"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

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

бекітілген бұйрығына
қосымша

Кәсіптік стандарт: "Киберқауіпсіздік саласындағы қызмет"

Ескерту. Стандарт жаңа редакцияда – ҚР Жасанды интеллект және цифрлық даму министрінің м.а. 07.07.2026 № 392/НҚ (алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі) бұйрығымен.

1-ші тарау. Жалпы ережелер

1. Кәсіптік стандарттың қолдану аясы: 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) Жүйелік ойлау – Маманның жеке фактілерді үлкен суретке біріктіру (жалпылау), әртүрлі жағдайларды (экономикалық, саяси, іскерлік) түсіну және ұзақ мерзімді шешімдер қабылдау үшін иерархиялық деңгейлер құру мүмкіндігі. Маңызды қасиет - бір элементтің өзгеруі басқа элементтерге қалай әсер ететінін түсіну

2) Киберқауіпсіздік (бұдан әрі – КҚ) – цифрлық объектілердің құпиялылығын, тұтастығын немесе қолжетімділігін бұзудан қорғалу жай-күйі;

3) Цифрлық технологиялар (бұдан әрі – ЦТ) – Ақпарат пен деректерді жасау, сақтау , беру, манипуляциялау және көрсету үшін қолданылатын аппараттық және бағдарламалық жасақтама.

3. Осы кәсіптік стандартта мынадай қысқартулар қолданылады

1) ААКТА – Ақпараттың ағып кетуінің техникалық арналары;

2) БА – Біліктілік анықтамалықтары;

3) БАҚ – Бағдарламалық-аппараттық құралдар;

4) БҚЕ – Бағдарламалық қамтамасыз ету;

5) БТБА – Бірыңғай тарифтік-біліктілік анықтамалығы;

6) ДД – Дербес деректер;

7) ЕТҚ – Есептеу техникасы құралдары;

8) ЖЭСжК – Жанама электромагниттік сәулелену және кеңестер;

9) ЖШС – Жауапкершілігі шектеулі серіктестік;

10) ЗТБ – Заңды тұлғалар бірлестігі;

11) КЕАҚ – Коммерциялық емес акционерлік қоғам;;
12) КҚ – Киберқауіпсіздік;
13) КРЗ – Қазақстан Республикасының Заңы;
14) МББЖ – Мәліметтер базасын басқару жүйесі
15) НҚА – Нормативтік-құқықтық актілер;
16) НТҚ – Нормативтік-техникалық құжаттама;
17) ОЖ – Операциялық жүйе;
18) РК – Рұқсатсыз кіру;
19) СБШ – Салалық біліктілік шеңбері;
20) ЦЖ – Цифрлық жүйелер;
21) ЦТ – Цифрлық технологиялар;
22) ЭМК – Электрондық медициналық карталар;
23) ACL – Access Control List;
24) API – Application Programming Interface;
25) BASH – Bourne Again Shell;
26) BDA – Battle Damage Assessment;
27) CARVER – Мақсаттарды талдау әдістемесі;
28) COA – Course of Action;
29) DoS – Denial of Service;
30) HIDS – Host Intrusion Detection System;
31) HIPS – Host Intrusion Prevention System;
32) ICS – Industrial Control Systems;
33) IDS – Intrusion detection system
34) IoT – Internet of Things;
35) IPS – Intrusion prevention system;
36) ISO – International Organization for Standardization;
37) JS – JavaScript;
38) KPI – Key Performance Indicators;
39) KRI – Key Risk Indicators;
40) NIDS – Network Intrusion Detection System;
41) NIPS – Network Intrusion Prevention System;
42) SIEM – Security Information and Event Management;
43) SQL – Structured Query Language;
44) SQLi – SQL injection;
45) TLP – Traffic Light Protocol
46) TTPs – Tactics, Techniques, and Procedures
47) VPN – Virtual Private Network
48) XSS – Cross-Site Scripting

2-ші тарау. Кәсіптік стандарттың паспорты

4. Кәсіптік стандарттың атауы: Киберқауіпсіздік саласындағы қызмет

5. Кәсіптік стандарттың коды: J62092101

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

62.09.2 Киберқауіпсіздік саласындағы қызмет

7. Кәсіптік стандарттың қысқаша сипаттамасы: 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.

