"Киберқауіпсіздік саласындағы қызмет" Кәсіптік стандартын бекіту туралы

Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2025 жылғы 30 маусымдағы № 329/НҚ бұйрығы

Қазақстан Республикасының "Кәсіптік біліктіліктер туралы" Заңының 5-бабының 5-тармағына сәйкес БҰЙЫРАМЫН:

1. Қоса беріліп отырған "Киберқауіпсіздік саласындағы қызмет" кәсіптік стандарт бекітілсін.

2. Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті Қазақстан Республикасының заңнамасында белгіленген тәртіппен қамтамасыз етсін:

1) күнтізбелік бес күн ішінде қол қойылғаннан кейін осы бұйрықтың қазақ және орыс тілдерінде "Қазақстан Республикасының Заңнама және құқықтық ақпарат институты" Қазақстан Республикасы Әділет министрлігінің ресми жариялау және енгізу үшін нормативтік құқықтық актілердің эталондық бақылау банкіне Қазақстан Республикасының құқықтық актілерінің шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберілуін қамтамасыз етсін;

2) осы бұйрықты Қазақстан Республикасы Әділет министрлігіне орналастыру интернет-ресурста Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің ресми жарияланғанынан кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі вице-министріне жүктелсін.

4. Осы бұйрық алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасының
Цифрлық даму, инновациялар және
аэроғарыш өнеркәсібі Министрі *Ж. Мәдиев*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Еңбек және халықты әлеуметтік
қорғау министрлігі

Бұйрықпен бекітілді

Кәсіптік стандарт: "Киберқауіпсіздік саласындағы қызмет"

1-ші тарау. Жалпы ережелер

1. Кәсіптік стандарттың қолдану аясы: Кәсіби стандарт "Киберқауіпсіздік саласындағы қызмет" Қазақстан Республикасының "Кәсіптік біліктілік туралы" Заңының 5-бабына сәйкес әзірленген және өтініш берушіге жұмысқа орналасуға қойылатын талаптарды қалыптастыруда, білім беру бағдарламаларын қалыптастыруда, оның ішінде кәсіпорындарда кадрларды даярлауда, білім беру ұйымдарының қызметкерлері мен түлектерінің кәсіби біліктілігін тануда, сондай-ақ ұйымдар мен кәсіпорындардағы персоналды басқару саласындағы міндеттер кең ауқымды мәселелерді шешуде қолданылуы мүмкін.

2. Осы кәсіптік стандартта мынадай терминдер, анықтамалар мен қысқартулар қолданылады:

1) Салалық біліктілік шеңберлері (СБШ) – ұлттық біліктілік жүйесінің құрамдас бөлігі (ішкі жүйесі), салада мойындалатын біліктіліктің сараланған деңгейлерінің негіздемелік құрылымы

2) еңбек қызметінің түрі – кәсіптік топтың бір бөлігі, еңбек функцияларының тұтас жиынтығымен қалыптасатын кәсіптер жиынтығы және қажеттіх олардың құзыреттерін орындау үшін

3) Еңбек функциясы (функциясы) – еңбек процесінің бір немесе бірнеше мәселелерін шешуге бағытталған өзара байланысты іс-шаралар жиынтығы

4) Кәсіби міндет (міндет) – еңбек функциясын жүзеге асыруға және белгілі бір кәсіптік топта немесе кіші топта қажетті нәтижеге қол жеткізуге байланысты іс-әрекеттер туралы нормативтік түсінік

5) Мамандық – білімі және/немесе жұмыс тәжірибесі туралы тиісті құжаттармен расталған, арнайы дайындық нәтижесінде алынған арнайы теориялық білімдердің, дағдылардың және практикалық дағдылардың кешенін меңгеруді талап ететін адамның еңбек қызметінің негізгі кәсібі

6) Лауазым – ұйымның ұйымдық-әкімшілік иерархиясы жүйесіндегі функционалдық орны, қызметкердің қызметтік жағдайы

7) Сабақ – орындалатын негізгі міндеттер мен міндеттердің жоғары дәрежеде сәйкес келуімен сипатталатын, табыс немесе табыс әкелетін жұмыс орнында орындалатын жұмыстар жиынтығы

8) Білімдер – жеке және кәсіби қызметте пайдаланылатын ақпарат, нормалар

9) Қабілет – екі белгісі бар белгілі бір кәсіп шеңберінде нақты тапсырмалар мен міндеттерді орындау қабілеті: - дағдылар деңгейі орындалатын міндеттер мен міндеттердің күрделілігі мен көлемін анықтайды; - дағдыларды мамандандыру пайдаланылатын білім саласын, пайдаланылатын құралдар мен жабдықтарды, өңделетін немесе пайдаланылатын материалдарды және өндірілетін тауарлар мен көрсетілетін қызметтердің түрлерін ескере отырып, орындалатын міндеттер мен міндеттердің сипаты мен шеңберін айқындайды.

10) Құзыреттілік – қызметкердің кәсіби стандарттардың талаптарына сәйкес еңбек функцияларын сапалы орындауын қамтамасыз ететін білімнің, дағдылардың, тәжірибенің және қарым-қатынастардың (құндылықтардың) органикалық тұтастығы

11) Біліктілік – білім беру, оқыту немесе еңбек қызметі процесінде қалыптасқан кәсіптік қызметтің белгілі бір түрі (кәсіптік стандарттың талаптары немесе тәжірибе нәтижесінде қалыптасқан талаптар) шеңберінде еңбек функцияларын орындауға қойылатын талаптарға сәйкес келетін тұлғаның құзыреттері бар екенін растайтын диплом, сертификат түріндегі құндылықты ресми тану (еңбек қызметін жүзеге асыруға құқық беретін жұмыс орнында оқыту;

3. Осы кәсіптік стандартта мынадай қысқартулар қолданылады

1) IPsec – Internet Protocol Security

2) NGFW – Next-Generation Firewall

3) DLP – Data Loss Prevention

4) IDS – Intrusion Detection System

5) АКТ – Ақпараттық-коммуникациялық технологиялар

6) АТ – Ақпараттық технологиялар

7) АЖ – Ақпараттық жүйелер

8) БҚ – Бағдарламалық қамтылым

9) СБШ – Салалық біліктілік шеңбері

10) КС – Кәсіби стандарт

11) КҚБЖ – Конструкторлық құжаттаманың бірыңғай жүйесі

12) ТҚБЖ – Технологиялық құжаттаманың бірыңғай жүйесі

13) БҚБЖ – Бағдарламалық құжаттаманың бірыңғай жүйесі

14) БТБА немесе БА – Жұмысшылардың жұмыстары мен кәсіптерінің бірыңғай тарифтік-біліктілік анықтамалығы немесе басшылар, мамандар және басқа қызметкерлер лауазымдарының біліктілік анықтамалығы

15) ЭҚЖЖ – Экономикалық қызмет түрлерінің жалпы жіктеуіші

16) БАҚ – Бағдарламалық-аппараттық құралдар

17) ДБ – Деректер базасы

18) БХСЖ – Білім берудің халықаралық стандартты жіктемесі

19) НҚА – нормативтік-құқықтық актілер

20) НТҚ – нормативтік-техникалық құжаттама

21) АТҚ – ақпаратты техникалық қорғау

22) ЖЭСН – жанама электромагниттік сәулелену және нысаналар

23) АТКТА – ақпараттың таралып кетуінің техникалық арналары

24) АҚ – ақпараттық қауіпсіздік

25) ДББЖ – Деректер базасымен басқару жүйесі

26) ОЖ – Операциялық жүйе

27) –

28) –

2-ші тарау. Кәсіптік стандарттың паспорты

4. Кәсіптік стандарттың атауы: "Киберқауіпсіздік саласындағы қызмет"

5. Кәсіптік стандарттың коды: J056

6. ЭҚЖЖ секциясын, бөлімін, тобын, сыныбын және кіші сыныбын көрсету:

J Ақпарат және байланыс

62 Компьютерлік бағдарламалау, консультациялық және басқа ілеспе көрсетілетін қызметтер

62.0 Компьютерлік бағдарламалау, консультациялық және басқа ілеспе көрсетілетін қызметтер

62.09 Ақпараттық технолгиялар және ақпараттық жүйелер саласындағы қызметтің басқа да түрлері

62.09.9 Басқа топтамаларға енгізілмеген, ақпараттық технологиялар мен ақпараттық жүйелер саласындағы қызметтің басқа да түрлері

7. Кәсіптік стандарттың қысқаша сипаттамасы: Ақпараттық қауіпсіздікке төнетін қатерлер жағдайында компьютерлік жүйелер мен желілердегі ақпараттың қауіпсіздігін қамтамасыз ету

8. Кәсіптер карточкаларының тізімі:

2) Цифрлық технологиялар жөніндегі маман-криминалист - 6 СБШ-нің деңгейі

3) Қауіпсіздік мәселелері жөніндегі маман (АКТ) - 7 СБШ-нің деңгейі

7) Сервистердің қауіпсіздігі жөніндегі маман - 6 СБШ-нің деңгейі

8) Ақпараттық қауіпсіздік аудиторы - 6 СБШ-нің деңгейі

9) Деректерді шифрлаушы - 6 СБШ-нің деңгейі

10) Ақпараттық қауіпсіздік аудиторы - 7 СБШ-нің деңгейі

11) Ақпараттық қауіпсіздік жөніндегі маман - 7 СБШ-нің деңгейі

12) Ақпараттық қауіпсіздік жөніндегі маман - 6 СБШ-нің деңгейі

13) Ақпаратты қорғау жөніндегі инженер - 6 СБШ-нің деңгейі

14) Ақпаратты қорғау жөніндегі инженер - 7 СБШ-нің деңгейі

15) Сервистердің қауіпсіздігі жөніндегі маман - 7 СБШ-нің деңгейі

16) Деректерді шифрлаушы - 7 СБШ-нің деңгейі

17) Цифрлық технологиялар жөніндегі маман-криминалист - 7 СБШ-нің деңгейі

18) Ақпараттық қауіпсіздік жөніндегі әкімші - 7 СБШ-нің деңгейі

19) Ақпаратты қорғау жөніндегі маман - 7 СБШ-нің деңгейі

20) Қауіпсіздік мәселелері жөніндегі маман (АКТ) - 6 СБШ-нің деңгейі

21) Ақпаратты қорғау жөніндегі маман - 6 СБШ-нің деңгейі

3-ші тарау. Кәсіптер карточкалары

10. Кәсіптің карточкасы "Цифрлық технологиялар жөніндегі маман-криминалист":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-008		
Кәсіптің атауы:	Цифрлық технологиялар жөніндегі маман-криминалист		
СБШ бойынша біліктілік деңгейі:	6		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Талдау және болатын оқиғаларды зерттеу компьютерлік ақпарат қол сұғушылық объектісі ретінде, компьютер қылмыс жасау құралы ретінде, сондай-ақ кез келген цифрлық дәлелдемелер пайда болады		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Компьютерлік қылмыстарды тергеу 2. Цифрлық құрылғылар мен жабдықтардың криминалистикалық сараптамасы	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Оқыс оқиғалардың туындау көздері мен себептерін анықтау; 2. Анықталған оқыс оқиғалардың салдарын бағалау; 3. Корпоративтік желіге енулерді анықтау; 4. Зиянкестердің ұйым желісіне кіруінің барлық белгіленген тәсілдерін жою; 5. Оқиғаның пайда болу механизмі мен мән-жайларының құрылымын талдау; 6. Бағдарламалық қамтамасыз етуді өзгертудің себебі мен шарттарын анықтау; 7. Ақпараттың белгілі бір дереккөзге тиесілігін анықтауға мүмкіндік беретін қасиеттері мен ерекшеліктерін бөліп көрсету; 8. Қолда бар ақпараттың оның ішінде жүйедегі орналасуын сәйкессіздігін анықтау.	

Еңбек функциясы 1: Компьютерлік қылмыстарды тергеу	Дағды 1: Компьютерлік қылмыстарға алғашқы ден қою	Білімдер: 1. Компьютерлік қылмыстардың негізгі түрлері; 2. Зиянкестердің ұйым желісіне кіру жолдары; 3. Ақпараттық қауіпсіздіктің негізгі қатерлері және ұйымның АЖ-да бұзушының модельдері; 4. Ақпаратты беру жүйелері мен желілерін құру және олардың жұмыс істеу принциптері; 5. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттар; 6. Ақпараттың "таралып кетуінің" техникалық арналары; 7. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер; 8. Ашық жүйелердің өзара әрекеттесуінің эталондық моделі, негізгі хаттамалар, заманауи жергілікті және ғаламдық компьютерлік желілерді құру және олардың жұмыс істеу кезеңдерінің реттілігі мен мазмұны; 9. Ақпараттандырудың техникалық құралдарына техникалық қызмет көрсетуді ұйымдастырудың және жүргізудің негізгі әдістері; 10. Ақпаратты қорғау жөніндегі ұйымдастырушылық шаралар; 11. Анықталған инциденттерді есепке алу регламенті; 12. Форматтары компьютерлік жүйеде талданатын ақпаратта ақпаратты сақтау; 13. Компьютерлік жүйелерде қолданылатын негізгі файл пішімдері; 14. Компьютерлік қылмыстардың, құқық бұзушылықтар мен оқыс оқиғалардың іздерін тіркеу және құжаттау тәртібі; 15. Компьютерлік ақпарат саласындағы қылмыстық және әкімшілік құқықтың нормалары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Бұзушылықтардың алдын алу және уақтылы анықтау шараларын әзірлеу; 2. Компьютерлерден анықтамалық ақпаратты іздеуді жүргізу; 3. Қарсы криминалистиканың әдістері мен құралдарын анықтау: толық дискілік шифрлау, ақпаратты қашықтықтан сақтау және т.б.; 4. Дәлелдемелер базасын жинауды және оны ресімдеуді/сақтауды жүзеге асыру; 5. Ұйымға нақты әлемдегі шабуылды модельдеу және одан келетін залалды азайту үшін әрекет ету дағдыларын үйрету.
		Білімдер: 1. Ақпаратты беру жүйелері мен желілерін құру және олардың жұмыс істеу принциптері;

	Дағды 2: Бұзушылықтардың және рұқсатсыз кірудің алдын алу шараларын жоспарлау	2. Ашық жүйелердің өзара әрекеттесуінің эталондық моделін, негізгі хаттамаларды, қазіргі заманғы жергілікті және ғаламдық компьютерлік желілерді құру және олардың жұмыс істеу кезеңдерінің реттілігі мен мазмұны; 3. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттар; 4. Ақпараттық қауіпсіздіктің негізгі қатерлері және ұйымның АЖ-да бұзушының модельдері ; 5. Контр-криминалистиканың әдістері мен құралдары; 6. Ақпаратты техникалық арналар арқылы "ағып кетуден" қорғау құралдарын құру принциптері; 7. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер; 8. АЖ-да ақпаратты қорғау үшін қолданылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар; 9. Компьютерлік техниканы алып қоюдың негізгі принциптері; 10. Дәлелдемелік деректерді табудан жасыру әдістері; 11. Тергеу бойынша ақпаратты құжаттау.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеп-тексеру; 2. Инциденттің уақытын белгілеу; 3. Бастапқы медициналық көмекті жүргізу компьютерлік құрылғының диагностикасын жүргізу ; 4. Аппараттық жазба блокаторларымен және сақтау құралдарының көшірмелерімен жұмыс істеу; 5. Криминалистикалық талдау үшін дистрибутивтермен жұмыс істеу; 6. Қатты дискінің (HDD) және басқа сақтау құралдарының кескінін (бірдей көшірмесін), соның ішінде қатты дискінің бөлімінен немесе жеке секторынан кескінді алып тастаңыз; 7. Дискілердің қалыптастырылған кескіндерін өңдеуді жүргізу; 8. Қатты дискілерден деректерді жинауды жүзеге асыру; 9. Қатты дискілерде табылған файлдарды талдауды жүзеге асыру; 10. Файлдардан деректерді шығарып алу; 11. ЖЖҚ үйінділеріне зерттеу жүргізу; 12. Қатты дискіде және периферияда артефактілерді іздеуді жүргізу;

Еңбек функциясы 2: Цифрлық құрылғылар мен жабдықтардың криминалистикалық сараптамасы	Дағды 1: Компьютерлердің криминалистикалық сараптамасы	13. Операциялық жүйелер мен қолданбалы бағдарламалардың жүйелік журналдарымен және журналдарымен жұмыс істеу; 14. Жойылған деректерді қалпына келтіру; 15. Дәлелдемелер базасын жинауды және оны ресімдеуді/сақтауды жүзеге асыру; 16. Қаражатта ПЭМИННІҢ болуына зерттеулер жүргізу ЕТ.
		Білімдер: 1. Файлдық жүйелер; 2. Операциялық жүйелер; 3. Ақпараттық қауіпсіздіктің негізгі қағидаттары және қауіпсіздік техникасы жұмысының әдістері; 4. Компьютерлік криминалистика құралдарының жиынтығы; 5. Қатты дискілердің және басқа дискілердің құрылғысы ; 6. Операциялық жүйелердің архитектурасын және пайдаланушылық интерфейстері; 7. Есептеу жүйелерінің архитектурасы, құрылғысы және жұмыс істеуі, 8. Деректерді қалпына келтіруді қоса алғанда, файлдық жүйемен жұмыс істеуге арналған құралдар жинағы; 9. Ақпаратты қорғауды қамтамасыз ету үшін пайдаланылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар; 10. ТКУИ бойынша ақпаратты ұстап қалу әдістері, 11. ЕТҚ құралдарын ПЭМИН болуына зерттеу әдістемесі; 12. Мәлімделмеген техникалық мүмкіндіктердің болуына ЕТҚ құралдарына зерттеулер жүргізу әдістемесі.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2:	Машықтар: 1. Желілік стек пен браузерлерге талдау жүргізу; 2. Email-хабарламаларға талдау жүргізу және электрондық пошта мекенжайының тиесілігін анықтау; 3. Желілік трафик дампасын жасау үшін құралдармен жұмыс істеу; 4. Желілік трафикті ұстап қалуды және зерттеуді жүзеге асыру; 5. Web-серверлердің логтарын зерттеуді жүзеге асыру; 6. IP-мекенжайдың тиесілігін және орналасуын анықтау; 7. Домендік атаудың тиесілігін орнату.
		Білімдер:

	Желілік құрылғылардың криминалистикалық сараптамасы	1. Ақпарат беру жүйелері мен желілерін құру және олардың жұмыс істеу қағидаттары; 2. Ашық жүйелердің өзара іс-қимылының эталондық моделі; 3. Компьютерлік желілерде сәйкестендіру, сәйкестендіру және авторлау әдістері мен хаттамалары; 4. Желілік криминалистиканы жүргізудің негізгі қағидаттары; 6. Желілік криминалистиканы жүргізу және оларды зерттеу үшін деректер көздері; 7. Желілік трафик дампасын жасауға арналған құралдардың ерекшеліктері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: Мобильді құрылғылардың криминалистикалық сараптамасы	Машықтар: 1. Ұялы байланыс құрылғысын сәйкестендіруді жүзеге асыру 2. Сандық құрылғыдан, перифериялық жабдықтардан және ақпараттық жинақтағыштардан барлық деректерді клондауды жүзеге асырыңыз 3. Ұялы телефондардан ақпарат алуды жүзеге асыру 4. SIM-картадан ақпарат алуды жүзеге асыру 5. Кіріктірілген және сыртқы жад картасынан ақпарат алуды жүзеге асыру 6. Пошта жөнелтілімдерін, телеграфтық және өзге де хабарларды бақылауды жүзеге асыру 8. Ұялы телефон деректеріне қол жеткізу үшін бағдарламалық және аппараттық құралдармен жұмыс істеу
		Білімдер: 1. Ұялы байланыстың принциптері мен құрылғылары; 2. Ұялы телефон деректеріне қол жеткізуге арналған бағдарламалық-аппараттық құрал-сайман; 3. Ақпаратты қорғауды қамтамасыз ету үшін пайдаланылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар; 4. Мобильді операциялық жүйелер; 5. Мобильді құрылғылардың файлдық жүйелері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Күйзеліске тұрақтылық Командада жұмыс істей білу Аналитикалық ойлау Сыни ойлау	
	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
	7	Цифрлық технологиялар жөніндегі маман-криминалист	
11. Кәсіптің карточкасы "Қауіпсіздік мәселелері жөніндегі маман (АКТ)":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-005		
Кәсіптің атауы:	Қауіпсіздік мәселелері жөніндегі маман (АКТ)		
СБШ бойынша біліктілік деңгейі:	7		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Инфокоммуникациялық жүйелердің ішкі жүйелеріне, құрылғыларына, элементтеріне және арналарына бағдарламалық-техникалық әсердің зиянды әсеріне қарсы тұру		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Компьютерлік жүйелер мен желілердің қауіпсіздік деңгейін бағалау 2. Компьютерлік жүйелер мен желілердің қауіпсіздік жүйесін әзірлеу	
	Қосымша еңбек функциялары:		
		Машықтар: 1, Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс істеу параметрлерін анықтау; 2, Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қорғалуын бағалау әдістемесін әзірлеу; 3, Ақпаратты қорғаудың тиімділігін бағалау;	

