1.William Stallings, Network Security Essentials: Applications and Standards, 6th Edition, 2017.

2.Олифер В.Г., Олифер Н.А. “Безопасность компьютерных сетей” 2017

3.Кучкаров Тахир Анварович, Безопасность сетей, 2022. с. 292

4.Ganiyev Salim Karimovich, Kuchkarov Taxir Anvarovich, Mobil tizimlar xavfsizligi, 2019. s. 139

5.O‘zbekiston Respublikasining Konstitutsiyasi. - T., 2023

6.S.K.Ganiyev, A.A.G aniyev, Z.T.Xudoyqulov. Kiberxafsizlik asoslari: o‘quv qo‘llanma, -T.: “Nihol print” OK, 2021. - 224 b

7.А.В.Бабаш, Е.К.Баранова, Информационная безопасность и защита информации. Учебное пособие 2019

8. А.Бирюков. Информационная безопасность: защита и нападение, 2017

9. O‘zbekiston Respublikasining 560-II-sonli «Axborotlashtirish to‘g‘risida»gi 2003 yil 11 dekabr qonuni // O‘zbekiston Respublikasi Oliy Majlisining axborotnomasi. - 2004. - № 1-2. - 10-m.

10.O‘zbekiston Respublikasining 848-XII-sonli «Davlat sirlarini saqlash to‘g‘risida»gi 1993 yil 7 may qonuni // O‘zbekiston Respublikasi Oliy Kengashining axborotnomasi. - 1993. - № 5 - 232-m.

11.O‘zbekiston Respublikasining 1060-XII-sonli «Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma’lumotlar bazasining huquqiy himoyasi to‘g‘risida»gi 1994 yil 6 may qonuni // O‘zbekiston Respublikasi Oliy Kengashining axborotnomasi. - 1994. - № 5 - 136-m.

12.O‘zbekiston Respublikasining 1006-XII-sonli «Maxsulotlar va xizmatlarni sertifikatlashtirish to‘g‘risida»gi 1993 yil 28 dekabr qonuni // O‘zbekiston Respublikasi Oliy Kengashining axborotnomasi. –T., 1994. - № 2 - 50-m.

13. CYBER SECURITY POLICY GUIDEBOOK. Jenifer L. Bayuk. Jason Healey. Paul Rohmeyer, et.c. WILLEY publisher.2018 y. 288 p. ISBN 978-1-118-02780-6

14. Cybersecurity Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (ACM, EEE-CS, AIS SIGSEC, IFIP WG 11.8) (Crosscutting concepts).

15. ISO/IEC 27000 Information technology. Security techniques. Information security management systems. Overview and vocabulary.

16. Ғаниев C.К., Каримов М.М., Ташев К.А. “Ахборот хавфсизлиги”, "Фан ва технология" нашриёти, Тошкент -2016

17. Mark Stamp. Information security. Principles and Practice. Second edition. A John Wiley& Sons, Inc., publication. Printed in the United States of America. 201l y. 584p.

18. Шангин В.Ф. «Комплекскная защита информации в корпоративных системах». Учебное пособие. М.: ИД «ФОРУМ» - ИНФРА - М. 2019. 591 с

19. Tim Boyles. CCNA Security Study Guide. Copyright © 2010 by Wiley Publishing, Inc., Indianapolis, Indiana. Published simultaneously in Canada ISBN: 978-0-470-52767-2

20. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности, 2014 г. 130 стр.

21. Шангин В.Ф., «Комплексная защита информации в корпоративных системах», Учебное пособие. М.: ИД. «ФОРУМ» - ИНФРА М. 2019, 591с.

22. Баранова Е.К.,Бабаш А.В. «Информационная безопасность и защита информации». Учебное пособие. М.:РИОР:ИНФРА-М, 2019.336с.

23. Katz J., Lindell Y. Introduction to modern cryptography. – CRC press, 2014

24. Stamp M. Information security: principles and practice. – New York : Wiley, 2011. – T. 2.

25. Akbarov D. Ye. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” – Toshkent, 2008 – 394 bet.

26. Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o‘quv qo‘llanma” – Toshkent, 2021 – 206 bet.

27.Kiberxavfsizlik asoslari: O‘quv qo‘llanma / S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: “Iqtisod-Moliya”, 2021. – 228 b.