8. Кәсіптер карточкаларының тізімі:

1) Ақпараттық қауіпсіздік жөніндегі әкімші - 7 СБШ-нің деңгейі;

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

3) Цифрлық технологиялар жөніндегі маман-криминалист - 7 СБШ-нің деңгейі;

4) Ақпаратты қорғау жөніндегі маман - 7 СБШ-нің деңгейі;

5) Ақпараттық қауіпсіздік аудиторы - 7 СБШ-нің деңгейі;

6) Ақпараттық қауіпсіздік жөніндегі маман - 7 СБШ-нің деңгейі;

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

8) Деректерді шифрлаушы - 7 СБШ-нің деңгейі;

9) Ақпаратты қорғау жөніндегі инженер - 7 СБШ-нің деңгейі;

10) Тәуекелдерді басқару менеджері - 6 СБШ-нің деңгейі;

11) Мақсат жасаушы - 6 СБШ-нің деңгейі;

12) Кибероперация операторы - 6 СБШ-нің деңгейі;

13) Кибер-нұсқаушы - 6 СБШ-нің деңгейі;

14) Зерттеу және әзірлеу жөніндегі маман - 6 СБШ-нің деңгейі;

15) IT инвестициялары/портфолио менеджері - 6 СБШ-нің деңгейі;

16) Бағдарлама менеджері - 6 СБШ-нің деңгейі;

17) Қауіптер мен ескертулер талдаушысы - 6 СБШ-нің деңгейі;

18) Желілік операциялар жөніндегі маман - 6 СБШ-нің деңгейі;

19) Кибер операцияларды жоспарлаушы - 6 СБШ-нің деңгейі;

20) Корпоративтік инфрақұрылым сәулетшісі - 6 СБШ-нің деңгейі;

21) Ақпараттық қауіпсіздік жөніндегі маман - 6 СБШ-нің деңгейі;

22) Кибер заң кеңесшісі - 6 СБШ-нің деңгейі;

23) Уәкілетті өкіл/авторландыруға жауапты - 6 СБШ-нің деңгейі;

24) Көлік инфрақұрылымы бойынша ақпараттық қауіпсіздік жөніндегі маман - 6 СБШ-нің деңгейі;

25) Цифрлық технологиялар жөніндегі маман-криминалист - 6 СБШ-нің деңгейі;

26) Білім менеджері - 6 СБШ-нің деңгейі;

27) Құқық қорғау/сот сараптамасы және қарсы барлау талдаушысы - 6 СБШ-нің деңгейі;

28) Деректерді шифрлаушы - 6 СБШ-нің деңгейі;

29) Ақпараттық қауіпсіздік аудиторы - 6 СБШ-нің деңгейі;

30) Сервистердің қауіпсіздігі жөніндегі маман - 6 СБШ-нің деңгейі;

31) Көптілді талдау жөніндегі маман - 6 СБШ-нің деңгейі;

32) Денсаулық сақтау саласындағы ақпараттық қауіпсіздік жөніндегі маманы - 6 СБШ-нің деңгейі;

33) Ақпаратты қорғау жөніндегі инженер - 6 СБШ-нің деңгейі;

34) Ақпаратты қорғау жөніндегі маман - 6 СБШ-нің деңгейі;

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

3-ші тарау. Кәсіптер карточкалары

9. 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: -
	1. Ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі I санатты маман: кадрларды даярлаудың тиісті		