		4, Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қорғалуын бағалаудың әзірленген әдістемелерін қолдану; 5, Қорғаудың бағдарламалық-аппараттық құралдарын олармен қамтамасыз етілетін қорғалу мен сенімділік деңгейін анықтау мақсатында талдау.
	Дағды 1: Нормативтік, әкімшілік, техникалық және ғылыми қамтамасыз ету қамтамасыз етумен ақпараттық инфрақұрылымның негізгі жүйелеріндегі ақпараттың қауіпсіздігі	Білімдер: 1. Компьютерлік жүйелер мен желілерді құру қағидаттары; 2. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қауіпсіздігін бағалау әдістері мен әдістемелері; 3. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын құру қағидаттары; 4. Компьютерлік жүйелердегі ақпаратты қорғаудың кіші жүйелерін құру қағидаттары; 5. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарында іске асырылған қауіпсіздік саясатының тиімділігін бағалау әдістері; 6. Ақпаратты қорғау алгоритмдерін бағдарламалық іске асырудың дұрыстығы мен тиімділігін бағалау әдістері мен құралдары; 7. Әлеуетті осалдықтар мен құжатталмаған мүмкіндіктерді іздеу мақсатында бағдарламалық кодты талдау әдістері; 8. Ақпаратты қорғаудың қолданылатын әдістері мен құралдарын қауіпсіздік саясатына сәйкестігі тұрғысынан талдау тәсілдері; 9. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар; 10. АҚ қамтамасыз ету саласындағы нормативтік құқықтық актілер.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Ақпаратты қорғаудың қолданылатын бағдарламалық-аппараттық құралдарының жұмысқа қабілеттілігі мен тиімділігіне бақылау тексерулерін жүргізу	Машықтар: 1. Қажетті қорғалу деңгейін анықтау үшін компьютерлік жүйені талдау; 2. Компьютерлік жүйелерді қорғау бейінін әзірлеу; 3. Компьютерлік жүйелердің қауіпсіздігі бойынша тапсырмаларды тұжырымдау; 4. Компьютерлік жүйелердің қауіпсіздігіне талдау жасау және ақпаратты қорғау жүйесін пайдалану жөнінде ұсынымдар әзірлеу.
		Білімдер: 1. Компьютерлік жүйелер мен желілерді құру қағидаттары; 2. Компьютерлік жүйелердің қауіпсіздік модельдері; 3. Компьютерлік жүйелер мен желілердің қауіпсіздік саясатының түрлері; 4. Ақпаратты криптографиялық қорғау құралдарын құру қағидаттары;

		5. АҚ қамтамасыз ету саласындағы ұлттық стандарттар; 6. Пайдаланылатын және пайдалануға жоспарланған ақпаратты қорғау құралдарының мүмкіндіктері; 7. АҚ қамтамасыз ету саласындағы нормативтік құқықтық актілер.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 1: Компьютерлік жүйелер мен желілердің қауіпсіздік деңгейін бағалау	Дағды 3: Компьютерлік жүйелер мен желілердің қауіпсіздік саясатын қалыптастыру	Машықтар: 1. Қорғалу деңгейін анықтау үшін компьютерлік жүйені талдау; 2. Ақпараттық қауіпсіздікті бұзушының іс-қимылдарын дамытудың ықтимал жолдарын болжау; 3. Барабарлық мәніне қауіпсіздік саясатына талдау жүргізу; 4. Операциялық жүйелерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының тиімділігіне мониторинг, талдау және салыстыру жүргізу; 5. жүргізілген талдау нәтижелері бойынша талдамалық есеп жасау және ресімдеу; 6. Анықталған осалдықтарды жою бойынша ұсыныстар әзірлеу.
		Білімдер: 1. Компьютерлік жүйелер мен желілерді құру қағидаттары; 2. Компьютерлік жүйелер мен желілердің осалдықтары; 3. ақпаратты қорғаудың криптографиялық әдістері; 4. Деректер базасын басқару жүйелерін құру қағидаттары; 5. Конфигурацияларды талдау құралдары; 6. АҚ қамтамасыз ету саласындағы ұлттық стандарттар; 7. АҚ қамтамасыз ету саласындағы нормативтік құқықтық актілер.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Қорғалу және сенім деңгейін анықтау үшін компьютерлік жүйені талдау; 2. Ақпараттық қауіпсіздікті бұзушының іс-қимылын дамытудың ықтимал жолдарын болжау; 3. Қауіпсіздік саясатына барабарлық тұрғысынан талдау жүргізу; 4. Операциялық жүйелерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының тиімділігіне мониторинг, талдау және салыстыру жүргізу;

		5. Жүргізілген талдау нәтижелері бойынша талдамалық есеп жасайды және ресімдейді; 6. Анықталған осалдықтарды жою бойынша ұсыныстар әзірлеу; 7. ТҚИ шеңберінде іс-шараларды жүзеге асыру; 8. ЕТҚ құралдарында ПЭМИН болуына зерттеу жүргізу.
	Дағды 4: Компьютерлік жүйелердің қауіпсіздігіне талдау жүргізу	Білімдер: 1. Компьютерлік жүйелер мен желілерді құру принциптері; 2. Компьютерлік жүйелер мен желілердің осалдықтары; 3. Ақпаратты қорғаудың криптографиялық әдістері; 4. Деректер қорын басқару жүйелерін құру принциптері; 5. Конфигурацияларды талдау құралдары; 6. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар; 7. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер; 8. Ақпаратты қорғау жөніндегі уәкілетті федералдық атқарушы органдардың нұсқаулық және әдістемелік құжаттары; 9. Ақпаратты қорғау жөніндегі ұйымдастырушылық шаралар; 10. ТКУИ бойынша ақпаратты ұстап қалу әдістері; 11. ЕТҚ құралдарын ПЭМИН болуына зерттеу әдістемесі; 12. Өткізу әдістемесін мәлімделмеген техникалық мүмкіндіктердің болуына ЕТҚ құралдарын зерттеу.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1:	Машықтар: 1. Қатерлердің модельдерін және компьютерлік жүйелердің қауіпсіздігін бұзушының модельдерін қалыптастыру; 2. Компьютерлік жүйенің ақпаратын қорғауды қамтамасыз етудің неғұрлым орынды тәсілдерін анықтау; 3. Компьютерлік жүйелер қауіпсіздігінің жеке саясатын, оның ішінде қолжетімділік пен ақпараттық ағындарды басқару саясатын әзірлеу; 4. Компьютерлік жүйенің қорғалуын бағалау үшін ақпаратты қорғау саласындағы ұлттық стандарттарды қолдану; 5. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын пайдалану қажеттілігі туралы шешім қабылдауды жүзеге асыру.
		Білімдер: 1. Ақпаратты қорғау жөніндегі жұмыстарды ұйымдастыру тәртібі;

	Компьютерлік жүйелер мен желілердің ақпаратын қорғаудың бағдарламалық-аппараттық құралдарына қойылатын талаптарды әзірлеу	2. операциялық жүйелерде, деректер базасын басқару жүйелерінде және компьютерлік желілерде ақпаратты алу, өңдеу және беру әдістері мен құралдары; 3. Компьютерлік жүйелердің қауіпсіздігін талдау әдістері; 4. Компьютерлік жүйелерде шабуылдардың түрлері және оларды іске асыру тетіктері; 5, Ақпараттың таралу арналарын анықтау әдістері; 6. Компьютерлік желілерде, операциялық жүйелерде және дерекқорларды басқару жүйелерінде ақпаратты қорғау әдістері мен құралдары; 7. Компьютерлік жүйелердің ақпаратын қорғау құралдарын құру қағидаттары; 8. кіруді басқарудың формальды модельдері; 9. Криптографиялық алгоритмдер және оларды бағдарламалық іске асыру ерекшеліктері; 10. АҚ қамтамасыз ету саласындағы нормативтік құқықтық актілер; 12. АҚ қамтамасыз ету саласындағы ұлттық стандарттар.
Еңбек функциясы 2: Компьютерлік жүйелер мен желілердің қауіпсіздік жүйесін әзірлеу	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Компьютерлік жүйелер мен желілердің ақпаратын қорғауға арналған бағдарламалық және аппараттық құралдарды жобалау	Машықтар: 1. Ақпаратты қорғауды қамтамасыз ету бойынша неғұрлым орынды практикалық шешімдерді табу үшін зерттеулер жүргізу; 2. Ақпаратты қорғау құралдарының архитектурасын және интерфейстерін 3. Істен шыққаннан кейін қорғау құралдары мен жүйелерінің жұмысқа қабілеттілігін қалпына келтіру рәсімдерін жүргізу.
		Білімдер: 1. Операциялық жүйелерде, деректер базасын басқару жүйелерінде және компьютерлік желілерде ақпаратты алу, өңдеу және беру әдістері мен құралдары; 2. Компьютерлік жүйелерде шабуылдардың түрлері және оларды іске асыру тетіктері; 3. Компьютерлік желілерде, операциялық жүйелерде және дерекқорларды басқару жүйелерінде ақпаратты қорғау әдістері мен құралдары; 4. Компьютерлік жүйелердің ақпаратын қорғау жүйелерін, оның ішінде вирусқа қарсы бағдарламалық қамтамасыз етуді құру қағидаттары; 5. Компьютерлік жүйелердің қауіпсіздігін талдау әдістері; 6. Ақпаратты қорғау құралдарында қолданылатын теориялық-сандық әдістер мен алгоритмдер; 7. Кіруді басқарудың формальды модельдері;

		8. Бағдарламалық-аппараттық қамтамасыз етуді жобалау қағидаттары мен әдістері; 9. Бағдарламалық қамтамасыз етуді әзірлеу әдіснамасы мен технологиялары; 10. Ақпараттық қауіпсіздік саласындағы жобаларды басқару қағидаттары мен әдістері; 11. Криптографиялық алгоритмдер және оларды бағдарламалық іске асыру ерекшеліктері; 12. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер; 13. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары; 14. Ақпаратты қорғау саласындағы ұлттық стандарттар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Аналитикалық ойлау Сыни талдау Жүйелік ойлау Стандартты емес мәселелерді шеше білу Егжей-тегжейге назар аудару	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	6	Қауіпсіздік мәселелері жөніндегі маман (АКТ)
15. Кәсіптің карточкасы "Сервистердің қауіпсіздігі жөніндегі маман":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-004	
Кәсіптің атауы:	Сервистердің қауіпсіздігі жөніндегі маман	
СБШ бойынша біліктілік деңгейі:	6	
СБШ бойынша біліктілік ішкі деңгейі:	-	
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:		
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:		

Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда АТ білім беру	
Кәсіптің басқа ықтимал атаулары:		
Қызметтің негізгі мақсаты:	Рұқсатсыз кіру үшін жүйенің осалдықтарын іздеу және анықтау	
Еңбек функциялардың сипаттамасы		
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Компанияның веб-қосымшаларының шабуылдарға төзімділігін тексеру 2. Сындарлы сервистердің бағдарламалық кодының осалдықтарын іздеу және жою
	Қосымша еңбек функциялары:	
Еңбек функциясы 1: Компанияның веб-қосымшаларының шабуылдарға төзімділігін тексеру	Дағды 1: Web-сервер архитектурасының қауіпсіздігін талдау және тексеру	Машықтар: 1. Осалдықтар туралы ақпарат жинау құралдары мен әдістерін қолдану; 2. Осалдықтар туралы алынған деректерді талдау; 3. Шектілік дәрежесі бойынша осалдықтарды жіктеу және басымдық беру; 4. Анықталған осалдықтарға байланысты әлеуетті қатерлер мен тәуекелдерді анықтау.
		Білімдер: 1. Осалдықтарды талдау әдіснамасы; 2. Осалдықтар туралы ақпарат көздері (осалдықтардың дерекқорлары, қауіпсіздік есептері); 3. Шабуылдардың негізгі түрлері және олардың салдары; 4. Қауіпсіздікті тестілеудің негізгі қағидаттары мен әдістері; 5. Қатерлер мен тәуекелдерді талдаудың қазіргі заманғы тәсілдері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Шабуыл векторларының сипаттамасы және тәуекелдерді бағалау	Машықтар: 1. Әзірлеушілер үшін осалдықтарды жою бойынша міндеттерді тұжырымдау; 2. Осалдықтарды түзету бойынша ұсынымдар әзірлеу; 3. Осалдықтарды түзету процесін бақылау және оның нәтижесін бағалау; 4. Қауіпсіздік мәселелері бойынша сервистерді әзірлеу және басқару командаларымен өзара іс-қимыл жасау; 5. Енгізілген түзетулердің дұрыстығын тексеру.
		Білімдер: 1. Желілік шабуылдарды болдырмау әдістері; 2. Корпоративтік желінің сыртқы периметрінің қорғалуын талдау әдістері;

		3. Аудит объектісінің ішкі АТ-инфрақұрылымының қорғалуын талдау әдістері; 4. БҚ тестілеуді өткізу әдістері мен тәртібі; 5. Бағдарламалау тілдері (Python, Bash, PowerShell, JS, SQL).
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Сындарлы сервистердің бағдарламалық кодының осалдықтарын іздеу және жою	Дағды 1: Сервистердің барлық ықтимал осалдықтарын анықтау, бағалау және жою	Машықтар: 1. Ақпараттық қауіпсіздік мәселелері бойынша талдамалық және сараптамалық материалдар әзірлейді; 2. Топ-менеджмент пен техникалық мамандарды қоса алғанда, әртүрлі мақсатты аудиториялар үшін күрделі техникалық мәліметтерді бейімдеу; 3. Қауіпсіздік саласында ақпараттық ілгерілету стратегиясын қалыптастыру; 4. Мамандандырылған басылымдарда және кәсіби платформаларда жарияланымдарды ұйымдастыру; 5. Жарияланымдардың құпиялылық талаптарына және нормативтік талаптарға сәйкестігін бақылау.
		Білімдер: 1. Мәтіндік және кестелік деректердің кең таралған форматтарының стандарттары; 2. Жарнамалық мәтіндерді жасау әдістері; 3. ҚР зияткерлік меншік саласындағы заңнамасы; 4. Ақпараттық материалдарды Интернетте пайдалану қағидалары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Жақсарту бойынша ұсыныстар беру ақпараттық сервистердің қауіпсіздігі	Машықтар: 1. Бизнестің қажеттіліктері мен саланың ерекшеліктерін ескере отырып, өнімді көрсету сценарийлерін әзірлеу; 2. Демонстрациялық материалдарды тапсырыс берушілер мен әріптестердің әртүрлі санаттарына бейімдеу; 3. Өнімнің бәсекелестік артықшылықтарын дәлелдеп ұсыну; 4. Презентация процесін басқару, аудиторияны тарту және сұрақтарға тиімді әрекет ету; 5. Көрсетілімнің тиімділігін талдау және өнімді жетілдіру бойынша ұсыныстар әзірлеу.
		Білімдер: 1. Өнімнің құрылғылары мен мүмкіндіктері; 2. Бағдарламаларды басқару; 3. Тиімділік көрсеткіштері; 4. Қауіпсіз IT-шешімдерді әзірлеудің және ықпалдастырудың қазіргі заманғы тәсілдері; 5. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар.

	Дағдыны тану мүмкіндігі:	Талап етілмейді	
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Ойлау икемділігі Командада жұмыс істей білу Тәртіптілік Бастамашылық Ұйымшылдық Зейінділік Еңбекқорлық Нәтижеге бағдарлану Жоғары оқу қабілеті		
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
	7	Сервистердің қауіпсіздігі жөніндегі маман	
16. Кәсіптің карточкасы "Ақпараттық қауіпсіздік аудиторы":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-002		
Кәсіптің атауы:	Ақпараттық қауіпсіздік аудиторы		
СБШ бойынша біліктілік деңгейі:	6		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:	Ақпараттық қауіпсіздік жөніндегі аудитор		
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Тәуекелдерді бағалау және оның жұмыс істеуін және қауіпсіздік шараларын сақтауды қамтамасыз ету үшін деректерді өңдеу жүйесіне сынақтар жүргізу		
Еңбек функциялардың сипаттамасы			
		1. Аудиторлық тапсырманың міндеттерін жоспарлау	

Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	2. Аудиторлық тапсырманың міндеттерін қамтамасыз ету 3. Аудиторлық тапсырманың міндеттерін орындау
	Қосымша еңбек функциялары:	
Еңбек функциясы 1: Аудиторлық тапсырманың міндеттерін жоспарлау	Дағды 1: Ақ аудиторының жұмысын жоспарлау	Машықтар: 1. Қауіптерді сәйкестендіру және бағалау үшін тәуекелдерді талдау әдістемелерін пайдалану. 2. Ақпараттық жүйелердегі қауіптерді азайту және осалдықтарды жою бойынша кешенді стратегияларды әзірлеу. 3. Ұйымға ықтимал қатерлердің әсерін бағалау, тәуекелдерді төмендету жөніндегі жоспарларды әзірлеу.
		Білімдер: 1. Сапалық та, сандық та әдістерді қоса алғанда, тәуекелдерді талдау әдістері. 2. Тәуекелдерді басқару және оларды азайту қағидаттары. 3. Тәуекелдерді талдауды және осалдықтарды бағалауды жүргізуге арналған құралдар мен технологиялар. 4. Қатерлерді болжау үшін Big Data пайдалануды қоса алғанда, тәуекелдерді талдаудың қазіргі заманғы әдіснамалары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Аудиторлық тексеруді жоспарлау	Машықтар: 1. Ұйым үшін қауіпсіздік саясатын, стандарттарды және ақпаратты қорғау рәсімдерін әзірлеу; 2. Стандартталған қауіпсіздік процестерін енгізу, оларды ұйымның қажеттіліктеріне бейімдеу; 3. Саясатты тұрақты жаңарту арқылы ұйымда қауіпсіздік мәдениетін қалыптастыру және қолдау.
		Білімдер: 1. Ақпараттық қауіпсіздік саясатын әзірлеудің қағидаттары мен тәсілдері; 2. Қауіпсіздік саясатын әзірлеу және енгізу саласындағы ұлттық стандарт; 3. Корпоративтік инфрақұрылым деңгейінде ақпаратты қорғау технологиялары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Аудиторлық қызметті регламенттейтін әдістемелік және ұйымдастырушылық-өкімдік құжаттарды әзірлеуге (өзектендіруге) қатысу; 2. Әдістемелік және ұйымдастырушылық-өкімдік құжаттардың тұсаукесерін өткізу;

	Дағды 1: АҚ аудитін әдістемелік қамтамасыз ету	3. Қызметкерлерді регламенттеуші құжаттамамен таныстыру.
		Білімдер: 1. Әдістемелік және ұйымдастырушылық-өкімдік құжаттарды әзірлеу, ресімдеу және бекіту тәртібі; 2. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар; 3. Персоналды АҚ аудитін қамтамасыз етудің әдістемелік құжаттарымен танысудың тиімді әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Аудиторлық тапсырманың міндеттерін қамтамасыз ету	Дағды 2: АҚ аудитін ұйымдастырушылық қамтамасыз ету	Машықтар: 1. Тексерілетін ұйымның (бөлімшенің) өкілдерімен АҚ аудиті мәселелері бойынша өзара іс-қимылды ұйымдастыруға қатысу; 2. Ақпаратқа қол жеткізу және беру тәртібі, сақтау мәселелері бойынша басшылық құжаттарды (бұйрықтар, өкімдер, нұсқаулықтар) жинауды жүзеге асырады; 3. АҚ аудитін жүргізу.
		Білімдер: 1. Іскерлік коммуникацияның кезеңдері мен нысандары; 2. Іскерлік ортадағы қарым-қатынас қағидаттары мен қағидалары; 3. АҚ аудитін жүргізу тәртібі.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: Ұйым қызметкерлерінің АҚ аудиті мәселелері жөніндегі кеңес беру және нұсқаулық өткізу	Машықтар: 1. Қызметкерлерді деректерді қорғау әдістеріне және қауіпсіз жұмыс ортасын құруға оқыту. 2. Қауіпсіздік саясатын, ақпараттық технологияларды қауіпсіз пайдалану жөніндегі ұсынымдарды сақтау мәселелері бойынша консультация беру. 3. Ағымдағы қауіптер және олардың алдын алу әдістері туралы басшылық үшін тұрақты консультациялар өткізу.
		Білімдер: 1. Деректерді қорғау қағидаттары, қауіпсіздік стандарттарының сақталуын бақылау әдістері. 2. Қызметкерлер үшін психология және қауіпсіздік талаптары. 3. Ұйымда қауіпсіздік саясатын құру және қолдау үшін процестер мен рәсімдер.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар:

Дағды 1: Жобаның сәйкестігін тексеру және талдау, АКТ және АҚ аудит объектісінің АҚ қамтамасыз ету саласындағы НҚА және НТҚ талаптары бойынша пайдалану	1. Деректерді қорғау жүйесін жақсарту бойынша тұжырымдары мен ұсынымдары бар есептерді жасау, 2. Аудит нәтижелерін ішкі және (немесе) сыртқы аудиторлармен талқылау және ұсыну; 3. Есепті қабылдауды және шешім қабылдауды жақсарту үшін деректерді визуализациялауды жүргізу.
	Білімдер: 1. Есептілік негіздері және қауіпсіздік тиімділігінің өлшемдері; 2. Ақпараттандыру саласындағы заңнама; 3. Нормативтік талаптар мен сертификаттарға сәйкестікті қамтамасыз ету тәсілдері.
Дағдыны тану мүмкіндігі:	Талап етілмейді
Дағды 2: АКТ саласындағы НҚА және НТҚ талаптарының нақты сақталуын және АҚ аудит объектісінің АҚ қамтамасыз ету процестерінде АҚ қамтамасыз етуді тексеру және талдау	Машықтар: 1. АЖ-да жобалық-пайдалану құжаттамасын жинау және зерделеу, қызметкерлермен сұхбаттасу және ақпаратты тіркеу. 2. АҚ аудит объектісіне НҚА мен НТҚ қолданылуын бағалау. 3. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қабылданған ұйымдастырушылық және бағдарламалық-техникалық шешімдердің нормативтік құқықтық актілер мен ғылыми-техникалық құжаттаманың талаптарына сәйкестігін бағалау. 4. Анықтау және бағалау аудит объектісінің ресурстарына және қорғаныстың осалдықтарына қатысты ықтимал қауіпсіздік қатерлері. 5. АҚ аудит объектісінің ресурстарына қатысты қауіпсіздікке төнетін қатерлерді жүзеге асыру мүмкіндігімен байланысты тәуекелдерді талдау. 6. Ақпараттық қауіпсіздік аудиті объектісінің қорғаныс жүйесі мен архитектурасындағы қиындықтарды анықтау.
	Білімдер: 1. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама; 2. АҚ тәуекелдері мен қатерлерін анықтаудың әдістемелері, бағдарламалық құралдары; 3. Аудиторлық куәліктерді жинау әдістері, рәсімдері және тәртібі.
Дағдыны тану мүмкіндігі:	Талап етілмейді
	Машықтар: 1. Аудит объектісінің физикалық қауіпсіздігінің жай-күйін тексеру. 2. Сәулетпен байланысты аудит объектісінің қауіпсіздік сипаттамаларын тексеру.