**QО‘SHIMCHA ADABIYOTLAR RО‘YXATI**

|  |  |
| --- | --- |
|  | O‘zbekistan Respublikasi Prezidentining 2022 yil 28 yanvardagiPF-60-son “2022 – 2026-yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida” gi Farmoni. |
|  | Mirziyoev Sh.M. Qonun ustuvorligi va inson manfaatlarini ta’minlash - yurt taraqqiyoti va xalq farovonligining garovi. 2017. |
|  | F.M.Muxtorov., D.X.Tojimatov., Sh.N.G‘aniyeva. Taxdid razvedkasi texnologiyalari. Farg‘ona “Classic”. 2023 yil. 170 bet |
|  | Г.Богомазова. Обезпечение информационной безапасности компьютерных сетей. "Академия" (2017) |
|  | Tim Boyles. CCNA Security Study Guide. Copyright © 2010 by Wiley Publishing, Inc., Indianapolis, Indiana. Published simultaneously in Canada ISBN: 978-0-470-52767-2. |
|  | Mark Ciampa. Security+.Guide to Network Security Fundamentals. Fifth Edition. Printed in the United States of America Print Number: 01 Print Year: 2014 |
|  | Emad S. Hassan. Security and Data Reliability in Cooperative Wireless Networks. © 2018 by Taylor & Francis Group, LLC |
|  | William Stallings. Cryptography and network security principles and practice. Fifth edition. Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall. |
|  | Joseph Migga Kizza. Computer Network Security and Cyber Ethics. Fourth edition. McFarland & Company, Inc., Publishers Jefferson, North Carolina © 2014. |
|  | Мирзиёев Ш.М. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. 2017 |
|  | Мирзиёев Ш.М. Қонун устуворлиги ва инсон манфаатларини таъминлаш – юрт тараққиёти ва халқ фаровонлигининг гарови. 2017 |
|  | Мирзиёев Ш.М. Эркин ва фаровон, демократик Ўзбекистон давлатини биргаликда барпо этамиз. 2017 |
|  | Мирзиёев Ш.М. Танқидий таҳлил, қатъий тартиб-интизом ва шахсий жавобгарлик – ҳар бир раҳбар фаолиятининг кундалик қоидаси бўлиши керак. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2016 йил якунлари ва 2017 йил истиқболларига бағишланган мажлисидаги Ўзбекистон Республикаси Президентининг нутқи. // Халқ сўзи газетаси. 2017 йил 16 январ, № 11. |
|  | Common Criteria for Information Technology Security Evaluation. Part III: Security Assurance Components [V Internete] // Common Criteria Portal. – 2012 |
|  | Бирюков, А.А. Информационная безопасност: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 c. |
|  | Joseph Migga Kizza. Computer Network Security and Cyber Ethics. Fourth edition. McFarland & Company, Inc., Publishers Jefferson, North Carolina © 2014. |
|  | William Stallings. Cryptography and network security principles and practice. Fifth edition. Copyright © 2011, 2006 Pearson Education, Inc., publishing as Prentice Hall. |
|  | Emad S. Hassan. Security and Data Reliability in Cooperative Wireless Networks. © 2018 by Taylor & Francis Group, LLC |
|  | Common Criteria for Information Technology Security Evaluation. Part III:Security Assurance Components [В Интернете] // Common Criteria Portal. – 2012 |
|  | Бирюков А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 c. |
|  | O’zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi PF-4947-son «O’zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida» gi Farmoni. |
|  | O’zbekiston Respublikasi Prezidentining 2007 yil 3 apreldagi PQ-614-son «O’zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida»gi Qarori. |
|  | Aumasson J. P. Serious cryptography: a practical introduction to modern encryption. – No Starch Press, 2017. |
|  | Akbarov D.Y., Xasanov P.F., Xasanov X.P., Axmedova O.P., Xolimtayeva I.U. “Kriptografiyaning matematik asoslari” - Aloqachi, 2019 – 192 bet. |
|  | Sen J. Homomorphic encryption-Theory and Application //Theory and Practice of Cryptography and Network Security Protocols and Technologies. – 2013. – S. 1-21. |

**Internet saytlar**

1. <http://www.tuit.uz>
2. <http://www.ziyonet.uz>
3. <http://www.cert.uz>
4. <http://www.uzinfocom.uz>