Жұмыс тәжірибесіне қойылатын талаптар:	бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білімі және ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі II санатты маман лауазымында кемінде 2 жыл жұмыс өтілі болуы тиіс	
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттыру бойынша қосымша кәсіби курстар	
Кәсіптің басқа ықтимал атаулары:		
Қызметтің негізгі мақсаты:	Қауіпсіздік тетіктерін әкімшілендіру және КҚ бұзушылықтарына уақтылы ден қою	
Еңбек функциялардың сипаттамасы		
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Ақпаратты қорғау және КҚ -ны қамтамасыз ету БАҚ-тың жұмыс қабілеттілігін басқару, пайдалану және қолдау 2. Қауіпсіздік тетіктерін әкімшілендіру 3. КҚ инциденттеріне ден қою 4. Ақпаратты қорғау және КҚ қамтамасыз ету БАҚ-тарын қолданудың тиімділігін бақылау және талдау
	Қосымша еңбек функциялары:	
	Дағды 1: Есептік құжаттаманы жүргізу	Машықтар: 1. Қауіпсіздік инциденттері бойынша есептерді жасау, оның ішінде оқиғаның сипаттамасын, қауіп-қатерді жою үшін қабылданған шараларды, себептерді талдауды және тергеу нәтижелерін көрсету 2. Қауіпсіздік оқиғалары журналдарын тұрақты түрде жаңарту және жүргізу, оның ішінде қол жеткізу әрекеттері, рұқсатсыз әрекеттер және басқа да оқиғалар туралы ақпаратты енгізу 3. Қауіпсіздік саясаттары мен рәсімдеріне қатысты құжаттаманы жасау және қолдау, оның ішінде қолжетімділік саясаты, деректерді шифрлау және парольдерді пайдалану саясаты 4. Осалдықтар және патч-менеджмент бойынша есептілікті жүргізу және ағымдағы осалдықтар мен патчтар туралы есептерді уақтылы жасау 5. Инциденттерге әрекет ету рәсімдерін құжаттау, оның ішінде қауіп-қатерлерді жою, деректерді қалпына келтіру және залалды азайту бойынша қадамдық нұсқаулықтар
		Білімдер: 1. Киберқауіпсіздік саласындағы есептілікке қойылатын стандарттар мен талаптар 2. Есептілік құрылымы мен форматтарын, оларды жасау тәртібін түсіну 3. Қауіпсіздік деректерін талдау және өңдеу әдістері , қауіпсіздік оқиғалары журналдары мен басқа да дереккөздерден алынған мәліметтерді түсіндіру

		4. Оқиғалар мен инциденттер журналдарын жүргізу қағидаттары, оның ішінде барлық маңызды оқиғаларды тіркеу 5. Қауіпсіздік инфрақұрылымындағы өзгерістер мен инциденттерді басқару қағидаттары мен процестері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Ену әрекеттерін анықтау/ болдырмау жүйесін әкімшілендіру	Машықтар: 1. Ықтимал қауіптерге уақтылы әрекет етуді және киберқауіпсіздік саясаттарын іске асыруды қамтамасыз ете отырып, ену әрекеттерін анықтау және алдын алу жүйелерін (IDS/IPS) қолдану арқылы желі қауіпсіздігін кешенді мониторингтеу 2. Рөлдік қолжетімділік (RBAC) әдістерін қолдана отырып, қолжетімділік құқықтарын қатаң ажыратуды іске асырумен пайдаланушы тіркелгілерін әкімшілендіру, сондай-ақ Zero Trust қағидаттарына сәйкес желілік инфрақұрылымды сегменттеу және трафикті сүзгілеуді жүзеге асыру 3. Парольдердің күрделілік талаптарын, оларды ауыстыру мерзімділігін қамтитын ұйымның парольдік саясатын баптау және сүйемелдеу, сондай-ақ аутентификация ережелері бұзылған жағдайда тіркелгілерді автоматты түрде бұғаттау тетіктерін іске асыру 4. VPN, желілік экрандар, NAT, DHCP, ACL және басқа да компоненттерді баптауды қоса алғанда, желілік қолжетімділік параметрлерін конфигурациялау, желі ресурстарына қауіпсіз және бақыланатын қосылуды қамтамасыз ету 5. IP-адрестер, хосттар және ішкі желілер бойынша критикалық маңызды ресурстарға қолжетімділікті шектеу, шабуыл беткейін азайту және сырттан рұқсатсыз кіруді болдырмау 6. Кәсіпорындық ортада бағдарламалық қамтамасыз етуді жаңарту процесін басқару, оның ішінде тестілеу, жоспарлау және жаңартуларды орталықтандырылған енгізу арқылы IT-инфрақұрылымның қорғалу деңгейі мен тұрақтылығын арттыру
		Білімдер: 1. Ену әрекеттерін анықтау/болдырмау жүйелерінің (IDS/IPS) тағайындалуы, жұмыс істеу қағидаттары, архитектурасы 2. Ену әрекеттерін анықтау жүйелерінің жұмыс істеуін реттейтін стандарттар 3. Ену әрекеттерін анықтау/болдырмау жүйесінің өндірушісінің оны орнату және пайдалану бойынша ұсынымдары 4. Ену әрекеттерін анықтаудың түрлері мен әдістері 5. Ену әрекеттерін болдырмау жүйелерінде қолданылатын технологиялар мен құралдар