	Дағды 3: АЖ аудит объектісі қауіпсіздігінің ағымдағы жағдайын тексеру және талдау	3. Аудит объектісінің серверлік және желілік жабдығының АҚ кіріктірілген тетіктерінің конфигурациясына байланысты қауіпсіздік сипаттамаларын тексеру. 4. Бағдарламалық қамтамасыз етудің конфигурациясын пайдалану осалдықтарының болуына тексеру.
		Білімдер: 1. Желілік шабуылдарды болдырмау әдістері. 2. Корпоративтік желінің сыртқы периметрінің қорғалуын талдау әдістері. 3. Аудит объектісінің ішкі АТ-инфрақұрылымының қорғалуын талдау әдістері. 4. БҚ тестілеуді өткізу әдістері мен тәртібі.
Еңбек функциясы 3: Аудиторлық тапсырманың міндеттерін орындау	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 4: Аудит объектісінің бағдарламалық қамтылымының осалдықтарын анықтау	Машықтар: 1. БҚ бастапқы кодына статикалық талдау жүргізу; 2. Бастапқы кодқа динамикалық талдау жүргізу; 3. Аудит объектісінің БҚ осалдықтарын анықтау.
		Білімдер: 1. БҚ кемшіліктерін анықтаудың бағдарламалық құралдары; 2. Бағдарламалық кодты статикалық талдау әдістері; 3. Бағдарламалық кодты динамикалық талдау әдістері; 4. Қорғалу мен осалдықтарды талдаудың аспаптық құралдары; 5. Бағдарламалау тілдері (Python, Bash, PowerShell, JS, SQL).
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 5: Әртүрлі жүктеме режимдеріндегі өнімділікті бағдарламалық қамтамасыз етуді тексеру	Машықтар: 1. "Қара жәшік" және "ақ жәшік" қағидаттары бойынша БҚ тестілеу сценарийлерін құрастырады. 2. Тест ортасында және жабық ортада (sandbox) БҚ тестілеу сценарийлерін орындау. 3. Тестілеу процесінде БҚ мінез-құлқын талдау. 4. БҚ шекті жұмыс режиміне тестілеу. 5. Аудит объектісін желілік шабуылдарға (DDoS, floodies және басқалар) төзімділікке тексеру. 6. Желілік шабуыл жағдайында жүктемемен аутентификация рәсімдерін тексеру.
		Білімдер: 1. Қорғалу мен осалдықтарды талдаудың әдістері мен бағдарламалық құралдары; 2. Жүктемелік тестілеуді өткізуге арналған әдістер мен бағдарламалық құралдар; 3. Бағдарламаларды жөндеуді жүргізу үшін әдістер мен бағдарламалық құралдар;

		4. Бағдарламалау тілдері (Python, Bash, PowerShell, JS, SQL).
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 6: Аудит объектісі желісі жабдықтарының осалдықтарын анықтау	Машықтар: 1. Желі ресурстарын сәйкестендіру және түгендеу. 2. Желінің сервистері мен ақпараттық ағындарын сәйкестендіру және есепке алу. 3. Желі сегменттеріндегі желі хосттарының OS деңгейінің осалдықтарын сканерлеу. 4. Желі сегменттерінің қауіпсіздік параметрлерін сәйкестендіру және есепке алу. 5. АҚ стандарттарына сәйкестігі туралы есептерді жасау және талдау.
		Білімдер: 1. Қорғалу мен осалдықты талдаудың әдістері мен бағдарламалық құралдары 2. Желі ресурстарын түгендеу техникасы 3. АҚ есептерін қалыптастыру қағидаттары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 7: Аудиторлық тапсырманы орындау процесі мен нәтижесін құжаттау	Машықтар: 1. Құжаттау алдында дайындық жұмыстарын жүргізу; 2. Аудиторлық ұйымның жұмыс құжаттамасын қалыптастыру, жүргізу, сақтау; 3. Аудиторлық тапсырманың нәтижелері бойынша қалыптастырылған қорытынды құжатты дайындау.
		Білімдер: 1. Құжаттау алдындағы дайындық іс-шараларын өткізу тәртібі; 2. Жұмыс және есептік құжаттаманы қалыптастыру және жүргізу қағидаттары; 3. Аудит нәтижелерін жүйелеу және қорыту әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Ойлау икемділігі Командада жұмыс істей білу Тәртіптілік Бастамашылық Ұйымшылдық Зейінділік Еңбекқорлық Нәтижеге бағдарлану Жоғары оқу қабілеті	
	ҚР СТ ISO/IEC 27001-2023 "Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздікті	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	қамтамасыз етудің әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 Ақпараттық технологиялар . Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
	7	Ақпараттық қауіпсіздік жөніндегі аудитор	
17. Кәсіптің карточкасы "Деректерді шифрлаушы":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-009		
Кәсіптің атауы:	Деректерді шифрлаушы		
СБШ бойынша біліктілік деңгейі:	6		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда АТ білім беру		
Кәсіптің басқа ықтимал атаулары:	4419-9-003 - Кодтаушы		
Қызметтің негізгі мақсаты:	Деректерді шифрлау жүйелерін әзірлеу және пайдалану		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Деректерді шифрлау жүйелерін пайдалану 2. Деректерді шифрлау жүйелерінің қауіпсіздік деңгейін бағалау	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Деректерді шифрлау жүйелерінің үздіксіз жұмыс істеуін ұйымдастыруды жүзеге асыру. 2. Деректерді шифрлау жүйелерінде енгізілген желілік протоколдардың параметрлерін орнатыңыз және реттеңіз. 3. Деректерді шифрлау жүйелерін қорғау бойынша қабылданатын техникалық шаралар мен өткізілетін ұйымдастыру іс-шараларының тиімділігін арттыру және жетілдіру жөнінде ұсыныстар әзірлеу.	

Еңбек функциясы 1: Деректерді шифрлау жүйелерін пайдалану	Дағды 1: Деректерді шифрлау жүйелерінің жұмысын басқару	4. Деректерді шифрлау жүйелеріне қол жетімділігі шектеулі ақпаратты қорғау режимінің талаптарын орындау бойынша жұмыстарды ұйымдастыру 5. Деректерді шифрлау жүйелері бойынша әдістемелік материалдар мен ұйымдастырушылық-өкімдік құжаттарды әзірлеу
		Білімдер: 1. Есептеу жүйелерінің сәулеті, құрылысы және жұмыс істеуі; 2. Желілік хаттамалар және олардың параметрлері; 3. Деректерді шифрлау жүйелерінде бағдарламалық, бағдарламалық-аппараттық және техникалық құралдарды қолдану ерекшеліктері; 4. Деректерді шифрлау жүйелерін қорғауды кешенді қамтамасыз ету әдістері; 5. Деректерді шифрлау жүйелерінде қолданылатын бағдарламалық, бағдарламалық-аппараттық және техникалық құралдардың тиімділік көрсеткіштері; 6. Қолжетімділігі шектеулі ақпаратты қорғау саласындағы нормативтік құқықтық актілер; 7. Ақпаратты қорғау саласындағы ұлттық стандарттар; 8. Деректерді шифрлаудың қазіргі заманғы жүйелерінің құрылысы және жұмыс істеуі.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Пайдалану процесінде арнайы іс қағаздарын және техникалық құжаттарды жүргізу	Машықтар: 1. Деректерді шифрлау жүйелерін пайдалану процесінде қолданылатын арнайы құжаттарды алу, сақтау, есепке алу, беру, қабылдау және кәдеге жарату жөніндегі міндеттерді орындау. 2. Деректерді шифрлау жүйелерін кепілдік және кепілдіктен кейінгі жөндеуді жүзеге асыратын ұйымдармен өзара іс-қимыл жасау. 3. Деректерді шифрлау жүйелерінің пайдалану құжаттамасын жүргізу.
		Білімдер: 1. Деректерді қамтамасыз ету жүйелерінің арнайы іс қағаздарын және техникалық құжаттарын жүргізу қағидалары; 2. Мемлекеттік құпияны, құпия ақпаратты және мемлекеттік құпияны қорғау органдарының қызметін қорғауды ұйымдастыру жөніндегі нормативтік құқықтық актілер; 3. Деректерді шифрлау жүйелеріндегі ақпаратты қорғау жөніндегі ұйымдастыру шаралары; 4. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама; 5. Қазіргі заманғы деректерді шифрлау жүйелерінің құрылысы және жұмыс істеуі.

	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Деректерді шифрлау жүйелерінің қауіпсіздік деңгейін бағалау	Дағды 1: Деректерді шифрлау жүйелерінің жұмыс қабілеттілігі мен тиімділігіне бақылау тексерулерін жүргізу	Машықтар: 1. Деректерді шифрлау жүйесінің бағдарламалық-аппараттық құралдарының жұмыс істеу параметрлерін анықтау. 2. Деректерді шифрлау жүйелерінің бағдарламалық-аппараттық құралдарының тиімділігін бағалау әдістемелерін әзірлеу. 3. Деректерді шифрлау жүйелерінің бағдарламалық-аппараттық құралдарының тиімділігін бағалау. 4. Олар қамтамасыз ететін қауіпсіздік пен сенім деңгейін анықтау мақсатында деректерді шифрлау жүйелерінің бағдарламалық-аппараттық құралдарын талдау
		Білімдер: 1. Деректерді шифрлау жүйелерінің бағдарламалық-аппараттық құралдарының тиімділігін бағалау әдістері мен әдістемелері; 2. Деректерді шифрлау жүйесінің бағдарламалық-аппараттық құралдарын құру қағидаттары; 3. Ақпаратты шифрлау алгоритмдерін бағдарламалық іске асырудың дұрыстығы мен тиімділігін бағалау әдістері мен құралдары; 4. Әлеуетті осалдықтар мен құжатталмаған мүмкіндіктерді іздеу мақсатында бағдарламалық кодты талдау әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Деректерді шифрлау жүйелерінің қауіпсіздігіне талдау жүргізу	Машықтар: 1. Қауіпсіздік пен сенім деңгейін анықтау үшін деректерді шифрлау жүйелерін талдаңыз; 2. Ақпараттық қауіпсіздікті бұзушының іс-әрекетін дамытудың мүмкін жолдарын болжау; 3. Сәйкестік үшін қауіпсіздік саясатына талдау жасаңыз; 4. Деректерді шифрлау жүйелеріндегі бағдарламалық-аппараттық құралдардың тиімділігіне мониторинг, талдау және салыстыру жүргізу; 5. Жүргізілген талдау нәтижелері бойынша талдамалық есеп жасау және ресімдеу; 6. Анықталған осалдықтарды жою бойынша ұсыныстар әзірлеу.
		Білімдер: 1. Компьютерлік жүйелер мен желілердің осалдығы; 2. Ақпаратты қорғаудың криптографиялық әдістері; 3. Конфигурацияны талдау құралдары.

	Дағдыны тану мүмкіндігі:	Талап етілмейді	
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Құрылымдық ойлау Табандылық пен зейін Аналитикалық ақыл Өзін-өзі оқыту қабілеті Математикалық қабілеттер		
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 "Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 Ақпараттық технологиялар. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті ҚР СТ 1073-2007 Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
	7	Деректерді шифрлаушы	
18. Кәсіптің карточкасы "Ақпараттық қауіпсіздік аудиторы":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-002		
Кәсіптің атауы:	Ақпараттық қауіпсіздік аудиторы		
СБШ бойынша біліктілік деңгейі:	7		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	АЖ аудитін жоспарлау және бақылау		
Еңбек функциялардың сипаттамасы			
		1. АҚ аудитін жоспарлау	

Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	2. АЖ аудитін қамтамасыз ету 3. АҚ аудитін бақылау
	Қосымша еңбек функциялары:	
Еңбек функциясы 1: АҚ аудитін жоспарлау	Дағды 1: АҚ аудит бөлімінің жұмысын жоспарлау	Машықтар: 1. АҚ аудит бөлімшесінің жұмысын жоспарлау. 2. Аудит жүргізу әдістемесін талдау, таңдау (әзірлеу). 3. Жобаларды басқару.
		Білімдер: 1. Аудиторлық қызметтің әдіснамалық негіздері. 2. Аудиторлық тексерулерді ұйымдастыру әдістері. 3. Аудит жүргізу тәсілдері, әдістері және техникасы.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Аудиторлық тексеруді жоспарлау	Машықтар: 1. Аудиттің көлемін, ауқымын анықтау; 2. Аудитті орындау үшін қажетті ресурстарды анықтау; 3. Аудиторлық топтың мүшелерін іріктеуге (тағайындауға); 4. Аудиторлық тапсырмаларды бөлуге және оларды орындаудың нақты мерзімдерін белгілеуге; 5. АҚ аудит жүргізу жоспары мен бағдарламасын дайындайды және келіседі.
		Білімдер: 1. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама; 2. Аудитті жоспарлау әдіснамасы, әдістемесі және технологиясы; 3. Жобаларды басқару әдістемесі.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: АҚ аудитін әдістемелік қамтамасыз ету	Машықтар: 1. Бизнес-мақсаттар мен қауіптерге сәйкес келетін ақпараттық қауіпсіздік стратегиясын қалыптастыру; 2. Ақпаратты қорғау процесіне инновациялық технологияларды ықпалдастыру жөніндегі жоспарларды әзірлеу; 3. Қауіпсіздікке ұзақ мерзімді қауіп-қатерлерді бағалау және ден қою сценарийлерін жасау.
		Білімдер: 1. Ақпараттық қауіпсіздік жөніндегі менеджмент жүйесіне қойылатын негізгі талаптар; 2. Киберқауіпсіздік тәуекелдерін басқару және төмендету тәсілдері; 3. Ақпараттық қауіпсіздік контекстінде тәуекелдерді басқару және оларды барынша азайту қағидаттары; 4. Ақпараттандыру саласындағы заңнама.

Еңбек функциясы 2: АЖ аудитін қамтамасыз ету	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: АҚ ұйымдастырушылық қамтамасыз ету	Машықтар: 1. Тексерілетін ұйымның (бөлімшенің) өкілдерімен АҚ аудиті мәселелері бойынша өзара іс-қимылды ұйымдастырады; 2. АҚ аудиторларын оқытуды және олардың біліктілігін арттыруды ұйымдастыру; 3. Аудиторлық қызметті басқару.
		Білімдер: 1. Іскерлік коммуникацияның кезеңдері мен нысандары; 2. Іскерлік ортадағы қарым-қатынас қағидаттары мен қағидалары; 3. Жұмыс орнында персоналды оқыту және біліктілігін арттыру нысандары мен әдістері; 4. Персоналды оқыту және біліктілігін арттыру процесінің кезеңдері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: АҚ аудиті мәселелері бойынша ұйым қызметкерлеріне консультация беру және нұсқама беру	Машықтар: 1. Тексерілетін ұйымның (бөлімшенің) қызметкерлеріне АҚ аудитіне байланысты мәселелер бойынша консультация беру; 2. Аудиторлық тапсырманы орындауға байланысты шешілмеген күрделі және даулы мәселелер бойынша аудиторлық топтың қатысушыларына консультация беру; 3. Аудиторлық топқа оның мүшелерінің мақсаттары мен міндеттерін түсіндіру және түсіну мақсатында тапсырма алдында нұсқау береді.
		Білімдер: 1. Ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі ұлттық стандарт; 2. Тәуекелдерді бағалау әдіснамасы (OCTAVE); 3. Кәсіпорындағы АТ басқару және басқару моделінің сипаттамасы; 4. Тәуекелдерді бағалауды және қатерлер мониторингін жүргізуге арналған технологиялар мен құралдар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1:	Машықтар: 1. Аудиторлық тапсырма рәсімдерін орындау мерзімдерін бақылау; 2. Аудиторлық тапсырма рәсімдерінің орындалу сапасын бақылау; 3. Аудиторлардың аудиторлық қызметті регламенттейтін ұйымдастырушылық-өкімдік құжаттарды сақтауын бақылау.

Еңбек функциясы 3: АҚ аудитін бақылау	Аудиторлық тапсырманы бақылау	Білімдер: 1. Бұлтты сервистерде дербес деректерді қорғау әдістері; 2. Деректерді қорғауға арналған криптография қағидаттары мен стандарттары; 3. Киберқорғаныстың заманауи технологиялары: машиналық оқыту, жасанды интеллект, блокчейн.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Аудитордың кәсіби қасиеттерін бақылау	Машықтар: 1. АҚ аудиторларының аудиторлық тапсырмаларды орындау кезінде тәуелсіздік қағидаларын және әдеп қағидаттарын сақтауын бақылау; 2. АҚ аудиторларының кәсіби білімі мен сапасын талдау және бағалау; 3. Кәсіби дағдыларын жетілдіру үшін АҚ аудиторларымен жұмыс істеу.
		Білімдер: 1. Аудит сапасын бақылаудың ұлттық стандарттары; 2. АҚ қамтамасыз ету жөніндегі аудиттің нормативтік-құқықтық актілері; 3. АҚ бойынша аудит жүргізу жөніндегі талаптар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: Аудиторлық тапсырманың нәтижелерін бақылау	Машықтар: 1. Осалдықтарды анықтау мақсатында қауіпсіздік жүйесіне кешенді тексерулер жүргізу. 2. Жүйенің қорғалуын бағалау үшін енуді тестілеу (penetration testing) әдістерін пайдалану. 3. Ақпаратты қорғау тиімділігін үнемі қадағалау үшін мониторинг құралдарын қолдану.
		Білімдер: 1. Кіруді тестілеудің құралдары мен әдістері (мысалы, Metasploit, Nessus, Burp Suite). 2. Шабуылдарды анықтау және болдырмау технологиялары (IDS, IPS). 3. Қауіптердің нақты сценарийлері негізінде қауіпсіздік аудитін жүргізу қағидаттары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Білімді біріктіру қабілеті Жағдайды талдау Іскерлік ортадағы өзгерістерді тану және бөлімшенің және/немесе кәсіпорынның стратегиялық бағытын анықтау мүмкіндігі	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 "Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Ақпараттық қауіпсіздік	

	менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 Ақпараттық технологиялар . Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
	6	Ақпараттық қауіпсіздік жөніндегі аудитор	
19. Кәсіптің карточкасы "Ақпараттық қауіпсіздік жөніндегі маман":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-007		
Кәсіптің атауы:	Ақпараттық қауіпсіздік жөніндегі маман		
СБШ бойынша біліктілік деңгейі:	7		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:	Параграф 3. Ақпаратты қорғау жөніндегі маман Ақпаратты қорғау жөніндегі маман		
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) АТ білімі болған кезде киберқауіпсіздік саласында біліктілікті арттырудың қосымша кәсіптік курстары		
Кәсіптің басқа ықтимал атаулары:	2524-0-003 - Ақпаратты қорғау жөніндегі инженерлер 2524-0-004 - Сервистердің қауіпсіздігі жөніндегі маман 2524-0-006 - Ақпаратты қорғау жөніндегі маман 2524-0-005 - Қауіпсіздік мәселелері жөніндегі маман (АКТ)		
Қызметтің негізгі мақсаты:	Ұйым деректерінің қорғалуын қамтамасыз ету		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Ұйымның АҚ-ын басқару және қамтамасыз ету процестерін үйлестіру 2. Ұйымның АҚ-ын қамтамасыз ету жөніндегі іс-шараларды басқару	
	Қосымша еңбек функциялары:		
	Дағды 1:	Машықтар: 1. АҚ саясатын, АҚ басқару процестерін ТД және АҚ қамтамасыз ету процестерін регламенттейтін құжаттарды әзірлеу (өзектендіру) жөніндегі қызметті үйлестіру. 2. Ұйымның АҚ-ның бекітілген (өзектендірілген) саясатын жариялайды және қызметкерлердің назарына жеткізеді.	

Еңбек функциясы 1: Ұйымның АҚ-ын басқару және қамтамасыз ету процестерін үйлестіру	Ұйымның АҚ-ын басқару және қамтамасыз ету процестерін әдістемелік қамтамасыз ету	3. Ұйымның қызметкерлерімен, мердігерлермен және үшінші тараптармен құпиялылық туралы келісімдерді әзірлеуге немесе ақпаратты жария етпеуге қатысу
		Білімдер: 1. Бизнес-процестерді регламенттеудің базалық қағидаттары; 2. АҚ қамтамасыз ету саласындағы заңнама; 3. АҚ қамтамасыз ету саласындағы ұлттық стандарттар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Ұйымның АҚ басқару және қамтамасыз ету процестерін жоспарлау кезіндегі тәуекелдерді басқару	Машықтар: 1. АҚ қамтамасыз ету процестерін регламенттейтін НТҚ ағымдағы деңгейін бағалау; 2. АҚ қамтамасыз ету процестерін регламенттейтін ТҚ әзірлеу (өзектендіру); 3. Ақпараттық-коммуникациялық инфрақұрылым компоненттері мен АЖ үшін қауіпсіздік бойынша тапсырмалар мен қорғау профильдерін әзірлеу.
		Білімдер: 1. Ұйымның бағдарламалық және аппараттық құралдарының қорғау тетіктерінің принциптері; 2. АҚ қамтамасыз ету саласындағы ғылыми зерттеулер; 3. АЖ жобалау принциптері мен әдіснамасы.
	Дағдыны тану мүмкіндігі:	талап етілмейді
Еңбек функциясы 2:	Дағды 1: Ұйымның АҚ қамтамасыз ету жөніндегі іс-шаралар жоспарын	Машықтар: 1. Ақпаратты автоматтандырылған өңдеумен байланысты бизнес-процестер мен активтердің қорғалуын талдау; 2. АҚ қамтамасыз ету құралдары мен әдістерін таңдау; 3. Ұйымның АҚ саясатын іске асыруға бағытталған іс-шараларды әзірлеу; 4. Бизнестің үздіксіздігін және АҚ оқыс оқиғалары мен форс-мажорлық жағдайлардан кейін қалпына келтіруді қамтамасыз ету бойынша жоспар жасайды.
		Білімдер: 1. АҚ қамтамасыз ету құралдары мен құралдарының отандық және шетелдік нарығын дамытудың негізгі үрдістері; 2. Ақпараттың таралу арналарын анықтау және бұғаттау қағидаттары мен әдістері; 3. НТҚ және ақпаратты өңдеуге байланысты активтерді жіктеу, есепке алу және таңбалау әдістері;

Ұйымның АҚ-ын қамтамасыз ету жөніндегі іс-шараларды басқару	дайындау	4. Бизнес-процестердің үздіксіздігін қамтамасыз ету саласындағы НТҚ.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Жабдықтарды, бағдарламалық құралдарды және жүйелерді (кіші жүйелерді) сатып алуды жүзеге асыру үшін техникалық құжаттаманы дайындау	Машықтар: 1. АҚ қамтамасыз етудің сатып алынатын құралдарына техникалық ерекшеліктерді, тендерлік құжаттаманы әзірлеу. 2. АЖ АЖ ішкі жүйелеріне қойылатын талаптарды, техникалық шарттарды әзірлеу. 3. Ақпараттық-коммуникациялық инфрақұрылымның ақпараттық жүйелері мен компоненттері үшін қауіпсіздік профильдері мен қауіпсіздік тапсырмаларын әзірлеу бойынша жұмыстарды ұйымдастыру және үйлестіру.
		Білімдер: 1. Талаптарды қалыптастыру және АЖ қауіпсіздігін бағалау тәсілдері. 2. Қағидаттары мен әдіснамасы АЖ жобалау. 3. Ұйымның бағдарламалық және аппараттық құралдарының қорғаныс механизмдерін қолдану әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Ойлау икемділігі Тәртіптілік Бастамашылық Командада жұмыс істей білу	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	6	Ақпараттық қауіпсіздік жөніндегі маман
20. Кәсіптің карточкасы "Ақпараттық қауіпсіздік жөніндегі маман":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-007	
Кәсіптің атауы:	Ақпараттық қауіпсіздік жөніндегі маман	
СБШ бойынша біліктілік деңгейі:	6	
СБШ бойынша біліктілік ішкі деңгейі:		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:		

Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда АТ білім беру		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	АҚ жоспарлау, бақылау, мониторингілеу және қамтамасыз ету		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. АҚ-ны басқару және қамтамасыз ету процесін құжаттау 2. Ақпаратты өңдеуді автоматтандыру жөніндегі іс-шараларды іске асыру 3. Ұйымның АҚ-ын басқару және қамтамасыз ету процестерін бақылау 4. АҚ қамтамасыз етудің ӨАЖ пайдалану	
	Қосымша еңбек функциялары:		
Еңбек функциясы 1:	Дағды 1: Әзірлеу (өзектінормативтік-техникалық құжаттама) АҚ-ны басқару процестерін регламенттейтін құжаттаманы	Машықтар: 1. АҚ бойынша талдамалық жұмысты үйлестіру; 2. Тәуекелдерді, активтерді басқару процестерін қамтитын АҚ басқару процестерін бағалау және іске асыру әдістемелері мен әдістерін талдау, таңдау; инциденттермен, техникалық осалдықтармен, қатерлермен, техникалық қауіп-қатерлерге қарсы іс-қимылдармен, бизнестің үздіксіздігімен; 3. АҚ басқару процестерінің НТҚ келісу; 4. АҚ саясатын, АҚ басқару процестерінің НТҚ және АҚ қамтамасыз ету процестерін регламенттейтін құжаттарды әзірлеу (өзектендіру) жөніндегі қызметті үйлестіру; 5. Ұйымның АҚ-ның бекітілген (өзектендірілген) саясатын жариялау және қызметкерлердің назарына жеткізу.	
		Білімдер: 1. Бизнес-процестерді регламенттеудің базалық қағидаттары; 2. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама; 3. АҚ саласындағы ұлттық стандарттар; 4. АЖ жобалау және пайдалану қағидаттары мен әдіснамасы; 5. Бизнес-процестерді регламенттеу қағидаттары; 6. Жобаларды басқару әдістері;	

АҚ-ны басқару және қамтамасыз ету процесін құжаттау		7. АҚ тәуекелдерін бағалау және басқару әдістемелері; 8. АЖ қатерлері мен осалдықтарын талдау әдістемесі; 9. Ақпаратты өңдеуге байланысты активтерді жіктеу , есепке алу және таңбалау әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: АҚ қамтамасыз ету процестерін регламенттейтін ҒТҚ әзірлеу (өзектендіру)	Машықтар: 1. АҚ қамтамасыз ету процестерін регламенттейтін НТҚ ағымдағы деңгейін бағалау; 2. АҚ қамтамасыз ету процестерін регламенттейтін ТҚ әзірлеу (өзектендіру); 3. Ақпараттық-коммуникациялық инфрақұрылым компоненттері мен АЖ үшін қауіпсіздік бойынша тапсырмалар мен қорғау профильдерін әзірлеу.
		Білімдер: 1. Ұйымның бағдарламалық және аппараттық құралдарының қорғау тетіктерінің принциптері; 2. АҚ басқару жүйесін құру қағидаттары; 3. АЖ жобалау принциптері мен әдіснамасы.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Ақпаратты өңдеуді автоматтандыру жөніндегі іс-шараларды іске асыру	Дағды 1: Ақпаратты автоматтандырылған өңдеумен байланысты активтерді санаттарға бөлу	Машықтар: 1. Ақпаратты автоматтандырылған өңдеумен байланысты активтерге түгендеу, жіктеу, таңбалау жүргізу; 2. Активтерді санаттау нәтижелері бойынша есептік құжаттама жасауға; 3. АҚ қамтамасыз ету активтеріндегі кемшіліктерді анықтау.
		Білімдер: 1. АҚ қамтамасыз ету саласындағы заңнама; 2. АҚ қамтамасыз ету саласындағы ұлттық стандарттар; 3. Бизнестің үздіксіздігі, АҚ оқиғаларын тіркеу және есепке алу, резервтік көшіру, вирусқа қарсы қорғау, қол жеткізуді бақылау, алмалы-салмалы жеткізгіштермен, мобильді құрылғылармен жұмыс істеу, қашықтан қол жеткізу, криптографияны және олардың жеткізгіштерін пайдалану, лицензиялар және БҚ нұсқалары бойынша іс-шараларды айқындау кезінде АҚ-ны қамтамасыз етудің қағидаттары, әдістері мен құралдары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ақпаратты автоматтандырылған өңдеумен байланысты бизнес-процестер мен активтер үшін

	Дағды 2: Ақпаратты автоматтандырылған өңдеумен байланысты бизнес-процестер мен активтер үшін тәуекелдерді, қауіптерді және ағып кету арналарын анықтау	тәуекелдерді, қауіп-қатерлерді және жылыстау арналарын анықтау; 2. ТҚИ шеңберінде іс-шараларды жүзеге асыру; 3. ЕТҚ құралдарында ПЭМИН болуына зерттеу жүргізу.
		Білімдер: 1. Ақпараттың таралу арналарын анықтау әдістемесі мен құралдары; 2. НТҚ, АҚ тәуекелдері мен қауіп-қатерлерін анықтау әдістемесі; 3. КУИ бойынша ақпаратты ұстап қалу әдістері; 4. ЕТҚ қаражатын ПЭМИН болуына зерттеу әдістемесі; 5. ЕТҚ құралдарын декларацияланбаған техникалық мүмкіндіктердің болуына зерттеу жүргізу әдістемесі .
	Дағдыны тану мүмкіндігі: 	Талап етілмейді
Еңбек функциясы 3: Ұйымның АҚ-ын басқару және қамтамасыз ету процестерін бақылау	Дағды 1: СҮ талаптарының орындалуын бақылауды қамтамасыз ету АҚ басқару процестерін	Машықтар: 1. Ақпаратты автоматтандырылған өңдеумен байланысты бизнес-процестер мен активтердің қорғалуын талдау; 2. АҚ қамтамасыз ету құралдары мен әдістерін таңдау; 3. Ұйымның АҚ саясатын іске асыруға бағытталған іс-шараларды әзірлеу; 4. Бизнестің үздіксіздігін және АҚ оқыс оқиғаларынан және форс-мажорлық жағдайлардан кейін қалпына келтіруді қамтамасыз ету бойынша жоспар жасау; 5. Сатып алынатын АҚ қамтамасыз ету құралдарына техникалық ерекшеліктерді, тендерлік құжаттаманы әзірлеу; 6. АЖ АҚ кіші жүйелеріне қойылатын талаптарды, техникалық тапсырмаларды әзірлеу; 7. Ақпараттық-коммуникациялық жүйе компоненттері мен АЖ үшін қауіпсіздік бойынша тапсырмалар мен қорғау бейіндерін әзірлеу бойынша жұмыстарды ұйымдастыру және үйлестіру инфрақұрылым.
		Білімдер: 1. Бизнес-процестерді сипаттау және формализациялау әдістемесі; 2. Ақпараттың таралу арналарын анықтау және бұғаттау қағидаттары мен әдістері; 3. АҚ қамтамасыз ету саласындағы заңнама; 4. АҚ қамтамасыз ету құралдары, осалдықтар мониторингі жүйелері, АҚ мониторингі жүйелері және ақпараттың жылыстауын болдырмау жүйелері, жүйелердің қорғау тетіктері;

		5. АҚ қамтамасыз ету саласындағы ұлттық стандарттар; 6. АЖ қауіпсіздігін бағалау және талаптарды қалыптастыру тәсілдері; 7. АЖ жобалау принциптері мен әдіснамасы; 8. Ұйымның бағдарламалық және аппараттық құралдарының қорғау тетіктерін қолдану тәсілдері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: АЖ және ИКИ компоненттерінің қауіпсіздік функциялары параметрлерінің белгіленген талаптарға сәйкестігін бақылау	Машықтар: 1. АЖ әзірлеу, тестілеу және пайдалану ортасын бөлуді бақылауды жүзеге асыру; 2. Қорғалатын ақпаратты өңдеудің технологиялық процесіне ағымдағы бақылауды жүзеге асыру; 3. Ақпараттық-коммуникациялық инфрақұрылым компоненттері мен АЖ үшін қауіпсіздік бойынша тапсырмалар мен қорғау бейіндерінің іске асырылуын бақылауды жүзеге асырады.
		Білімдер: 1. АҚ құралдары мен әдістерін әзірлеу, тестілеу және байқаудан өткізу бойынша жұмыстарды орындаудың базалық қағидаттары мен тәсілдері; 2. Бағдарламалық құралдарды, қорғау тетіктерін, АЖ және ИКИ компоненттерін пайдалану қағидалары; 3. Баптаулардағы бұзушылықтарды анықтау әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 4:	Дағды 1: АҚ қамтамасыз етудің ӨАЖ және мониторинг жүйелерін пайдалану	Машықтар: 1. АҚ-ны қамтамасыз ету жөніндегі іс-шаралар жоспарының іске асырылуын бақылауды жүзеге асыру; 2. Ұйымдағы АҚ және АҚ басқару процестерінің НТҚ қамтамасыз ету процестерін регламенттейтін құжаттар талаптарының орындалуын тексеру нәтижелерін талдау; 3. Ұйым қызметкерлерімен мердігерлер мен үшінші тараптар құпиялылық туралы келісімдерді әзірлеуге немесе ақпаратты жария етпеуге қатысу .
		Білімдер: 1. СЖ-да және оларға кіріктірілген қорғау тетіктерінде әкімшілік ету қағидаттары мен құралдары; 2. АҚ қамтамасыз ету АЖЖ жұмыс істеу қағидаттары; 3. Жасақтау және қолдану қағидаттары, осалдықтар мониторингі жүйелері, АҚ мониторингі жүйелері; 4. Ақпараттың жылыстауын болдырмау жүйелері;

АҚ қамтамасыз етудің ӨАЖ пайдалану		5. АҚ инциденттерін, сыни (авариялық) жағдайларды анықтау, алдын алу және салдарын жою әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: ҚББЖ және жүйелердің жұмыс істеуін әкімшілендіру және мониторингілеу бейнебақылау	Машықтар: 1. Әкімшілендіру ҚББЖ және бейнебақылау жүйелері 2. Жұмыс істеуіне мониторинг жүргізу ҚББЖ және бейнебақылау жүйелері 3. Қабылданған шешімдердің АҚ-ның ең жоғары деңгейіне сәйкестігі туралы қорытындылар жасау
		Білімдер: 1. Тағайындалуы, техникалық сипаттамалары, ҚББЖ конструкциясы, ерекшеліктері 2. ҚББЖ және бейнебақылау жүйелерін пайдалану ережелері. 3. Бейнебақылау жүйелерінің мақсаты, техникалық сипаттамалары, құрылымы, ерекшеліктеріқоныстар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Командада жұмыс істей білу Тәртіптілік Бастамашылық Ұйымдастыру қабілеті Мұқияттылық Атқарушылық Талдап ойлау Жоспарлау Шешім қабылдау Нәтижеге бағдарлану Кәсіби деңгейін көтеруге ұмтылу	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	7	Ақпараттық қауіпсіздік жөніндегі маман
21. Кәсіптің карточкасы "Ақпаратты қорғау жөніндегі инженер":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-003	
Кәсіптің атауы:	Ақпаратты қорғау жөніндегі инженер	
СБШ бойынша біліктілік деңгейі:	6	

СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:	Параграф 2. Ақпаратты қорғау жөніндегі инженер Ақпаратты қорғау жөніндегі инженер		
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда АТ білім беру		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Ақпаратты қорғау құралдарымен қолданбалы және жүйелік бағдарламалық қамтамасыз етудің өнімділігін қамтамасыз ету		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Қолданбалы және жүйелік бағдарламалық қамтамасыз етудің ақпаратты қорғау құралдарына қызмет көрсету 2. Операциялық залдарда ақпаратты қорғаудың бағдарламалық-аппараттық құралдарына қызмет көрсету	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Ақпаратты қорғаудың арнайы техникалық және бағдарламалық-математикалық құралдарын жобалау және енгізу, ақпараттық жүйелерді қорғаудың ұйымдастырушылық және техникалық шараларын қамтамасыз ету жөніндегі жұмысты орындау; 2. Неғұрлым орынды практикалық шешімдерді таңдау үшін зерттеулер жүргізу; 3. Ақпаратты қорғаудың техникалық құралдары мен тәсілдері бойынша ғылыми-техникалық әдебиетті, нормативтік және әдістемелік материалдарды іріктеуді, зерделеуді және қорытуды жүзеге асыру; 4. Ақпаратты техникалық қорғау жөніндегі жұмыстарды жүргізудің техникалық тапсырмаларының, жоспарлары мен кестелерінің жобаларын қарауға, қажетті техникалық құжаттаманы әзірлеуге қатысу; 5. Ақпаратты техникалық қорғау бойынша есептеу әдістемелері мен эксперименттік зерттеулер бағдарламаларын жасайды, әзірленген әдістемелер мен бағдарламаларға сәйкес есептеулерді орындау;	

Еңбек функциясы 1: Қолданбалы және жүйелік бағдарламалық қамтамасыз етудің ақпаратты қорғау құралдарына қызмет көрсету	Дағды 1: Нормативтік реттеу, қатерлер, ақпаратты қорғаудың әдістері мен құралдары	6. Зерттеулер мен сынақтардың деректеріне салыстырмалы талдау жүргізеді, ақпараттың жылыстау көздері мен арналарын зерделеу; 7. Ақпаратты қорғау жүйесін техникалық қамтамасыз етуді әзірлеуді, ақпаратты қорғау құралдарына техникалық қызмет көрсетуді жүзеге асыру, 8. Ақпаратты қорғауды жетілдіру және тиімділігін арттыру бойынша ұсынымдар мен ұсыныстар жасауға, ғылыми-техникалық есептердің бөлімдерін жазуға және ресімдеуге қатысу; 9. Ақпаратты техникалық қорғау бойынша ақпараттық шолулар жасау; 10. Ақпаратты қорғау жүйесінің техникалық құралдары мен тетіктерін бақылауды қамтамасыз етуге байланысты жедел тапсырмаларды орындау, ақпаратты қорғау жөніндегі нормативтік-техникалық құжаттаманың талаптарын орындау бойынша ұйымдарға тексеру жүргізуге, нормативтік-әдістемелік материалдар мен техникалық құжаттамаға пікірлер мен қорытындылар дайындауға қатысу; 11. Ақпаратты қорғаудың техникалық құралдары саласында қызмет көрсететін өзге де ұйымдармен келісімдер мен шарттар жасасу жөнінде ұсыныстар дайындайды, қажетті материалдарға, жабдықтарға, аспаптарға өтінімдер жасау; 12. Объектілерді, үй-жайларды, техникалық құралдарды, бағдарламаларды, алгоритмдерді тиісті қауіпсіздік сыныптары бойынша ақпаратты қорғау талаптарына сәйкестігі тұрғысынан аттестаттау жүргізуге қатысу; 13. Ақпаратты қорғаудың қолданыстағы жүйелері мен техникалық құралдарының жұмыс қабілеттілігі мен тиімділігіне бақылау тексерулерін жүргізу, бақылау тексерулерінің актілерін жасау және ресімдеу, тексеру нәтижелерін талдау және қабылданатын шараларды жетілдіру және тиімділігін арттыру бойынша ұсыныстар әзірлеу; 14. Ақпаратты қорғаудың техникалық құралдары мен тәсілдерін пайдалану бойынша өзге де ұйымдардың жұмыс тәжірибесін зерделеу және қорытады; 15. Жұмыстарды жүргізу режимі жөніндегі нұсқаулықтардың талаптарын сақтай отырып, белгіленген мерзімде жоғары ғылыми-техникалық деңгейде жұмыстарды орындау.
		Білімдер: 1. Ақпараттандыру саласындағы заңнама; 2. Ұйымның мамандануы және оның қызметінің ерекшеліктері; 3. Ақпаратты алу, өңдеу және беру әдістері мен құралдары;

		4. Ақпаратты қорғаудың техникалық құралдары, ақпаратты қорғаудың бағдарламалық-математикалық құралдары; 5. Ақпараттың ықтимал жылыстау арналары; 6. Ақпаратты талдау және қорғау әдістері; 7. Ақпаратты қорғау жөніндегі жұмыстарды ұйымдастыру; 8. Арнайы жұмыстарды жүргізу режимін сақтау жөніндегі нұсқаулықтар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Бағдарламалық қамтамасыз етуді сақтай отырып баптау ақпаратты қорғау жөніндегі талаптарды	Машықтар: 1. Деректер базасын басқару жүйелерін және электрондық құжат айналымы құралдарын қоса алғанда, бағдарламалық қамтамасыз ету жұмысының параметрлерін баптауды орындау; 2. Ақпаратты қорғау бойынша қолданыстағы талаптарды сақтай отырып, бағдарламалық қамтамасыз етумен жұмыс істеу; 3. Деректерді сақтауды теңшеу.
		Білімдер: 1. Бағдарламалық қамтамасыз етуді, деректер базасын басқару жүйелерін және электрондық құжат айналымы құралдарын баптау тәртібі; 2. Ақпаратты қорғау әдістері, құралдары және жүйелері; 3. Ақпаратты қорғау құралдарын пайдалану кезінде ақпаратты қорғауға қойылатын талаптар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2:	Дағды 1: Вирусқа қарсы қорғаныс құралдарын дұрыс күйге келтіру бағдарламалық қамтамасыз етудің жұмыстары бойынша берілген үлгілерге	Машықтар: 1. Қол жетімділігі шектеулі ақпаратты өңдеудің техникалық құралдарына арнайы зерттеулер мен арнайы тексерулер жүргізуді ұйымдастыруға; 2. Ұйымның ақпаратты қорғау жүйесінің құрамына кіретін ақпаратты қорғаудың техникалық, бағдарламалық (бағдарламалық-техникалық) құралдарын орнату және баптау; 3. Ұйымдастырушылық-өкімдік құжаттарды әзірлейді.
		Білімдер: 1. АҚ қамтамасыз ету саласындағы нормативтік-құқықтық актілер; 2. Ақпаратты қорғау әдістері, құралдары және жүйелері; 3. Ақпаратты қорғаудың техникалық құралдарының архитектурасы; 4. АҚ қамтамасыз ету саласындағы ұлттық стандарттар.