Еңбек функциясы 1: Ақпаратты қорғау және АҚ-ны қамтамасыз ету БАҚ-тың жұмыс қабілеттілігін басқару, пайдалану және қолдау	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: Желіаралық экранды теңшеу және баптау	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 4. Оқиғаларды мониторингілеу және журналға түсіру 5. Жаңарту және патчинг жүйесі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ақпаратты қорғау БАҚ-тарын және КҚ қамтамасыз етуді пайдалану 2. Ақпаратты қорғау БАҚ-тарын және КҚ қамтамасыз етуді жеткізушіден және/немесе жұмыс орындаушыдан қабылдап алу 3. Құпия ақпарат тасымалдағыштарын есепке алу және сақтау 4. Құпия ақпаратты қорғау БАҚ-тарын пайдалану 5. Ақпаратты қорғау және КҚ қамтамасыз ету құралдарына техникалық қызмет көрсету бойынша регламенттік және профилактикалық жұмыстарды жүргізу
		Білімдер: 1. Мемлекеттік құпияны және қолжетімділігі шектеулі өзге де ақпаратты қорғау қызметін реттейтін заңнамалық және өзге де нормативтік құқықтық актілер 2. Ақпаратты техникалық қорғауды қамтамасыз ету мәселелері бойынша нормативтік және әдістемелік құжаттар 3. Қорғалуға жататын цифрландыру объектілері

	Дағды 4: Ақпаратты қорғаудың және КҚ қамтамасыз етудің ӨҚБ пайдалану	4. Ұйымның және оның бөлімшелерінің мамандану бағыты мен қызмет бағыттары 5. Қолданылатын ақпараттық технологиялар мен жүйелер 6. Басқару, байланыс, автоматтандыру құрылымы 7. Техникалық барлау құралдары және олардың мүмкіндіктерін бағалау әдістері 8. Киберқауіпсіздік қатерлері және бұзушылықтарды жіктеу (санаттары) 9. Цифрландыру объектілерінің негізгі және қосымша техникалық құралдармен, жүйелермен, кешендермен, ақпаратты техникалық қорғау құралдарымен, сервистермен және автоматтандырылған басқару жүйелерінің қауіпсіздік тетіктерімен жарақтандырылуы 10. Қолжетімділікті шектеу ішкіжүйелері 11. Шабуылдарды анықтау ішкіжүйелері 12. Қасақана әсер етуден қорғау ішкіжүйелері 13. Ақпарат тұтастығын бақылау әдістері, олардың даму және жаңғырту перспективалары 14. Қауіпсіздік жүйелерінің жай-күйін бағалау, ақпараттың ағып кету арналарының анықталуы, сыни есептеу және ақпараттық ресурстарды резервтеу мен дублирлеу процесін бақылау әдістері 15. Ақпаратты қорғаудың техникалық, бағдарламалық, бағдарламалық-аппараттық құралдарымен және бақылау құралдарымен, автоматтандырылған басқару жүйелерінің қауіпсіздік сервистері мен тетіктерімен және олардың жай-күйіне аудит жүргізу тәртібі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ақпараттық ресурстарды уақтылы қорғауды қамтамасыз ете отырып, орталықтандырылған басқару жүйелерін қолдана отырып, антивирустық бағдарламалық қамтамасыз етуді және вирустық деректер базасын қашықтан орнатуды және жаңартуды тиімді жүзеге асыру 2. Барлық IT-инфрақұрылым объектілеріне орталықтандырылған орнату үшін олардың өзектілігі мен қолжетімділігін қамтамасыз ете отырып, желілік серверлерде антивирустық шешімдер дистрибутивтерінің репозиторийлерін ұйымдастыру және қолдау 3. Ұйымның қауіпсіздік саясатына сәйкес қорғаныс деңгейін оңтайландыру арқылы жұмыс станциялары мен серверлерде антивирустық шешімдерді қашықтан реттеңіз 4. Басқару процестерінің тиімділігі мен автоматтандырылуын арттыра отырып, дереу немесе кейінге қалдырылған іске қосу