Операциялық залдарда ақпаратты қорғаудың бағдарламалық-аппараттық құралдарына қызмет көрсету	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Берілген үлгілер бойынша бағдарламалық қамтылым ақпаратын қорғаудың кіріктірілген құралдарын баптау	Машықтар: 1. Кіріктірілген бағдарламалық қамтамасыз ету ақпаратын қорғау құралдарының ағымдағы баптауларын бағалау; 2. Дерекқорды басқару жүйелерін және электрондық құжат айналымы құралдарын қоса алғанда, бағдарламалық қамтамасыз ету жұмысының параметрлерін теңшеуді орындау; 3. Ақпаратты қорғау бойынша қолданыстағы талаптарды сақтай отырып, бағдарламалық қамтамасыз етумен жұмыс істеу.
		Білімдер: 1. Бағдарламалық қамтамасыз етуді, деректер базасын басқару жүйелерін және электрондық құжат айналымы құралдарын баптау тәртібі; 2. Бағдарламалық қамтамасыз етуді пайдалану кезінде ақпараттың қауіпсіздігін қамтамасыз ету тәртібі; 3. Бағдарламалау тілдері (Python, Bash, PowerShell, JS, SQL).
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Ойлау икемділігі Командада жұмыс істей білу Тәртіптілік Бастамашылық Ұйымшылдық Зейінділік Еңбекқорлық Нәтижеге бағдарлану Жоғары оқу қабілеті	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	7	Ақпаратты қорғау жөніндегі инженер
22. Кәсіптің карточкасы "Ақпаратты қорғау жөніндегі инженер":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-003	
Кәсіптің атауы:	Ақпаратты қорғау жөніндегі инженер	
СБШ бойынша біліктілік деңгейі:	7	

СБШ бойынша біліктілік ішкі деңгейі:			
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:	2524-0-006 - Ақпаратты қорғау жөніндегі маман		
Қызметтің негізгі мақсаты:	Жұмыспен қамтуды қамтамасыз етуді қамтамасыз етуқолданбалы және жүйелік ақпарат ақпаратты қорғау құралдарымен бағдарламалық қамтамасыз ету		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Ұйымда ақпаратты қорғау жүйесін құру 2. Ұйымда ақпаратты қорғау жүйесін пайдалануға беру 3. Ақпаратты қорғау жүйесін пайдалану барысында оны сүйемелдеу	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Арнайы техникалық және технологиялық жабдықтарды жобалау және енгізу бойынша жұмыстарды орындайды. ақпаратты қорғаудың бағдарламалық-математикалық құралдары, ақпараттық жүйелерді қорғаудың ұйымдастырушылық және техникалық шараларын қамтамасыз ету; 2. Қойылған міндеттер шегінде неғұрлым мақсатқа сай практикалық шешімдерді табу және таңдау мақсатында зерттеулер жүргізу; 3. Ақпаратты қорғаудың техникалық құралдары мен тәсілдері бойынша ғылыми-техникалық әдебиеттерді, нормативтік және әдістемелік материалдарды іріктеуді, зерделеуді және қорытуды жүзеге асыру; 4. Ақпаратты техникалық қорғау бойынша жұмыстарды жүргізудің техникалық тапсырмаларының жобаларын, жоспарлары мен кестелерін қарауға, қажетті техникалық құжаттаманы әзірлеуге қатысу;	

	Дағды 1: Нормативтік реттеу, қатерлер, ақпаратты қорғаудың әдістері мен құралдары	5. Ақпаратты техникалық қорғау бойынша есептеу әдістемелерін және эксперименттік зерттеулер бағдарламаларын құрастырады, әзірленген әдістемелер мен бағдарламаларға сәйкес есептеулерді орындау; 6. Зерттеулер мен сынақтардың деректеріне салыстырмалы талдау жүргізеді, ақпараттың таралып кетуінің ықтимал көздері мен арналарын зерделеу; 7. Ақпаратты қорғау жүйесін техникалық қамтамасыз етуді әзірлеуді, ақпаратты қорғау құралдарына техникалық қызмет көрсетуді жүзеге асырады, ақпаратты қорғауды жетілдіру және тиімділігін арттыру бойынша ұсынымдар мен ұсыныстарды әзірлеуге, ғылыми-техникалық есептердің бөлімдерін жазуға және ресімдеуге қатысу; 8. Ақпаратты техникалық қорғау бойынша ақпараттық шолуларды құрастыру; 9. Ақпаратты қорғау жүйесінің техникалық құралдары мен механизмдерін бақылауды қамтамасыз етуге байланысты жедел тапсырмаларды орындау, ақпаратты қорғауға арналған нормативтік-техникалық құжаттаманың талаптарын орындау бойынша ұйымдарға тексерулер жүргізуге, нормативтік-әдістемелік материалдар мен техникалық құжаттамаға шолулар мен қорытындылар дайындауға қатысу; 10. Ақпаратты қорғаудың техникалық құралдары саласында қызметтер көрсететін өзге де ұйымдармен келісімдер мен шарттар жасасу жөнінде ұсыныстар дайындау, қажетті материалдарға, жабдықтарға, аспаптарға өтінімдер жасау; 11. Объектілерді, үй-жайларды, техникалық құралдарды, бағдарламаларды, алгоритмдерді сәйкестік мәніне аттестаттауды, қауіпсіздіктің тиісті сыныптары бойынша ақпаратты қорғау талаптарына жүргізуге қатысу; 12. Ақпаратты қорғаудың қолданыстағы жүйелері мен техникалық құралдарының жұмыс қабілеттілігі мен тиімділігіне бақылау тексерулерін жүргізу, бақылау тексерулерінің актілерін жасау және ресімдеу, тексерулердің нәтижелерін талдау және қабылданған шараларды жетілдіру және тиімділігін арттыру бойынша ұсыныстар әзірлеу; 13. Өзге ұйымдардың ақпаратты қорғаудың техникалық құралдары мен тәсілдерін пайдалану жөніндегі жұмыс тәжірибесін зерделеу және қорытындылу, оны құпиялылық режимінде қорғау және сақтау бойынша жұмыстардың тиімділігін арттыру және жетілдіру; 14. Жұмыстарды белгіленген мерзімде жоғары ғылыми-техникалық деңгейде, жұмыстарды жүргізу

Еңбек функциясы 1: Ұйымда ақпаратты қорғау жүйесін құру		тәртібі жөніндегі нұсқаулықтардың талаптарын сақтай отырып орындау.
		Білімдер: 1. Ақпаратты техникалық қорғауды қамтамасыз етуге байланысты заңнамалық, өзге де нормативтік құқықтық актілер мен әдістемелік материалдар; 2. Ұйымның мамандануы және оның қызметінің ерекшеліктері; 3. Алу, өңдеу және өңдеу әдістері мен құралдары. ақпаратты беру; 4. ақпаратты қорғауды техникалық қамтамасыз ету жөніндегі ғылыми-техникалық және өзге де арнайы әдебиеттерді; 5. Ақпаратты қорғаудың техникалық құралдары, ақпаратты қорғаудың бағдарламалық-математикалық құралдары; 6. Ақпаратты қорғау жөніндегі техникалық құжаттаманы ресімдеу тәртібі; 7. Ақпараттың ықтимал таралу арналары; 8. Ақпаратты талдау және қорғау әдістері; 9. Ақпаратты қорғау бойынша жұмыстарды ұйымдастыру; 10. Арнайы жұмыстарды жүргізу режимін сақтау жөніндегі нұсқаулықтар; 11. Техникалық барлау және ақпаратты қорғау саласындағы отандық және шетелдік тәжірибе; 12. Еңбек заңнамасы, ішкі еңбек тәртібінің тәртібі, еңбек қауіпсіздігі және еңбекті қорғау, өндірістік санитария, өрт қауіпсіздігі талаптары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Мақсаты, функциялары, жұмыс істеу шарттары туралы деректерді талдау және өңдеудің техникалық құралдарының қолжетімділігі шектеулі ақпарат	Машықтар: 1. АҚ қамтамасыз ету құралдарының ағымдағы жай-күйін бағалау; 2. Персоналдың өңдеуге (талқылауға, беруге) қатысу дәрежесін анықтау, ақпаратты сақтау); 3. Негізгі техникалық құралдар мен жүйелердің мақсаты, функциялары, жұмыс істеу шарттары туралы деректерді талдау.
		Білімдер: 1. АҚ техникалық құралдарының негізгі параметрлері; 2. Ақпаратты қорғау жүйесіне арналған пайдалану құжаттамасы; 3. Ақпаратты градациялау (санаттау) типтері, санаттары, түрлері мен деңгейлері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ұйымдағы ақпараттық қауіпсіздікке төнетін қатерлердің модельдерін әзірлеу;

	Дағды 3: Ұйымдағы ақпараттық қауіпсіздікке төнетін қатерлер моделін әзірлеу	2. Қатерлер моделін әзірлеудің бағдарламалық құралдарын пайдалану; 3. Ұйымда ақпаратты қорғау жүйесін құру қажеттілігінің аналитикалық негіздемесін әзірлеу; 4. Техникалық тапсырмаға сәйкес объектінің ақпараттық қауіпсіздігін басқарудың жүйелері мен ішкі жүйелерінің жобаларын әзірлеу.
		Білімдер: 1. Қолжетімділігі шектеулі ақпаратты қорғау саласындағы нормативтік-құқықтық актілер, әдістемелік құжаттар, ұлттық стандарттар; 2. Ақпаратты қорғаудың тиімділігін бақылау әдістері мен әдістері; 3. Ақпаратты қорғау жөніндегі ұйымдастырушылық-өкімдік құжаттама.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 4: Ақпаратты қорғау жүйесін құруға арналған техникалық шарттарды әзірлеу	Машықтар: 1. Ақпараттандыру объектісіне және ақпаратты қорғау құралдарына пайдалану құжаттамасын әзірлеу; 2. Жүйенің техникалық тапсырмасын әзірлеу; 3. Ақпаратты қорғау жүйесіне конструкторлық-технологиялық құжаттаманы әзірлеу.
		Білімдер: 1. Бағдарламалық (бағдарламалық-техникалық) қорғау құралдары; 2. Қазіргі заманғы ақпараттық технологиялар (операциялық жүйелер, мәліметтер базасы, компьютерлік желілер); 3. ЕСКД, ЕСТД және ЕСПД стандарттары; 4. Ақпаратты қорғаудың әдістері, құралдары және жүйелері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: Ақпаратты қорғау жүйесінің тиімділігін қамтамасыз ететін ұйымдастырушылық шараларды әзірлеу және енгізу	Машықтар: 1. Қолжетімділігі шектеулі ақпаратты өңдеудің техникалық құралдарына арнайы зерттеулер мен арнайы тексерулер жүргізуді ұйымдастыру; 2. Ұйымның ақпаратты қорғау жүйесінің құрамына кіретін ақпаратты қорғаудың техникалық, бағдарламалық (бағдарламалық-техникалық) құралдарын орнату және күйге келтіру; 3. Ұйымдастырушылық-өкімдік құжаттарды әзірлеу.
		Білімдер: 1. Ақпаратты қорғау саласындағы нормативтік-құқықтық актілер, әдістемелік құжаттар, ұлттық стандарттар; 2. Ақпаратты қорғаудың әдістері, құралдары және жүйелері;

		3. Ақпаратты қорғаудың техникалық құралдарының архитектурасы.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Ұйымдастырунұсқама жүргізуді ерсациялау басшылық құрамның және персоналды мәселелер бойынша оқытудың ақпаратты техникалық қорғау	Машықтар: 1. Персоналды ақпаратты қорғаудың техникалық, бағдарламалық (бағдарламалық-техникалық) құралдарын пайдалануға оқытуды ұйымдастыру; 2. Ақпаратты техникалық қорғау мәселелері бойынша нұсқама жүргізу; 3. Қызметкерлермен сабақтар өткізу;
		Білімдер: 1. Ұйымдастырушылық-өкімдік құжаттар; 2. Персоналға нұсқау беру әдістемесі; 3. Оқу сабақтарын өткізу қағидалары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Ұйымда ақпаратты қорғау жүйесін пайдалануға беру	Дағды 3: Жүйенің тәжірибелік пайдаланылуын және жетілдірілуін ұйымдастыру ақпаратты қорғау	Машықтар: 1. Алдын ала сынақтардың бағдарламалары мен әдістемелерін әзірлеу; 2. Ақпаратты қорғау жүйесін тәжірибелік пайдалануды және жетілдіруді ұйымдастыру; 3. Ақпаратты қорғау жүйесін алдын ала сынау бағдарламалары мен әдістемелерін әзірлеу.
		Білімдер: 1. Ақпаратты қорғау саласындағы нормативтік-құқықтық актілер, әдістемелік құжаттар, ұлттық стандарттар; 2. ЕСКД, ЕСТД және ЕСПД стандарттары; 3. Ақпаратты қорғаудың әдістері, құралдары және жүйелері; 4. 4. Бағдарламалау тілдері (Python, Bash, PowerShell, JS, SQL).
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 4: Ақпаратты қорғау жүйесін пайдалануға енгізу	Машықтар: 1. Алдын ала сынақтардың бағдарламалары мен әдістемелерін әзірлеу; 2. Ақпаратты қорғау жүйесінің қабылдау сынақтарын ұйымдастыру; 3. Ақпаратты қорғау жүйесін пайдалануға беруді ұйымдастыру.
		Білімдер: 1. Ақпаратты қорғау саласындағы нормативтік-құқықтық актілер, әдістемелік құжаттар, ұлттық стандарттар; 2. ЕСКД, ЕСТД және ЕСПД стандарттары; 3. Заманауи ақпараттық технологиялар; 4. Ақпараттың типтері, санаттары, түрлері және градация (санаттау) деңгейлері.

	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 3: Ақпаратты қорғау жүйесін пайдалану барысында оны сүйемелдеу	Дағды 1: Ұйымдастырушылық және техникалық іс-шараларды жетілдіру жөнінде ұсыныстар әзірлеу	Машықтар: 1. Ақпаратты қорғау жүйесінің жай-күйіне бақылау (мониторинг) жүргізу; 2. Ақпаратты қорғау жүйесінің жай-күйін бақылау; 3. Ақпаратты техникалық қорғау бойынша ұйымдастыру және техникалық іс-шараларды жетілдіру бойынша ұсыныстар әзірлеуді басқару; 4. Ұйымдағы ақпаратты техникалық қорғау жүйесінің тиімділігін бағалау және жетілдіру.
		Білімдер: 1. Қазіргі заманғы ақпараттық технологиялар; 2. Ақпаратты қорғау саласындағы нормативтік-құқықтық актілер, әдістемелік құжаттар, ұлттық стандарттар; 3. Қорғау әдістері, құралдары мен жүйелері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Іс-шараларды ұйымдастыру бойынша ақпараттандыру жүйелеріне техникалық қызмет көрсету және оларды пайдаланудан шығару және олардың элементтерін кәдеге жарату бойынша	Машықтар: 1. Бойынша жұмыстарды ұйымдастыру ақпаратты қорғаудың техникалық және бағдарламалық-техникалық құралдарына техникалық қызмет көрсету; 2. Пайдаланудан шығару бойынша жұмыстарды жүргізуді ұйымдастырады және олардың орындалуына басшылық жасау; 3. Пайдаланудан шығарылған БҚ мен техникалық құралдарды кәдеге жарату.
		Білімдер: 1. Нормативтік-құқықтық актілер, әдістемелік құжаттар, ақпаратты қорғау саласындағы ұлттық стандарттар; 2. Баспа ақпаратын кепілді жою әдістері; 3. Әртүрлі машиналық ақпарат тасымалдағыштарын кепілді жою әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Ойлау икемділігі Тәртіптілік Бастамашылық Командада жұмыс істей білу	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
	СБШ-нің деңгейі:	Кәсіптің атауы:

СБШ -нің ішіндегі басқа кәсіптермен байланыс:	6	Ақпаратты қорғау жөніндегі инженер	
23. Кәсіптің карточкасы "Сервистердің қауіпсіздігі жөніндегі маман":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-004		
Кәсіптің атауы:	Сервистердің қауіпсіздігі жөніндегі маман		
СБШ бойынша біліктілік деңгейі:	7		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:	2524-0-005 - Қауіпсіздік мәселелері жөніндегі маман (АКТ) 2524-0-006 - Ақпаратты қорғау жөніндегі маман		
Қызметтің негізгі мақсаты:	Рұқсатсыз кіру үшін жүйенің осал тұстарын іздеу және анықтау		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Анықталған осалдықтарды жою үшін сервистерді әзірлеушілермен және менеджерлермен өзара іс-қимыл жасау 2. Ақпараттық қауіпсіздікке байланысты жаңа функционалдылықтың кеңесшісі және тапсырыс берушісі ретінде әрекет ету	
	Қосымша еңбек функциялары:		
	Дағды 1: Сервистердің анықталған осалдықтары туралы	Машықтар: 1. Осалдықтарды сканерлеу құралдарын пайдалану; 2. Шабуылдарды анықтау үшін логтар мен желілік трафикті талдау; 3. Деректер базасындағы және мамандандырылған ресурстардағы осалдықтар туралы ақпаратты іздеу; 4. Осалдықтардың сыншылығын анықтау және олардың жүйенің қауіпсіздігіне әсерін бағалау; 5. Осалдықтарды жою бойынша есептер мен ұсынымдар дайындау.	
		Білімдер:	

	ақпаратты жинау және талдау	1. Шабуылдардың негізгі түрлерін түсіну; 2. Осалдықтарды бағалау әдіснамасы; 3. Оқиғаларды логикалау және талдау - SIEM-жүйелермен жұмыс істеу; 4. Сервистердің хаттамалары мен архитектурасы; 5. Бағдарламалау тілдері (Python, Bash, PowerShell, JS, SQL); 6. Қауқарсыздықтың жария базаларымен жұмыс.
Еңбек функциясы 1: Анықталған осалдықтарды жою үшін сервистерді әзірлеушілермен және менеджерлермен өзара іс-қимыл жасау	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Қою және қабылдау сервистердің анықталған осалдықтарын жою жөніндегі міндеттер	Машықтар: 1. Әзірлеушілер мен әкімшілерге осалдықтарды жою бойынша нақты міндеттерді тұжырымдау; 2. Түзетулерді қайта тестілеу жолымен тексеруге; 3. Осалдықтарды жою процестерін көмегімен автоматтандыру; 4. Осалдықтар бойынша құжаттаманы жүргізу, олардың табиғаты мен жою тәсілдерін сипаттау; 5. Қауіпсіздік талаптарын түсіндіре отырып, әзірлеушілер мен жүйелік әкімшілер командаларымен жұмыс істеу.
		Білімдер: 1. БҚ әзірлеудің өмірлік циклі және қауіпсіз әзірлеу; 2. Осалдықтарды түзету әдістері - бағдарламалық жасақтаманы жаңарту, патчинг, конфигурацияны өзгерту, WAF баптау; 3. Нұсқаларды бақылау және осалдықтарды басқару - Git, Jira, ServiceNow, Tenable; 4. Қауіпсіздікке тестілеу әдістері; 5. Бағдарламалау тілдері (Python, Bash, PowerShell, JS, SQL); 6. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: Бұқаралық ақпарат құралдарында және басқа да ашық қолжетімді сервистер туралы	Машықтар: 1. Құпия ақпараттың және жасырын қауіптердің болуы мәніне жарияланымдарды талдау; 2. Жариялау алдында ақпаратты ашуға қабілетті метадеректердің болуын тексеру; 3. Қауіптерді барынша азайтып, қауіпсіздік қағидаттарын ескере отырып, хабарламаларды сауатты тұжырымдау; 4. Ақпаратты беру кезінде қорғалған байланыс арналарын пайдалану (шифрлау, цифрлық қолтаңбалар); 5. Ақпараттық қауіпсіздікке төнген қатерлер тұрғысынан жарияланымның ықтимал салдарын бағалау; 6. Сервиске бағытталған дезинформациялық шабуылдарды анықтау және болдырмау.

Еңбек функциясы 2: Ақпараттық қауіпсіздікке байланысты жаңа функционалдылықтың кеңесшісі және тапсырыс берушісі ретінде әрекет ету	жарияланымдар мен хабарламаларды дереккөздерде дайындау және орналастыру	Білімдер: 1. Ақпараттық қауіпсіздік негіздері - ақпаратты жариялауға байланысты тәуекелдерді, оның ішінде деректердің жылыстауы мен киберқұралдарды түсіну; 2. Қаскүнемдердің ақпарат жинау үшін ашық көздерді қалай пайдалана алатынын білу; 3. Жарияланымдарда қандай деректер қалуы мүмкін екенін түсіну (құпия файл метадеректері, геолокация, құрылғы туралы ақпарат); 4. Ақпаратты қорғау саласындағы заңнама - деректерді өңдеу және тарату қағидалары; 5. Әлеуметтік инженерия - шабуыл жасаушылар жарияланған мәліметтерді шабуыл жасау үшін пайдалана алатын әдістерді білу.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Организация и проведение аудита	Машықтар: 1. Деректерді компрометациялау мүмкіндігін болдырмай, қауіпсіздік талаптарын ескере отырып, көрсету стендтерін дайындау; 2. Жауынгерлік жүйелердің жұмысын бұзбай, бақыланатын жағдайларда шабуыл және қорғаныс сценарийлерін көрсету; 3. Нақты уақытта қауіпсіздік мониторингі құралдарымен жұмыс істеу; 4. Нақты уақыт режимінде осалдықтарды анықтай отырып, көрсету сервистерінде қауіпсіздікті тестілеуді жүргізу; 5. Ең аз артықшылықтар қағидатын ескере отырып, көрсету ортасына қол жеткізуді теңшеу; 6. Қауіпсіздіктің техникалық аспектілерін әртүрлі аудиториялар (әзірлеушілер, менеджерлер, клиенттер) үшін түсінікті тілмен түсіндіру.
		Білімдер: 1. Сервистердің қауіпсіздігін тестілеу әдістері; 2. Сервистерге қауіп-қатерлер мен шабуылдар; 3. Көрсету үшін қауіпсіз орта; 4. Онлайн-демонстрацияларды өткізу кезіндегі қорғау әдістері - қауіпсіз қосылыстар, деректерді ұстаудан қорғау әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Ойлау икемділігі Тәртіптілік Бастамашылық Жауапкершілік Командада жұмыс істей білу	
	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
	6	Сервистердің қауіпсіздігі жөніндегі маман	
24. Кәсіптің карточкасы "Деректерді шифрлаушы":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-009		
Кәсіптің атауы:	Деректерді шифрлаушы		
СБШ бойынша біліктілік деңгейі:	7		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда АТ білім беру		
Кәсіптің басқа ықтимал атаулары:	4419-9-003 - Кодтаушы		
Қызметтің негізгі мақсаты:	Деректерді шифрлау жүйелерін әзірлеу және пайдалану		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Деректерді шифрлаудың бағдарламалық, бағдарламалық-аппараттық жүйелерін әзірлеу 2. Ақпараттық қауіпсіздік регламенттері мен талаптарына сәйкес деректерді шифрлау және ашып көрсету	
	Қосымша еңбек функциялары:		
		Машықтар: 1.Деректерді шифрлау жүйелерінің жұмыс істеуі саласында қолданыстағы нормативтік базаны қолдану 2.Техникалық барлауға қарсы іс-қимыл жөніндегі нормативтік құжаттарды қолдану 3.Қорғалатын ақпаратты құпия түрлері мен құпиялылық дәрежелері бойынша жіктеу	

	Дағды 1: Деректерді шифрлау жүйелеріне арналған жобалық шешімдерді әзірлеу	4.Қорғау объектілері болып табылатын қол жеткізу субъектілері мен қол жеткізу объектілерінің түрлерін айқындау 5.Қол жеткізуді басқару әдістерін, қол жеткізу түрлерін және деректерді шифрлау жүйелерінде іске асырылатын қол жеткізу объектілеріне қол жеткізуді шектеу ережелерін анықтау 6.Деректерді шифрлау саласындағы нормативтік құқықтық құжаттардың талаптарына сәйкес деректерді шифрлау жүйелерінің құрылымын анықтау
		Білімдер: 1. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама; 2. Деректерді шифрлаудың қазіргі заманғы жүйелерін құру және жұмыс істеу қағидаттары, іске асыру мысалдары; 3. Деректерді шифрлау құралдарының тиімділігі мен сенімділігін бағалау критерийлері; 4. Деректерді шифрлау жүйелерін ұйымдастыру қағидаттары мен құрылымы; 5. Деректерді шифрлаудың техникалық құралдарының негізгі сипаттамалары; 6. Деректерді шифрлаудың қазіргі заманғы жүйелерінің жұмыс істеуі; 7. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 1: Деректерді шифрлаудың бағдарламалық, бағдарламалық-аппараттық жүйелерін әзірлеу	Дағды 2: Деректерді шифрлаудың бағдарламалық,	Машықтар: 1. Криптографиялық алгоритмдер мен есептеулердің күрделілігін бағалау 2. Нормативтік құжаттардың, ЭСҚД және ЭСҚД талаптарын ескере отырып, деректерді шифрлау жүйелерін құруға арналған техникалық шарттарды әзірлеу 3. Деректерді шифрлау жүйелеріндегі қауіпсіздіктің ықтимал осалдықтарын анықтау мақсатында деректерді шифрлау жүйелерінің компоненттерінің бағдарламалық, архитектуралық, техникалық және схемалық шешімдерін талдау 4. Аппараттық және бағдарламалық қамтамасыз етуді кешенді тестілеуді жүргізу бағдарламалық құралдардың
		Білімдер: 1.Ақпарат қауіпсіздігі және деректерді шифрлау саласындағы кәсіби және криптографиялық терминология; 2.Деректерді шифрлау жүйелерінде қолданылатын негізгі ақпараттық технологиялар мен техникалық құралдар;

	бағдарламалық-аппараттық жүйелерін іске асыру	3.Ақпараттың қауіпсіздігін қамтамасыз ету құралдары мен тәсілдері, деректерді шифрлау жүйелерін құру принциптері; 4.Деректерді шифрлау жүйелерінде қолданылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар; 5.Заманауи бағдарламалау технологиялары; 6.Ашық жүйелердің өзара әрекеттесуінің эталондық моделі, негізгі хаттамалар, заманауи жергілікті және ғаламдық компьютерлік желілердің құрылысы мен жұмыс істеу кезеңдерінің реттілігі мен мазмұны; 7.Электрондық аппаратураның элементтері мен функционалдық тораптарының жұмыс принциптері, электрондық аппаратураның негізгі тораптары; мен блоктарының үлгілік схемотехникалық шешімдері; 8.Бағдарламалық және аппараттық қамтамасыз етуді құжаттауды әзірлеу мен сүйемелдеу процесін ұйымдастыру қағидаттары; 9.Бағдарламалық және аппараттық құралдарды сынау және жөндеу әдістері; 10.Ақпаратты қорғау саласындағы заңнама.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: Деректерді шифрлаудың әзірленген жүйелерін тестілеу	Машықтар: 1. таңдалған бағдарламалау тілінде бағдарламалық қамтамасыз етудің жұмысқа қабілеттілігін тексеру рәсімін тестілеу; 2. Тестілеудің әдістері мен құралдарын қолдану; 3. таңдалған бағдарламалау ортасын таңдалған бағдарламалау тілінде бағдарламалық қамтамасыз етудің жұмысқа қабілеттілігін тексеру рәсімдерін әзірлеу үшін пайдалану; 4. Бағдарламалық қамтамасыз етудің жұмысқа қабілеттілігін тексеру үшін бақылау мысалдарын әзірлеу және ресімдеу; 5. Бағдарламалық қамтамасыз етудің жұмысқа қабілеттілігін тексеру процесінде пайдаланылатын деректер жиынтығын дайындау.
		Білімдер: 1. Бағдарламалық қамтамасыз етудің жұмыс қабілеттілігін автоматты және автоматты тексеру әдістері; 2. Диагностикалық деректердің негізгі түрлері және оларды ұсыну тәсілдері; 3. Утилиталар және бағдарламалау ортасы және рәсімдерді пакеттік орындау құралдары; 4. Бақылау мысалдары мен тестілік деректер жиынтығын жасау және құжаттау әдістері; 5. тестілік деректер жиынтығын жасау қағидалары, алгоритмдері және технологиялары;

		6. Тестілік деректер жиынтығын, криптографиялық алгоритмдерді сақтау құрылымдары мен форматтары.
	Дағдыны тану мүмкіндігі:	Не требуется
Еңбек функциясы 2: Ақпараттық қауіпсіздік регламенттері мен талаптарына сәйкес деректерді шифрлау және ашып көрсету	Дағды 2: Деректерді шифрлау жүйелеріне пайдалану құжаттамасын әзірлеу	Машықтар: 1. Деректерді шифрлау жүйелеріне арналған шараларды (ережелер, рәсімдер, практикалық тәсілдер, басшылық қағидаттар, әдістер, құралдар) айқындау; 2. деректерді шифрлау жүйелерінің АҚ кіші жүйелерін құруға арналған техникалық тапсырмаларды әзірлеу; 3. Қолданыстағы нормативтік және әдістемелік құжаттарды ескере отырып, деректерді шифрлау жүйелерінің кіші жүйелерін жобалау; 4. Деректерді шифрлау жүйелерінің әлеуетті осалдықтарын анықтау мақсатында деректерді шифрлау жүйелері компоненттерінің бағдарламалық, сәулет-техникалық және схемалық-техникалық шешімдерін талдау; 5. Деректерді шифрлау жүйелеріндегі ақпараттық тәуекелдерді бағалау және қорғауға жататын ақпараттық инфрақұрылым мен ақпараттық ресурстарды айқындау; 6. Қорғаудың талап етілетін деңгейін қамтамасыз ету мақсатында деректерді шифрлау жүйелерінде бағдарламалық-аппараттық құралдардың жобалық шешімдеріне техникалық-экономикалық негіздеме жүргізу; 7. Деректерді шифрлау жүйелерінде бағдарламалық-аппараттық құралдардың жобалық шешімдерінің тиімділігін зерттеу.
		Білімдер: 1. Бағдарламалық қамтамасыз етудің жұмыс қабілеттілігін автоматты және автоматты тексеру әдістері; 2. Диагностикалық деректердің негізгі түрлері және оларды ұсыну тәсілдері; 3. Утилиталар және бағдарламалау ортасы және рәсімдерді пакеттік орындау құралдары; 4. Бақылау мысалдары мен тестілік деректер жиынтығын жасау және құжаттау әдістері; 5. тестілік деректер жиынтығын жасау қағидалары, алгоритмдері және технологиялары; 6. Тестілік деректер жиынтығын, криптографиялық алгоритмдерді сақтау құрылымдары мен форматтары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Жауапкершілік Құрылымдық ойлау	

Жеке құзыреттерге қойылатын талаптар:	Табандылық пен зейін Аналитикалық ақыл Өзін-өзі оқыту қабілеті Математикалық қабілеттер			
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті ҚР СТ 1073-2007 Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар			
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:		
	6	Деректерді шифрлаушы		
25. Кәсіптің карточкасы "Цифрлық технологиялар жөніндегі маман-криминалист":				
Топтың коды:	2524-0			
Қызмет атауының коды:	2524-0-008			
Кәсіптің атауы:	Цифрлық технологиялар жөніндегі маман-криминалист			
СБШ бойынша біліктілік деңгейі:	7			
СБШ бойынша біліктілік ішкі деңгейі:	-			
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:				
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -	
Жұмыс тәжірибесіне қойылатын талаптар:				
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары			
Кәсіптің басқа ықтимал атаулары:				
Қызметтің негізгі мақсаты:	Қол сұғушылық объектісі ретінде компьютерлік ақпарат, қылмыс жасау құралы ретінде компьютер, сондай-ақ қандай да бір сандық дәлелдемелер пайда болатын оқиғаларды талдау және тексеру			
Еңбек функциялардың сипаттамасы				
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Компьютерлік қылмыстарды тергеу 2. Сараптамалық деректерге талдау жүргізу		
	Қосымша еңбек функциялары:			
		Машықтар: 1. Ұйымдағы деректердің әлеуетті көздерін анықтау		

		2. Деректерді жинау жоспарын әзірлеу 3. Деректерді алуды және алынған деректердің тұтастығын тексеруді жүзеге асыру 4. Деректерді, соның ішінде процесте қолданылатын әрбір құрал туралы ақпаратты жинау үшін жасалған әрбір қадамның егжей-тегжейлі журналын жүргізуді жүзеге асыру 5. Ақпараттың белгілі бір дереккөзге тиесілігін анықтауға мүмкіндік беретін қасиеттері мен ерекшеліктерін бөліп көрсету 6. Бағдарламалық қамтамасыз етуді топтарға бөлу принциптерін, олардың спецификалық қасиеттерін және компьютерлік жүйемен өзара байланысын анықтау
	Дағды 1: Әлеуетті ақпарат көздерінен деректерді алу	Білімдер: 1. Әлеуетті деректер көздерінің түрлері; 2. Компьютерлік ақпарат тасығыштар; 3. алынған ақпараттың сақталуын, тұтастығын және құпиялылығын қамтамасыз ету әдістері; 4. Ақпарат беру жүйелері мен желілерін құру және олардың жұмыс істеу қағидаттары; 5. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама; 6. Есептеу жүйелерінің архитектурасы, құрылысы және жұмыс істеуі; 7. Ақпаратты қорғауды қамтамасыз ету үшін пайдаланылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар; 8. Компьютерлік қылмыстардың, құқық бұзушылықтар мен инциденттердің іздерін іздеу және талдау технологиялары; 9. Компьютерлік қылмыстардың, құқық бұзушылықтар мен инциденттердің іздерін тіркеу және құжаттау тәртібі.
Еңбек функциясы 1: Компьютерлік қылмыстарды тергеу	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2:	Машықтар: 1.Тасымалдағыштардан ақпаратты алу/Оқуды жүзеге асыру 2.Ақпаратты декодтауды және одан іске қатысты ақпаратты оқшаулауды жүзеге асыру 3.Ақпаратты зерттеудің автоматтандырылған құралдарын пайдалану 4.Зерттелетін тасымалдағыштардан ақпараттың тұтастығы мен сақталуын қамтамасыз ету 5.Ақпаратты қорғауды қамтамасыз ету саласындағы қолданыстағы заңнамалық базаны қолдану 6.Криминалистикалық сараптама және криминалистикалық талдау жүргізу кезінде нормативтік және құқықтық актілерді қолдану
		Білімдер:

	Жиналған ақпаратты сараптамалық зерттеу компьютерлік қылмыстар кезіндегі (тасымалдаушы объектілер)	1. Компьютерлік ақпарат тасығыштардан деректерді алу/оқу әдістері; 2. алынған ақпараттың сақталуын, тұтастығын және құпиялылығын қамтамасыз ету әдістері; 3. деректерді зерттеудің және сүзудің бағдарламалық құралдары; 4. Ақпаратты қорғауды қамтамасыз ету үшін пайдаланылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар; 5. Ақпарат беру жүйелері мен желілерін құру және олардың жұмыс істеу қағидаттары; 6. Цифрлық криминалистика саласындағы нормативтік құқықтық актілер; 7. Компьютерлік қылмыстардың, құқық бұзушылықтар мен инциденттердің іздерін іздеу және талдау технологиялары; 8. Компьютерлік қылмыстарды, құқық бұзушылықтар мен инциденттерді тергеу әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Сараптамалық деректерге талдау жүргізу	Дағды 1: Сараптамалық деректерді өңдеу	Машықтар: 1.Тергеудің алдыңғы кезеңдерінде жиналған ақпаратты талдаңыз. 2.Әр түрлі көздерден, деректерден алынған интерпретацияланған деректерге талдау жасаңыз 3.Компьютерлік файлдардың түрін анықтаңыз, оның ішінде кеңейтусіз 4.Компьютерлік ақпараттың әртүрлі көздерін біріктіре отырып, компьютерлік оқиға оқиғаларын қайта құру 5.Криминалистикалық сараптама және криминалистикалық талдау жүргізу кезінде нормативтік және құқықтық актілерді қолдану
		Білімдер: 1. Алынған ақпараттың сақталуын, тұтастығын және құпиялылығын қамтамасыз ету әдістері; 2. Есептеу жүйелерінің архитектурасы, құрылысы және жұмыс істеуі; 3. Ақпарат беру жүйелері мен желілерін құру және олардың жұмыс істеу қағидаттары; 4. Ақпаратты өңдеудің бағдарламалық құралдары; 5. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама; 6. Талданатын компьютерлік жүйеде ақпаратты сақтау форматтары; 7. компьютерлік жүйелерде пайдаланылатын файлдардың негізгі форматтары; 8. Компьютерлік жүйелерде конфигурациялық және жүйелік ақпаратты сақтау ерекшеліктері; 9. Компьютерлік жүйелер мен желілердің осалдықтары;

		10. Компьютерлік қылмыстарды, құқық бұзушылықтар мен инциденттерді тергеу әдістері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Зерттеу және талдау нәтижелерін заңда белгіленген және маман емес адамдарға түсінікті нысанда ресімдеу	Машықтар: 1. Талдау қорытындылары бойынша есептік материалдарды жасау; 2. Талдау жөніндегі ақпаратты өзектендіру; 3. Компьютерлік оқыс оқиғалар мен қылмыстарды болдырмау бойынша ұсынымдар әзірлеу.
		Білімдер: 1. Алынған ақпараттың сақталуын, тұтастығын және құпиялылығын қамтамасыз ету әдістері; 2. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама; 3. Есептеу жүйелерінің архитектурасы, құрылысы және жұмыс істеуі; 4. Ақпарат беру жүйелері мен желілерін құру және олардың жұмыс істеу қағидаттары; 5. Ақпаратты өңдеудің бағдарламалық құралдары; 6. Компьютерлік жүйелердің ақпараттық-талдамалық және техникалық сараптамасы бойынша орындалған жұмыстардың нәтижелері бойынша ғылыми-техникалық сараптамалық қорытындыларды дайындау тәртібі.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Күйзеліске тұрақтылық Аналитикалық ойлау Сыни талдау Ұйымдастыру Оқу мүмкіндігі Командада жұмыс істей білу	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	6	Цифрлық технологиялар бойынша криминалист-маман
26. Кәсіптің карточкасы "Ақпараттық қауіпсіздік жөніндегі әкімші":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-001	
Кәсіптің атауы:	Ақпараттық қауіпсіздік жөніндегі әкімші	

СБШ бойынша біліктілік деңгейі:	7		
СБШ бойынша біліктілік ішкі деңгейі:			
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:	- -		
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда АТ білім беру		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Механиканы басқару қауіпсіздік талаптары және уақтылы АҚ бұзушылықтарына ден қою		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Ақпаратты қорғау және АҚ-ны қамтамасыз ету үшін ӨҚБ-ны әкімшілендіру, пайдалану және жұмысқа қабілеттілігін қолдау 2. Қауіпсіздік механизмдерін әкімшілендіру 3. АҚ инциденттеріне ден қою 4. Ақпаратты қорғаудың және АҚ қамтамасыз етудің ӨҚБ қолдану тиімділігін бақылау және талдау	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Ақпаратты қорғау және АҚ қамтамасыз ету БАҚ-ын пайдалану; 2. Ақпаратты қорғау және АҚ қамтамасыз ету БАҚ-ын жұмыс берушіден және/немесе орындаушыдан қабылдау; 3. Құпия ақпарат көздерін есепке алу және сақтау; 4. Құпия ақпаратты қорғау БАҚ пайдалану; 5. Ақпаратты қорғау және АҚ қамтамасыз ету құралдарына техникалық қызмет көрсету бойынша регламенттік және алдын алу жұмыстарын жүргізу.	
		Білімдер: 1. Мемлекеттік құпияны және қолжетімділігі шектеулі өзге де ақпаратты қорғау жөніндегі қызметті реттейтін заңнамалық және өзге де нормативтік құқықтық актілер;	

	Дағды 1: Ақпаратты қорғаудың және АҚ қамтамасыз етудің ӨҚБ пайдалану	2. Ақпараттың техникалық қорғалуын қамтамасыз етуге байланысты мәселелер бойынша нормативтік және әдістемелік құжаттар; 3. Қорғауға жататын ақпараттандыру объектілері; 4. Ұйымның және оның бөлімшелерінің мамандануы мен қызметінің бағыттары; 5. Қолданылатын ақпараттық технологиялар мен жүйелер; 6. Басқару, байланыс, автоматтандыру құрылымы; 7. Техникалық барлау құралдары және олардың мүмкіндіктерін бағалау әдістері; 8. Ақпараттың қауіпсіздігіне төнетін қатерлер және бұзушылықтардың сыныптамасы (санаттары); 9. Ақпараттандыру объектілерінің негізгі және қосалқы техникалық құралдармен және жүйелермен , кешендермен және ақпаратты техникалық қорғау құралдарымен жарақтандырылуы, автоматтандырылған басқару жүйелерінің сервистері мен қауіпсіздік механизмдерімен; 10. Қолжетімділікті шектеудің ішкі жүйелері; 11. Шабуылдарды анықтаудың ішкі жүйелері; 12. Қасақана әсер етуден қорғаудың ішкі жүйелері; 13. Ақпараттың тұтастығын бақылау әдістері, олардың дамуы мен модернизациясының болашағы; 14. Қауіпсіздік жүйелерінің жай-күйін бағалау, ақпараттың таралу арналарын анықтау, резервтеу процесін бақылау және маңызды есептеу және ақпараттық ресурстардың қайталануын бақылау әдістері; 15. Ақпаратты қорғаудың және бақылаудың техникалық, бағдарламалық, бағдарламалық-аппараттық құралдарымен, автоматтандырылған басқару жүйелерінің қызметтері мен қауіпсіздік механизмдерімен және олардың жай-күйін тексерумен жұмыс істеу тәртібі.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ақпараттық ресурстарды уақтылы қорғауды қамтамасыз ете отырып, орталықтандырылған басқару жүйелерін қолдана отырып, вирусқа қарсы бағдарламалық қамтамасыз ету мен вирустық дерекқорды қашықтықтан орнатуды және жаңартуды тиімді жүзеге асыру; 2. Барлық IT-инфрақұрылым объектілеріне орталықтандырылған орнату үшін олардың өзектілігі мен қолжетімділігін қамтамасыз ете отырып, желілік серверлерде вирусқа қарсы шешімдер дистрибутивтерінің репозиторийлерін ұйымдастыру және қолдау; 3. Ұйымның қауіпсіздік саясатына сәйкес қорғау деңгейін оңтайландыра отырып, жұмыс