	Дағды 5: Антивирустық БҚЕ әкімшілендіру	мүмкіндігімен желі құрылғыларында сканерлеуді, жаңартуларды және басқа операцияларды орындауға арналған тапсырмаларды әзірлеу және жоспарлау
		Білімдер: 1. Қауіп-қатерді анықтаудың қолтаңба, эвристикалық, мінез-құлық әдістерін, сондай-ақ проактивті қорғау және басқа киберқауіпсіздік құралдарымен интеграциялау технологияларын қоса алғанда, антивирустық бағдарламалардың мақсаты, жіктелуі және жұмыс принциптері 2. Операциялық жүйелердің, қауіпсіздік саясатының және корпоративтік инфрақұрылымның ерекшеліктерін, сондай-ақ ортаны алдын ала дайындау жөніндегі талаптарды ескере отырып, вирусқа қарсы бағдарламалық жасақтама өндірушілерінің оны дұрыс орнату жөніндегі ресми әдістемелік ұсынымдарын 3. Қауіпсіздік саясатын басқаруды, жаңартуларды автоматтандыруды, есептілікті ұйымдастыруды, инциденттерді мониторингілеуді және қауіп-қатерлерге уақтылы ден қоюды қоса алғанда, оларды баптау, әкімшілендіру және сүйемелдеу бойынша антивирустық шешімдерді әзірлеушілердің ұсынымдарын
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: Әкімшілендіру процестерін басқару	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
		Білімдер: 1. ЦТ процестерін басқарудың өмірлік циклі: жоспарлау, жобалау, енгізу, пайдалану, Қолдау және аяқтау 2. ЦТ қызметтерін басқарудың принциптері мен модельдері 3. Жүйенің жұмыс істеу қаупі жоқ өзгерістер мен конфигурацияларды басқару 4. Әр түрлі құралдардың көмегімен жүйенің жұмысын бақылау және бақылау 5. Қауіпсіздік тәуекелдері мен инциденттерін немесе жүйенің дұрыс жұмыс істемеуін басқару
	Дағдыны тану мүмкіндігі:	Талап етілмейді

Еңбек функциясы 2: Қауіпсіздік тетіктерін әкімшілендіру		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
	Дағды 2: Саясатты орнату ОЖ, ДҚБЖ, ҚБҚ қауіпсіздігі	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
	Дағды 1: АҚ оқиғалары мен инциденттерінің мониторингі	Машықтар: 1. КҚ мониторингіндегі жүйелердегі оқиғаларды жинау және талдау 2. Оқиғаларды, сериялық оқиғаларды және оқиғалар үйлесімін КҚ бұзушылықтары ретінде жіктеу 3. Оқиғаларды өңдеу рәсімдерін теңшеу және КҚ оқиғаларын анықтау
		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. КҚ тосын оқиғасы туралы тіркеу және хабарлау (хабарлау) 2. КҚ тосын оқиғасының себептерін анықтау 3. КҚ тосын оқиғасы мен оның зардаптарын жою шараларын қабылдау 4. Инцидент туралы дәлелдемелер жинауға 5. КҚ 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
Еңбек функциясы 4: Ақпаратты қорғау және КҚ қамтамасыз ету БАҚ-тарын қолданудың тиімділігін бақылау және талдау	Дағды 1: Қорғалатын ақпаратты өңдеудің технологиялық процесін ағымдағы бақылау	Машықтар: 1. Ақпаратты қорғау және КҚ 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 ЦЖ және қорғалатын ақпараттық ресурстарға әрекеттерін анықтау мақсатында жүйелік және қолданбалы БҚ оқиғаларын тіркеу журналдарын талдау
		Білімдер: 1. Бақылауды жүзеге асырудың әдістері, қағидаттары мен тәсілдері 2. КҚ 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. КҚ оқиғалар журналын талдаудың бағдарламалық құралдары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ақпаратты қорғау және КҚ қамтамасыз ету ПАС оқиғаларын тіркеу журналдарын талдау