		станциялары мен серверлерде вирусқа қарсы шешімдерді қашықтықтан реттеу; 4. Әкімшілендіру процестерінің тиімділігін және автоматтандырылуын арттыра отырып, дереу немесе кейінге қалдыру мүмкіндігімен желі құрылғыларында сканерлеуді, жаңартуларды және басқа да операцияларды орындауға тапсырмаларды әзірлеу және жоспарлау.
	Дағды 2: Техникалық сүйемелдеу (регламенттік, қалпына келтіру және профилактикалық жұмыстар)	Білімдер: 1. Қауіптерді анықтаудың сигнатуралық, эвристикалық, мінез-құлық әдістерін, сондай-ақ проактивті қорғау және ақпараттық қауіпсіздіктің басқа құралдарымен интеграциялау технологияларын қоса алғанда, вирусқа қарсы бағдарламалардың мақсаты, жіктелуі және жұмыс істеу қағидаттары; 2. Операциялық жүйелердің, қауіпсіздік саясатының және корпоративтік инфрақұрылымның ерекшеліктерін, сондай-ақ ортаны алдын ала дайындау жөніндегі талаптарды ескере отырып, вирусқа қарсы бағдарламалық қамтамасыз етуді өндірушілердің оны дұрыс орнату жөніндегі ресми әдістемелік ұсынымдарын; 3. Қауіпсіздік саясатын басқаруды, жаңартуларды автоматтандыруды, есептілікті ұйымдастыруды, инциденттердің мониторингін және қауіптерге уақтылы ден қоюды қоса алғанда, вирусқа қарсы шешімдерді әзірлеушілердің оларды баптау, әкімшілендіру және сүйемелдеу жөніндегі ұсынымдары.
	Дағдыны тану мүмкіндігі :	Талап етілмейді
Еңбек функциясы 1: Ақпаратты қорғау және АҚ-ны қамтамасыз ету үшін ӨҚБ-ны әкімшілендіру, пайдалану және жұмысқа қабілеттілігін қолдау		Машықтар: 1. Әлеуетті қатерлерге уақтылы ден қоюды және ақпараттық қауіпсіздік саясатын іске асыруды қамтамасыз ете отырып, басып кіруді анықтау және болдырмау жүйелерін (IDS/IPS) қолдана отырып, желі қауіпсіздігінің кешенді мониторингін жүзеге асыру; 2. Рөлдік қолжетімділік әдістерін (RBAC) қолдана отырып, сондай-ақ Zero Trust қағидаттарына сәйкес желілік инфрақұрылымды сегменттеуді және трафикті сүзуді іске асыра отырып, қол жеткізу құқықтарын қатаң шектеуді іске асыра отырып, пайдаланушылардың есептік жазбаларын әкімшілендіру; 3. Парольдердің күрделілігіне қойылатын талаптарды, оларды ауыстыру кезеңділігін қоса алғанда, сондай-ақ аутентификация ережелері бұзылған кезде есептік жазбаларды автоматты бұғаттау тетіктерін іске асыра отырып, ұйымның парольдік саясатын баптау және сүйемелдеу;

	Дағды 3: Вирусқа қарсы БҚ әкімшілендіру	4. VPN, желілік экрандарды, NAT, DHCP, ACL және басқа компоненттерді конфигурациялауды қоса алғанда, желі ресурстарына қауіпсіз және бақыланатын қосылуды қамтамасыз ете отырып, желілік қолжетімділік параметрлерін конфигурациялауды орындау; 5. IP-мекенжайлар, хосттар және кіші желілер бойынша өте маңызды ресурстарға қол жеткізуді шектеу, шабуыл жасау бетін барынша азайту және сырттан рұқсатсыз кіруді болдырмау; 6. АТ-инфрақұрылымының қорғалуы мен тұрақтылығын арттыру мақсатында жаңартуларды тестілеуді, жоспарлауды және орталықтандыруды қоса алғанда, корпоративтік ортада бағдарламалық қамтамасыз етуді жаңарту процесін басқару.
		Білімдер: 1. Басып кіруді анықтау/болдырмау жүйелерінің мақсаты, жұмыс істеу қағидаттары, архитектурасы; 2. Басып кіруді анықтау жүйелерінің жұмыс істеуін регламенттейтін стандарттар; 3. Басып кіруді анықтау/болдырмау жүйесін өндірушінің оны орнату және пайдалану жөніндегі ұсынымдары; 4. Басып кіруді анықтау түрлері мен әдістері; 5. Басып кіруді болдырмау жүйелерінде пайдаланылатын технологиялар мен құралдар;
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 4:	Машықтар: 1. Желіаралық экран және сүзгілеу саясаты режимдерін баптау; 2. Әкімшінің тіркелгісін жасауды, кіру құқықтарын шектеуді жүзеге асыру; 3. Резервтік көшіруді және қалпына келтіруді орындау; 4. Сервистерді баптауды жүзеге асыру (DNS, DHCP және басқа да ішкі желілік сервистер); 5. Оқиғаларды логикалау және мониторингілеу; 6. Бағыттауды баптау және реттеу; 7. Виртуалды домендер мен желілерді теңшеу; 8. IPsec VPN қорғалған қосылымдарын теңшеу; 9. Аутентификация саясатын теңшеу; 10. Криптографиялық сертификаттарды басқару және қолдану.
		Білімдер: 1. Сүзу ережесі және оларды қолдану тәртібі; 2. Желіаралық экрандардың түрлері мен функциялары; 3. NAT пайдалану;

	Желіаралық экранды теңшеу және баптау	4. Оқиғаларды мониторингілеу және журналға түсіру; 5. Жаңарту және патчинг жүйесі.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 5: Жүйені әкімшілендіру интрузияларды анықтау/ алдын алу	Машықтар: 1. Оқиғаны сипаттауды, қауіп-қатерді жою үшін қабылданған әрекеттерді, себептерді талдауды, сондай-ақ тергеу нәтижелерін қоса алғанда, қауіпсіздік инциденттері бойынша есептер жасауға; 2. Қол жеткізу әрекеттері, рұқсат етілмеген әрекеттер және басқа да оқиғалар туралы ақпаратты қоса алғанда, қауіпсіздік оқиғаларының журналдарын үнемі жаңартып отыру және жүргізу; 3. Деректерге қол жеткізу, шифрлау және парольдерді пайдалану саясатын қоса алғанда, қауіпсіздік саясаттары мен рәсімдері бойынша құжаттамаларды жасау және қолдау; 4. Осалдықтар мен патч-менеджмент бойынша есептілікті жүргізеді және ағымдағы осалдықтар мен патчтар туралы есептерді уақтылы жасайды; 5. Қауіп-қатерлерді жою, деректерді қалпына келтіру және залалды азайту жөніндегі қадамдық нұсқаулықтарды қоса алғанда, инциденттерге ден қою рәсімдерін құжаттау.
		Білімдер: 1. Ақпараттық қауіпсіздік саласындағы есептілікке қойылатын стандарттар мен талаптар; 2. Есептіліктің құрылымы мен форматтарын, оларды жасау тәртібін түсіну; 3. Қауіпсіздік деректерін талдау және өңдеу, қауіпсіздік оқиғалары журналдарынан және басқа да көздерден деректерді түсіндіру әдістері; 4. Барлық маңызды оқиғаларды тіркеуді қоса алғанда, оқиғалар мен инциденттер журналдарын жүргізу қағидаттары; 5. Қауіпсіздік инфрақұрылымындағы өзгерістер мен инциденттерді басқару принциптері мен процестері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1:	Машықтар: 1. Қызметкерлердің қорғалатын ақпаратқа қол жеткізу құқықтары мен өкілеттіктерінің тізімін жасауға және өзекті жағдайда ұстауға; 2. Жаңартулардың шығуын мониторингілеу және серверлік және желілік жабдықтардың ҚБҚ, ДББЖ, БЖ нұсқаларын басқару; 3. Бағдарламалық қамтамасыз ету нұсқаларын және қол жеткізу құқықтарының тізімдерін жаңарту бойынша келісілген жұмысты қамтамасыз ету үшін басқа әкімшілермен өзара іс-қимыл жасау.

Еңбек функциясы 2: Қауіпсіздік механизмдерін әкімшілендіру	Әкімшілендіру бойынша процестерді басқару	Білімдер: 1. АТ-процестерін басқарудың өмірлік циклі: жоспарлау, жобалау, енгізу, пайдалану, қолдау және аяқтау; 2. АТ-қызметтерін басқаруға арналған қағидаттар мен модельдер; 3. Жүйенің жұмыс істеуіне қауіп төндірмейтін өзгерістерді және конфигурацияларды басқару; 4. Түрлі құралдардың көмегімен жүйенің өнімділігін бақылау және мониторингілеу; 5. Қауіпсіздік қатерлері мен инциденттерін немесе жүйе жұмысындағы ақауларды басқару.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Саясатты орнату ОЖ, ДҚБЖ, ҚБҚ қауіпсіздігі	Машықтар: 1. Криптографиялық кілттерді басқару (генерациялау және бөлу); 2. Шифрлауды басқару (Криптографиялық параметрлерді орнату және синхрондау); 3. Аутентификацияны басқару (аутентификация үшін қажетті ақпаратты - парольдерді, кілттерді және т.б. бөлу); 4. Кіруді басқару (басқару үшін қажетті ақпаратты - парольдерді, кіру тізімдерін және т.б. бөлу); 5. Желі домендерінің бақылаушыларын орнату және теңшеу.
		Білімдер: 1. Мақсаттарды, тәуекелдер мен талаптарды айқындауды қоса алғанда, қауіпсіздік саясатын әзірлеу қағидаттары; 2. Қауіпсіздік саясатының түрлері, оның ішінде: кіруді басқару саясаты; парольдерді пайдалану саясаты; деректерді өңдеу саясаты; инциденттерді басқару саясаты; 3. Әртүрлі нормативтік актілермен және стандарттармен белгіленген қауіпсіздік талаптары; 4. Қызметкерлерді оқытуды, саясаттың сақталуын бақылау және қамтамасыз ету жүйесін құруды қоса алғанда, саясатты іске асыру және енгізу процесі; 5. Ұйымдастыру құрылымындағы өзгерістерге, жаңа қатерлерге немесе заңнамадағы өзгерістерге жауап ретінде қауіпсіздік саясатына мониторинг жүргізу және қайта қарау.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. АҚ мониторингіндегі жүйелердегі оқиғаларды жинау және талдау; 2. Оқиғаларды, сериялық оқиғаларды және оқиғалар үйлесімін АҚ бұзушылықтары ретінде жіктеу;

		3. Оқиғаларды өңдеу рәсімдерін теңшеу және АҚ оқиғаларын анықтау.
	Дағды 1: АҚ оқиғалары мен инциденттерінің мониторингі	Білімдер: 1. Нақты уақыттағы қауіпсіздік оқиғалары туралы деректерді жинайтын, талдайтын және қадағалайтын басқару жүйелерін пайдалануды қоса алғанда, қауіпсіздік мониторингі процесі; 2. Қауіпсіздік оқиғаларының түрлері және олардың жіктелуі; 3. Машиналық оқытуды және үлкен деректерді талдауды қоса алғанда, инциденттерді талдау және қауіп-қатерді анықтау қағидаттары; 4. Қауіпсіздік оқиғаларының журналдарын жүргізу және үрдістерді талдау және тәуекелдерді анықтау үшін есептерді жасау тәртібі.
Еңбек функциясы 3: АҚ инциденттеріне ден қою	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: АҚ инциденттеріне ден қою	Машықтар: 1. АҚ тосын оқиғасы туралы тіркеу және хабарлау (хабарлау); 2. АҚ тосын оқиғасының себептерін анықтау; 3. АҚ тосын оқиғасы мен оның зардаптарын жою шараларын қабылдау; 4. Инцидент туралы дәлелдемелер жинауға; 5. АҚ тосын оқиғаларын тексеруге қатысу; 6. Құзыретті органдармен (CERT, ішкі істер органдары және басқалар) өзара іс-қимыл жасайды.
		Білімдер: 1. Инциденттерге ден қою процестері және процестің негізгі кезеңдері; 2. Қауіпсіздік инциденттерін түрлері мен күрделілігі бойынша жіктеу; 3. Дәлелдемелерді жинауға және болып жатқан оқиғаларды талдауға көмектесетін тосын оқиғаларды тексеруге арналған құралдар; 4. Ден қою процесіндегі коммуникацияның рөлі; 5. Қауіпсіздікті жақсарту үшін тосын оқиғаларды құжаттандыру және талдау тәртібі.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: Технологиялық процесті а ғ ы м д ы қ бақылауқорғалатын	Машықтар: 1. Ақпаратты қорғау және АҚ қамтамасыз ету АЖЖ орналастыру және конфигурациялау жөніндегі құжаттаманы жасау және өзекті жағдайда ұстау; 2. Серверлік және телекоммуникациялық жабдықтардың ҚБҚ, ДББЖ, БЖ қауіпсіздік тетіктерін баптаудың тұтастығын бақылау; 3. ЖТӘ АЖ және қорғалатын ақпараттық ресурстарға әрекеттерін анықтау мақсатында жүйелік және қолданбалы БҚ оқиғаларын тіркеу журналдарын талдау.

Еңбек функциясы 4: Ақпаратты қорғаудың және АҚ қамтамасыз етудің ӨҚБ қолдану тиімділігін бақылау және талдау	материалды өңдеу процесі туралы ақпараттың	Білімдер: 1. Бақылауды жүзеге асырудың әдістері, қағидаттары мен тәсілдері; 2. АҚ оқиғалар журналын талдау рәсімдері (талдау міндеттерін орындау, тексеру жүргізу және стандартты емес оқиғаларды талдау, рәсімдердің орындалуын құжаттау және дәлелдемелерді жинау, басшылық үшін есептілікті қалыптастыру); 3. АҚ оқиғалар журналын талдаудың бағдарламалық құралдары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Ақпаратты қорғау және АҚ қамтамасыз ету БАҚ жұмысын ағымдағы және мерзімді бақылау	Машықтар: 1. Ақпаратты қорғау және АҚ қамтамасыз ету ПАС оқиғаларын тіркеу журналдарын талдау; 2. Ақпаратты қорғау және АҚ қамтамасыз ету ПАС ресурстарын пайдалануды бағалау; 3. Ақпаратты қорғаудың және АҚ-ны қамтамасыз етудің АЖЖ пайдалану тиімділігін жетілдіру және арттыру бойынша ұсыныстар әзірлеу.
		Білімдер: 1. Жұмыс принципі және ақпаратты қорғау ЖАЖ пайдалану ережесі; 2. Ақпаратты қорғау және АҚ қамтамасыз ету ПАС ресурстарын пайдалану нәтижелілігінің өлшемдері мен көрсеткіштері; 3. Ақпаратты қорғау және АҚ қамтамасыз ету ПАС бақылау параметрлері.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Ойлау икемділігі Командада жұмыс істей білу Тәртіптілік Бастамашылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	-	-
27. Кәсіптің карточкасы "Ақпаратты қорғау жөніндегі маман":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-006	
Кәсіптің атауы:	Ақпаратты қорғау жөніндегі маман	

СБШ бойынша біліктілік деңгейі:	7		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) АТ білімі болған кезде киберқауіпсіздік саласында біліктілікті арттырудың қосымша кәсіптік курстары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	АЖ ақпаратты қорғау жүйелерін әкімшілендіру		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. АЖ ақпаратын қорғау жүйелерін әзірлеу 2. Компьютерлік жүйелер мен желілердің қауіпсіздік жүйесін әзірлеу	
	Қосымша еңбек функциялары:		
	Дағды 1: Ақпаратты қорғау процесін нормативтік,	Машықтар: 1, Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс істеу параметрлерін анықтау; 2, Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қорғалуын бағалау әдістемесін әзірлеу; 3, Ақпаратты қорғаудың тиімділігін бағалау; 4, Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қорғалуын бағалаудың әзірленген әдістемелерін қолдану; 5, Қорғаудың бағдарламалық-аппараттық құралдарын олармен қамтамасыз етілетін қорғалу мен сенімділік деңгейін анықтау мақсатында талдау.	
		Білімдер: 1. Компьютерлік жүйелер мен желілерді құру қағидаттары; 2. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қауіпсіздігін бағалау әдістері мен әдістемелері; 3. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын құру қағидаттары;	

Еңбек функциясы 1: АЖ ақпаратын қорғау жүйелерін әзірлеу	әкімшілік, техникалық және ғылыми қамтамасыз ету	4. Компьютерлік жүйелердегі ақпаратты қорғаудың кіші жүйелерін құру қағидаттары; 5. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарында іске асырылған қауіпсіздік саясатының тиімділігін бағалау әдістері; 6. Ақпаратты қорғау алгоритмдерін бағдарламалық іске асырудың дұрыстығы мен тиімділігін бағалау әдістері мен құралдары; 7. Әлеуетті осалдықтар мен құжатталмаған мүмкіндіктерді іздеу мақсатында бағдарламалық кодты талдау әдістері; 8. Ақпаратты қорғаудың қолданылатын әдістері мен құралдарын қауіпсіздік саясатына сәйкестігі тұрғысынан талдау тәсілдері; 9. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар; 10. АҚ қамтамасыз ету саласындағы нормативтік құқықтық актілер.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: АЖ ақпаратын қорғау жүйесіне пайдалану құжаттамасын әзірлеу	Машықтар: 1. Қажетті қорғалу деңгейін анықтау үшін компьютерлік жүйені талдау; 2. Компьютерлік жүйелерді қорғау бейінін әзірлеу; 3. Компьютерлік жүйелердің қауіпсіздігі бойынша тапсырмаларды тұжырымдау; 4. Компьютерлік жүйелердің қауіпсіздігіне талдау жасау және ақпаратты қорғау жүйесін пайдалану жөнінде ұсынымдар әзірлеу.
		Білімдер: 1. Компьютерлік жүйелер мен желілерді құру қағидаттары; 2. Компьютерлік жүйелердің қауіпсіздік модельдері; 3. Компьютерлік жүйелер мен желілердің қауіпсіздік саясатының түрлері; 4. Ақпаратты криптографиялық қорғау құралдарын құру қағидаттары; 5. АҚ қамтамасыз ету саласындағы ұлттық стандарттар; 6. Пайдаланылатын және пайдалануға жоспарланған ақпаратты қорғау құралдарының мүмкіндіктері; 7. АҚ қамтамасыз ету саласындағы нормативтік құқықтық актілер.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Қатерлердің модельдерін және компьютерлік жүйелердің қауіпсіздігін бұзушының модельдерін қалыптастыру;

Еңбек функциясы 2: Компьютерлік жүйелер мен желілердің қауіпсіздік жүйесін әзірлеу	Дағды 1: Компьютерлік жүйелер мен желілердің ақпаратын қорғаудың бағдарламалық-аппараттық құралдарына қойылатын талаптарды әзірлеу	2. Компьютерлік жүйенің ақпаратын қорғауды қамтамасыз етудің неғұрлым орынды тәсілдерін анықтау; 3. Компьютерлік жүйелер қауіпсіздігінің жеке саясатын, оның ішінде қолжетімділік пен ақпараттық ағындарды басқару саясатын әзірлеу; 4. Компьютерлік жүйенің қорғалуын бағалау үшін ақпаратты қорғау саласындағы ұлттық стандарттарды қолдану; 5. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын пайдалану қажеттілігі туралы шешім қабылдауды жүзеге асыру.
		Білімдер: 1. Компьютерлік жүйелер мен желілерді құру қағидаттары; 2. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қауіпсіздігін бағалау әдістері мен әдістемелері; 3. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын құру қағидаттары; 4. Компьютерлік жүйелердегі ақпаратты қорғаудың кіші жүйелерін құру қағидаттары; 5. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарында іске асырылған қауіпсіздік саясатының тиімділігін бағалау әдістері; 6. Ақпаратты қорғау алгоритмдерін бағдарламалық іске асырудың дұрыстығы мен тиімділігін бағалау әдістері мен құралдары; 7. Әлеуетті осалдықтар мен құжатталмаған мүмкіндіктерді іздеу мақсатында бағдарламалық кодты талдау әдістері; 8. Ақпаратты қорғаудың қолданылатын әдістері мен құралдарын қауіпсіздік саясатына сәйкестігі тұрғысынан талдау тәсілдері; 9. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар; 10. АҚ қамтамасыз ету саласындағы нормативтік құқықтық актілер.
	Дағдыны тану мүмкіндігі:	-
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Жүйелі ойлау Аналитикалық ойлау Сыни талдау Ұйымдастыру Стандартты емес мәселелерді шеше білу Егжей-тегжейге назар аудару	
	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
	6	Ақпаратты қорғау жөніндегі маман	
28. Кәсіптің карточкасы "Қауіпсіздік мәселелері жөніндегі маман (АКТ)":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-005		
Кәсіптің атауы:	Қауіпсіздік мәселелері жөніндегі маман (АКТ)		
СБШ бойынша біліктілік деңгейі:	6		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:			
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:	2524-0-004 - Сервистердің қауіпсіздігі жөніндегі маман 2524-0-006 - Ақпаратты қорғау жөніндегі маман 2524-0-007 - Ақпараттық қауіпсіздік жөніндегі маман		
Қызметтің негізгі мақсаты:	Инфокоммуникациялық жүйелердің ішкі жүйелеріне, құрылғыларына, элементтеріне және арналарына бағдарламалық-техникалық әсердің зиянды әсеріне қарсы тұру		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Компьютерлік жүйелер мен желілердегі ақпаратты қорғау құралдарын әкімшілендіру 2. Ақпараттық қауіпсіздік саласындағы тәуекелдерді бағалау және басқару	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Операциялық жүйелердің қауіпсіздік саясатын тұжырымдау; 2. операциялық жүйелердің қауіпсіздік саясатын баптау; 3. Операциялық жүйелер ақпаратының қауіпсіздігіне қауіп-қатерлерді бағалау; 4. Операциялық жүйелердің ақпаратты қорғаудың кіріктірілген құралдарын пайдалана отырып,	

		ақпарат қауіпсіздігіне төнген қатерлерге қарсы іс-қимыл жасау; 5. Операциялық жүйелерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс режимдерін таңдау; 6. операциялық жүйелерде ақпаратты қорғаудың вирусқа қарсы құралдарын баптау; 7, Бағдарламалық қамтамасыз ету және вирусқа қарсы қорғау құралдарын жаңартуды орнату; 8. Операциялық жүйелерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс істеуіне мониторинг жүргізу; 9. Операциялық жүйелерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының тиімділігіне талдау жүргізу; 10. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын және олардың операциялық жүйелерде жұмыс істеу режимдерін таңдаудың оңтайлылығын бағалау.
	Дағды 1: Нормативтік, әкімшілік, техникалық және ғылыми қамтамасыз ету қамтамасыз етумен ақпараттық инфрақұрылымның негізгі жүйелеріндегі ақпараттың қауіпсіздігі	Білімдер: 1. операциялық жүйелерді құру архитектурасы мен принциптері; 2. операциялық жүйелердің бағдарламалық интерфейстері; 3. Операциялық жүйелерге қатысты қолжетімділікті және ақпараттық ағындарды басқару саясаттарының түрлері; 4. Операциялық жүйелердегі ақпаратты қорғаудың кіші жүйелерінің архитектурасы; 5. Операциялық жүйелерде, оның ішінде криптографиялық алгоритмдерді пайдаланатын ақпаратты қорғау құралдарының жұмыс істеу қағидаттары; 6. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының типтік конфигурацияларының құрамы; 7. Операциялық жүйелерге арналған ақпаратты қорғау кіші жүйелерінің құрамына және сипаттамаларына қойылатын талаптар; 8. Операциялық жүйелерде вирусқа қарсы қорғау әдістері мен құралдарын іске асыру тәртібі; 9. Бағдарламалық-аппараттық құралдар және операциялық жүйелердегі ақпаратты қорғау әдістері; 10. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс істеу қағидаттары мен пайдалану қағидалары; 11. Ақпаратты қорғау саласындағы заңнама.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар:

		1, Компьютерлік желілердегі ақпарат қауіпсіздігіне төнген қатерлерді бағалау; 2. компьютерлік желілерде пакеттерді сүзу ережелерін баптау; 3, Компьютерлік желілерде ақпаратты қорғаудың пайдаланылатын бағдарламалық-аппараттық құралдарын таңдау; 4, Компьютерлік желілерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын конфигурациялау және баптаудың дұрыстығын бақылау; 5, Компьютерлік желілерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс режимдерін таңдау; 6, Компьютерлік желілерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс істеуіне мониторинг жүргізу; 7, Компьютерлік желілерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының тиімділігіне талдау жүргізу; 8, Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын және олардың компьютерлік желілерде жұмыс істеу режимдерін таңдаудың оңтайлылығын бағалау.
Еңбек функциясы 1: Компьютерлік жүйелер мен желілердегі ақпаратты қорғау құралдарын әкімшілендіру	Дағды 2: Операциялық жүйелердегі ақпаратты қорғаудың ішкі жүйелерін басқару	Білімдер: 1. Компьютерлік желілерді құру принциптері; 2. операциялық жүйелердің желілік хаттамаларының стегі; 3. Желілік жабдық хаттамаларының стегі; 4. Желіаралық экрандау әдістері мен құралдарын іске асыру тәртібі; 5. Криптографиялық алгоритмдерді қамтитын желілік хаттамалардың жұмыс істеу қағидаттары; 6. Компьютерлік желілердегі қолжетімділікті және ақпараттық ағындарды басқару саясатының түрлері; 7. Компьютерлік желілердегі ақпараттық қауіпсіздікке төнген қатерлердің көздері және олардың алдын алу жөніндегі шаралар; 8. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының типтік конфигурацияларының және олардың компьютерлік желілерде жұмыс істеу режимдерінің құрамы; 9. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының сипаттамаларын өлшеу, бақылау және техникалық есептеу әдістері; 10. Ақпаратты қорғаудың пайдаланылатын бағдарламалық-аппараттық құралдарының жұмыс істеу қағидаттары мен пайдалану қағидалары; 11. Бағдарламалық-аппараттық құралдар және компьютерлік желілердегі ақпаратты қорғау әдістері ;

		12. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар..
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Бағдарламалық қамтамасыз ету ақпаратының қауіпсіздігіне төнген қатерлерді талдау; 2. Бағдарламалық қамтамасыз етуді қауіпсіз пайдалану ережелерін тұжырымдау; 3. Бағдарламалық қамтамасыз етуді қауіпсіз пайдалану ережелерін негіздеу; 4. Ықтимал зиянды әсерді анықтау мақсатында бағдарламалық қамтамасыз етудің жұмыс істеуін талдау; 5. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының нақты сипаттамаларының олардың техникалық құжаттамасында мәлімделгенге сәйкестігін тексеру; 6. Бағдарламалық қамтамасыз етуді пайдалану кезінде туындайтын ақпарат қауіпсіздігіне қауіп-қатерлерге қарсы іс-қимыл жөніндегі іс-шараларды жүзеге асыру; 7. Ақпаратты қорғауды қамтамасыз ету мақсатында бағдарламалық қамтамасыз етудің жұмыс істеу тәртібін айқындау; 8. Бағдарламалық қамтамасыз етудің ақпаратты қорғаудың кіріктірілген құралдарына қойылатын тұжырымдалған талаптардың тиімділігін талдау.
	Дағды 3: Компьютерлік желілердегі ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын әкімшілендіру	Білімдер: 1. Операциялық жүйелердегі ақпаратты қорғаудың кіші жүйелерінің архитектурасы; 2. Компьютерлік желілерді құру принциптері; 3. Операциялық жүйелердің желілік протоколдарының стегі; 4. Желілік жабдық хаттамаларының стегі; 5. Желіаралық экрандаудың әдістері мен құралдарын енгізу тәртібі; 6. Криптографиялық алгоритмдерді қамтитын желілік хаттамалардың жұмыс істеу принциптері; 7. Компьютерлік желілердегі қол жетімділікті және ақпараттық ағындарды басқару саясатының түрлері; 8. Компьютерлік желілердегі ақпараттық қауіпсіздікке төнетін қатерлердің көздері және олардың алдын алу шаралары; 9. Үлгілік құрамдардың құрамы ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының конфигурацияларын және олардың компьютерлік желілерде жұмыс істеу режимдері; 10. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының сипаттамаларын өлшеу, бақылау және техникалық есептеулер әдістері;

		11. Ақпаратты қорғаудың пайдаланылатын бағдарламалық-аппараттық құралдарының жұмыс істеу қағидаттары мен пайдалану қағидалары; 12. Компьютерлік желілердегі ақпаратты қорғаудың бағдарламалық-аппараттық құралдары мен әдістері; 13. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер; 14. Ақпаратты қорғау жөніндегі ұйымдастырушылық шаралар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2:	Дағды 1: Қолданбалы және жүйелік бағдарламалық қамтамасыз ету ақпаратын қорғау құралдарын әкімшілендіру	Машықтар: 1. Бағдарламалық қамтамасыз ету ақпаратының қауіпсіздігіне төнген қатерлерді талдау; 2. Бағдарламалық қамтамасыз етуді қауіпсіз пайдалану ережелерін тұжырымдау; 3. Бағдарламалық қамтамасыз етуді қауіпсіз пайдалану ережелерін негіздеу; 4. Ықтимал зиянды әсерді анықтау мақсатында бағдарламалық қамтамасыз етудің жұмыс істеуін талдау; 5. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының нақты сипаттамаларының олардың техникалық құжаттамасында мәлімделгенге сәйкестігін тексеру; 6. Бағдарламалық қамтамасыз етуді пайдалану кезінде туындайтын ақпарат қауіпсіздігіне қауіп-қатерлерге қарсы іс-қимыл жөніндегі іс-шараларды жүзеге асыру; 7. Ақпаратты қорғауды қамтамасыз ету мақсатында бағдарламалық қамтамасыз етудің жұмыс істеу тәртібін айқындау; 8. Бағдарламалық қамтамасыз етудің ақпаратты қорғаудың кіріктірілген құралдарына қойылатын тұжырымдалған талаптардың тиімділігін талдау.
		Білімдер: 1. Операциялық жүйелердегі ақпаратты қорғаудың кіші жүйелерінің архитектурасы; 2. Дерекқорларды басқару жүйелерін құру қағидаттары; 3. Бағдарламалық іске асыруды талдаудың негізгі құралдары мен әдістері; 4. Вирусқа қарсы бағдарламалық қамтамасыз етуді құру қағидаттары; 5. Қолданбалы бағдарламалық қамтамасыз етуге қатысты қолжетімділікті және ақпараттық ағындарды басқару саясаттарының түрлері; 6. Бағдарламалық қамтамасыз етудің ақпараттық қауіпсіздігіне қатер төндіру көздері және оларды болдырмау жөніндегі шаралар;

Ақпараттық қауіпсіздік саласындағы тәуекелдерді бағалау және басқару		7. Пайдаланылатын бағдарламалық қамтамасыз етудің осалдықтары және оларды пайдалану әдістері ; 8. Зиянды бағдарламалық қамтамасыз етудің түрлері мен жұмыс істеу нысандары; 9. Зиянды бағдарламалық қамтамасыз етудің болуына тән белгілер; 10. Бұрын белгісіз зиянды бағдарламалық қамтамасыз етуді табу құралдары мен әдістері; 11. Ақпаратты криптографиялық қорғаудың бағдарламалық құралдарының жұмыс істеу қағидаттары; 12. Бағдарламалық қамтамасыз етуді пайдалану кезінде ақпарат қауіпсіздігін қамтамасыз ету тәртібі; 13. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер; 14. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары.
	Дағдыны тану мүмкіндігі :	Не требуется
	Дағды 2: АКТ пайдаланумен байланысты тәуекелдерді бағалау әдістемелерін әзірлеу және енгізу	Машықтар: 1. Қауіп-қатерлерді, осалдықтар мен салдарларды қоса алғанда, АКТ-ны пайдалануға байланысты әлеуетті тәуекелдерді анықтау және талдау; 2. Ұйымның және оның ақпараттық жүйелерінің ерекшеліктерін ескере отырып, тәуекелдерді бағалау әдістемелерін әзірлеу және бейімдеу; 3. Басшылық пен техникалық персоналды қоса алғанда, тәуекелдерді бағалау нәтижелерін құжаттау және оларды мүдделі тараптарға ұсыну; 4. Қорғау құралдары мен бақылау іс-шараларын енгізуді қоса алғанда, тәуекелдерді төмендету және басқару бойынша ұсынымдарды тұжырымдау.
		Білімдер: 1. Ақпараттық қауіпсіздік негіздері; 2. Тәуекелдерді бағалау әдіснамасы; 3. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар; 4. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама.
	Дағдыны тану мүмкіндігі :	-
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Жүйелі ойлау Аналитикалық ойлау Сыни талдау Ұйымдастыру Стандартты емес мәселелерді шеше білу Егжей-тегжейге назар аудару	
	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар"	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
	7	Қауіпсіздік мәселелері жөніндегі маман (АКТ)	
29. Кәсіптің карточкасы "Ақпаратты қорғау жөніндегі маман":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-006		
Кәсіптің атауы:	Ақпаратты қорғау жөніндегі маман		
СБШ бойынша біліктілік деңгейі:	6		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:	Параграф 3. Ақпаратты қорғау жөніндегі маман Ақпаратты қорғау жөніндегі маманы		
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:	I санатты ақпаратты қорғау маманы: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білім және II санаттағы ақпаратты қорғау маманы лауазымында кемінде 3 жыл жұмыс өтілі; II санатты ақпаратты қорғау маманы: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білім және санатсыз ақпаратты қорғау маманы лауазымында кемінде 3 жыл жұмыс өтілі; Ақпаратты қорғау маманы: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білім, жұмыс өтіліне талаптар қойылмайды.		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:	2524-0-007 - Ақпараттық қауіпсіздік жөніндегі маман 2524-0-005 - Қауіпсіздік мәселелері жөніндегі маман (АКТ) 2524-0-004 - Сервистердің қауіпсіздігі жөніндегі маман		
Қызметтің негізгі мақсаты:	АЖ ақпаратты қорғау жүйелерін әкімшілендіру		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. АЖ-да оларды пайдалану процесінде ақпараттың қорғалуын қамтамасыз ету 2. АЖ-да ақпаратты қорғау жүйелерін енгізу	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Ақпараттық қауіпсіздікке қатерлерді жіктеу және бағалау;	

	Дағды 1: Ақпаратты қорғау процесін нормативтік, әкімшілік, техникалық және ғылыми қамтамасыз ету	2. АЖ-дағы ақпарат қауіпсіздігінің әлеуетті осалдықтарын анықтау мақсатында автоматтандырылған жүйелер компоненттерінің бағдарламалық, сәулет-техникалық және схемалық-техникалық шешімдерін талдау; 3. Автоматтандырылған жүйелердің ақпарат қауіпсіздігі саясатын іске асыру бойынша қабылданған шаралардың тиімділігін бақылау; 4. Қауіпсіздік оқиғаларын және автоматтандырылған жүйелерді пайдаланушылардың іс-қимылдарын бақылау; 5. Ақпаратты қорғау шараларының тиімділігін бақылаудың техникалық құралдарын қолдану; 6. Автоматтандырылған жүйенің ақпаратты қорғау жүйесінің жұмыс істеуін бақылау рәсімдері мен нәтижелерін құжаттау.
		Білімдер: 1. Қорғалған АЖ және АЖ қауіпсіздігінің кіші жүйелерін пайдалану жөніндегі персонал қызметінің мазмұны мен тәртібі; 2. Ақпараттық жүйедегі ақпарат қауіпсіздігіне және бұзушының моделіне негізгі қатерлер; 3. АЖ ақпаратты қорғау үшін пайдаланылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар; 4. АЖ ақпаратын қорғауды қамтамасыз етудің бағдарламалық-аппараттық құралдары; 5. Техникалық арналар бойынша ақпаратты "ағып кетуден" қорғау әдістері; 6. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 1: АЖ-да оларды пайдалану процесінде ақпараттың қорғалуын қамтамасыз ету	Дағды 2: АЖ ақпаратты қорғау жүйелерін әкімшілендіру	Машықтар: 1. АЖ пайдаланушыларының тіркелгілерін жасау, жою және өзгерту; 2. АЖ бағдарламалық құрамдас бөліктерінің қауіпсіздік саясатын жоспарлау; 3. Операциялық жүйелерді, деректер базасын басқару жүйелерін, компьютерлік желілер мен бағдарламалық жүйелерді орнату және баптау; 4. АЖ-да ақпаратты қорғаудың криптографиялық әдістері мен құралдарын пайдалану; 5. АЖ-да ақпаратты қорғауға байланысты оқиғаларды тіркеу және талдау.
		Білімдер: 1. АЖ АҚ саясатын қалыптастыру қағидаттары; 2. АЖ ақпаратын қорғаудың бағдарламалық-аппараттық құралдары; 3. АЖ ақпаратты қорғау үшін пайдаланылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар;

		4. Техникалық арналар бойынша ақпаратты " жылыстаудан" қорғау тиімділігін бақылау әдістері; 5. АЖ бағдарламалық қамтамасыз етуді қорғау құралдарының тиімділігі мен сенімділігін бағалау критерийлері; 6. Ақпаратты қорғау шараларының тиімділігін бақылаудың техникалық құралдары; 7. АЖ бағдарламалық қамтамасыз етуді қорғау жүйелерін ұйымдастыру қағидаттары мен құрылымы; 8. Персоналдың қорғалған автоматтандырылған жүйелерді және АЖ қауіпсіздік жүйелерін пайдалану жөніндегі қызметінің мазмұны мен тәртібі; 9. АЖ-да ақпаратты қорғау жөніндегі негізгі шаралар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: АЖ-да ақпаратты қорғауды басқару	Машықтар: 1. АЖ-дағы ақпараттық тәуекелдерді бағалау; 2. Ақпараттың қауіпсіздігіне төнетін қатерлерді жіктеу және бағалау; 3. Автоматтандырылған жүйелердің қорғалуға жататын ақпараттық ресурстарын анықтау; 4. АЖ ақпаратын қорғауды басқару жүйесін жетілдіру бойынша ұсыныстар әзірлеу; 5. АЖ ақпаратын қорғау жүйесінің параметрлерін конфигурациялау; 6. Ақпаратты қорғау шараларының тиімділігін бақылаудың техникалық құралдарын қолдану.
		Білімдер: 1. Ақпаратты қорғауды басқарудың негізгі әдістері; 2. Ақпараттық қауіпсіздіктің негізгі қатерлері және АЖ-дағы бұзушының модельдері; 3. Ақпаратты техникалық арналар арқылы "ағып кетуден" қорғау әдістері; 4. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер; 5. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1:	Машықтар: 1.Ақпараттық қауіпсіздік қатерлерін жіктеу және бағалау; 2.Техникалық барлауға қарсы іс-қимыл жөніндегі нормативтік құжаттарды қолдану; 3.АЖ ақпаратты қорғау жүйесінің бағдарламалық жасақтамасын баптау параметрлерін анықтау; 4.АЖ-да ақпаратты қорғау бойынша қабылданған шаралардың тиімділігін бақылау.

Еңбек функциясы 2: АЖ-да ақпаратты қорғау жүйелерін енгізу	АЖ-да ақпаратты қорғау жүйелерін енгізу АЖ-да ақпаратты қорғау бойынша ұйымдастырушылық-өкімдік құжаттарды әзірлеу	Білімдер: 1.Қорғалған АЖ және ақпаратты қорғау жүйелерін пайдалану жөніндегі персонал қызметінің мазмұны мен тәртібі; 2.Ақпарат қауіпсіздігінің негізгі қауіптері және АЖ-дағы бұзушы модельдері; 3.АЖ-да ақпаратты қорғау үшін қолданылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар; 4.Техникалық арналар бойынша "ағып кетуден" ақпаратты қорғау құралдарын құру қағидаттары; 5.Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы заңнама.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Енгізу автоматтандырылған жүйелердегі ақпаратты қорғаудың ұйымдастырушылық шаралары	Машықтар: 1. Персоналдың қол жеткізу объектілеріне қол жеткізуін шектеу қағидаларын іске асыру; 2. Ақпаратты қорғау жүйесін жобалау кезінде бағдарламалық және бағдарламалық-аппараттық шешімдерді талдау; 3. ақпаратты қорғауды қамтамасыз ету үшін АЖ персоналын шаралар кешеніне (ережелер, рәсімдер, практикалық тәсілдер, басшылық қағидаттар, әдістер, құралдар) оқыту; 4. Ақпаратты қорғау жөніндегі талаптарды ескере отырып, АЖ персоналының жұмысын жоспарлауды және ұйымдастыруды жүзеге асыру; 5. Аттестатталған АЖ және АЖ ақпаратын қорғау жүйесін конфигурациялау.
		Білімдер: 1. Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы нормативтік құқықтық актілер; 2. Автоматтандырылған жүйелерді қорғау жүйелері мен АЖ әзірлеу кезеңдерінің әдістері, тәсілдері, құралдары, жүйелілігі және мазмұны; 3. Техникалық арналар бойынша ақпаратты "жылыстаудан" қорғаудың техникалық құралдарын ақпарат қауіпсіздігі жөніндегі талаптарға сәйкестігіне сертификаттық сынау әдістемесі; 4. Автоматтандырылған ақпараттық жүйелердің істен шығуға төзімділігін қамтамасыз ету әдістері, тәсілдері мен құралдары.
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Жеке құзыреттерге қойылатын талаптар:	Жауапкершілік Жүйелі ойлау Аналитикалық ойлау Сыни талдау Ұйымдастыру	

	Стандартты емес мәселелерді шеше білу Егжей-тегжейге назар аудару	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ҚР СТ ISO/IEC 27001-2023 " Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар" ҚР СТ ISO/IEC 27006-2017 Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелерінің аудитін және сертификаттауын жүзеге асыратын органдарға қойылатын талаптар ҚР СТ 34.030-2008 ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	7	Ақпаратты қорғау жөніндегі маман

4-ші тарау. Кәсіптік стандарттың техникалық деректері

30. Мемлекеттік органның атауы:

Қазақстан Республикасының Цифрлық даму, инновациядар және аэроғарыш өнеркәсібі министрлігі

Орындаушы:

Советханова Ақжарқын Бақдәулетқызы, +7 (717) 264 94 07, a.sovetkhanova@ mdai.gov.kz

31. Әзірлеуге қатысатын ұйымдар (кәсіпорындар):

Ақпараттық қауіпсіздік комитеті

Жоба жетекшісі:

Қалим Ерболат Теміруұлы

E-mail: e.kalim@mdai.gov.kz

Телефон нөмірі: +7 (717) 264 93 96

Орындаушылар:

Советханова Ақжарқын Бақдәулетқызы, +7 (717) 264 94 07, a.sovetkhanova@ mdai.gov.kz

32. Кәсіптік біліктілік жөніндегі салалық кеңес: 3 , 04.12.2024 г.

33. Кәсіптік біліктілік жөніндегі ұлттық орган: 02.06.2025 г.

34. "Атамекен" Қазақстан Республикасының Ұлттық кәсіпкерлер палатасы: 24.12.2024 г.

35. Нұсқа нөмірі және шығарылған жылы: Нұсқа 1, 2025 г.

36. Болжамды қайта қарау күні: 05.12.2028 г.

© 2012. Қазақстан Республикасы Әділет министрлігінің «Қазақстан Республикасының Заңнама және құқықтық ақпарат институты» ШЖҚ РМК