	Дағды 2: Ақпаратты қорғау және КҚ қамтамасыз ету БАҚ жұмысын ағымдағы және мерзімді бақылау	2. Ақпаратты қорғау және КҚ қамтамасыз ету ПАС ресурстарын пайдалануды бағалау 3. Ақпаратты қорғаудың және КҚ -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 КҚ қамтамасыз ету ПАС ресурстарын пайдалану нәтижелілігінің өлшемдері мен көрсеткіштері 3. Ақпаратты қорғау және КҚ 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:	
	-	-	
10. 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-коммуникациялық технологиялар	Біліктілік: -
	1. Ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі I санатты маман: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білімі және		

Жұмыс тәжірибесіне қойылатын талаптар:	ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі II санатты маман лауазымында кемінде 2 жыл жұмыс өтілі болуы тиіс	
Формалды емес және информалы біліммен байланыс:		
Кәсіптің басқа ықтимал атаулары:		
Қызметтің негізгі мақсаты:	Ақпараттық-коммуникациялық жүйелердің ішкі жүйелеріне, құрылғыларына, элементтері мен арналарына бағдарламалық-техникалық әсердің зиянды әсеріне қарсы іс-қимыл	
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:	
	Дағды 1: Компьютерлік жүйелер мен желілердің қауіпсіздік саясатын қалыптастыру	Машықтар: 1. Қажетті қауіпсіздік пен сенім деңгейін анықтау үшін компьютерлік жүйені талдау 2. Компьютерлік жүйелерді қорғау профильдерін әзірлеу 3. Компьютерлік жүйелердің қауіпсіздігі бойынша тапсырмаларды тұжырымдау 4. Компьютерлік жүйелердің қауіпсіздігіне талдау жасау және ақпаратты қорғау жүйесін пайдалану бойынша ұсыныстар әзірлеу
		Білімдер: 1. Компьютерлік жүйелер мен желілерді құру принциптері 2. Компьютерлік жүйелердің қауіпсіздік модельдері 3. Компьютерлік жүйелер мен желілердің қауіпсіздік саясатының түрлері 4. Ақпаратты криптографиялық қорғау құралдарын құру принциптері 5. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттар 6. Пайдаланылатын және пайдалануға жоспарланған ақпаратты қорғау құралдарының мүмкіндіктері 7. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 8. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс істеу параметрлерін анықтау

Еңбек функциясы 1: Компьютерлік жүйелер мен желілердің қауіпсіздік деңгейін бағалау	Дағды 2: Ақпаратты қорғаудың қолданылатын бағдарламалық-аппараттық құралдарының жұмысқа қабілеттілігі мен тиімділігіне бақылау тексерулерін жүргізу	2. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қорғалуын бағалау әдістемелерін әзірлеу 3. Ақпаратты қорғаудың тиімділігін бағалау 4. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қорғалуын бағалаудың әзірленген әдістемелерін қолдану 5. Олар қамтамасыз ететін қауіпсіздік пен сенім деңгейін анықтау мақсатында бағдарламалық-аппараттық қорғау құралдарын талдау
		Білімдер: 1. Компьютерлік жүйелер мен желілерді құру принциптері 2. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының қауіпсіздігін бағалау әдістері мен әдістемелері 3. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын құру принциптері 4. Компьютерлік жүйелердегі ақпаратты қорғаудың ішкі жүйелерін құру принциптері 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. Ықтимал осалдықтар мен құжатталмаған мүмкіндіктерді іздеу мақсатында бағдарламалық кодты талдау әдістері 8. Қауіпсіздік саясатына сәйкестігі тұрғысынан ақпаратты қорғаудың қолданылатын әдістері мен құралдарын талдау тәсілдері 9. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттар 10. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 11. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Қауіпсіздік пен сенім деңгейін анықтау үшін компьютерлік жүйені талдау 2. киберқауіпсіздік ті бұзушының іс-әрекетін дамытудың ықтимал жолдарын болжау 3. Сәйкестік үшін қауіпсіздік саясатына талдау жасаңыз 4. Операциялық жүйелердегі ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының тиімділігіне мониторинг, талдау және салыстыру жүргізу

	Дағды 3: Компьютерлік жүйелердің қауіпсіздігіне талдау 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 принциптері 2. Компьютерлік жүйелер мен желілердің осалдығы 3. Ақпаратты қорғаудың криптографиялық әдістері 4. Мәліметтер базасын басқару жүйелерін құру принциптері 5. Конфигурацияны талдау құралдары 6. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттар 7. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 8. Ақпаратты қорғау жөніндегі уәкілетті федералды атқарушы органдардың басшылық және әдістемелік құжаттары 9. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: Компьютерлік жүйелер мен желілер ақпаратын қорғаудың бағдарламалық-аппараттық құралдарын жобалау	Машықтар: 1. Ақпаратты қорғауды қамтамасыз ету бойынша неғұрлым орынды практикалық шешімдерді табу мақсатында зерттеулер жүргізу 2. Компьютерлік жүйенің ақпаратты қорғау құралдарын жобалау үшін ақпаратты қорғау саласындағы отандық стандарттарды қолдану 3. Ақпаратты қорғау құралдарының архитектурасы мен интерфейстерін, сәтсіздіктерден кейін қорғаныс құралдары мен жүйелерінің жұмысын қалпына келтіру процедураларын әзірлеу 4. Ақпаратты қорғаудың бағдарламалық және аппараттық құралдары мен тәсілдері бойынша, оның ішінде ағылшын тілінде ғылыми-техникалық әдебиеттерді, әдістемелік материалдарды іріктеу және жинақтау
		Білімдер: 1. Операциялық жүйелерде, мәліметтер базасын басқару жүйелерінде және компьютерлік желілерде ақпаратты алу, өңдеу және беру әдістері мен құралдары 2. Шабуылдардың түрлері және оларды компьютерлік жүйелерде іске асыру тетіктері 3. Компьютерлік желілердегі, операциялық жүйелердегі және дерекқорды басқару жүйелеріндегі ақпаратты қорғау әдістері мен құралдары

Еңбек функциясы 2: Компьютерлік жүйелер мен желілердің қауіпсіздік жүйесін әзірлеу		4. Компьютерлік жүйелердің, оның ішінде антивирустық бағдарламалық қамтамасыз етудің ақпаратты қорғау жүйелерін құру принциптері 5. Компьютерлік жүйелердің қауіпсіздігін талдау әдістері 6. Ақпаратты қорғау құралдарында қолданылатын теориялық-сандық әдістер мен алгоритмдер 7. Қол жеткізуді басқарудың ресми модельдері 8. Бағдарламалық қамтамасыз етуді жобалау принциптері мен әдістері 9. Бағдарламалық қамтамасыз етуді әзірлеу әдістемелері мен технологиялары 10. Киберқауіпсіздік саласындағы Жобаларды басқару принциптері мен әдістері 11. Криптографиялық Алгоритмдер және оларды бағдарламалық қамтамасыз етудің ерекшеліктері 12. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 13. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары 14. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттар
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Компьютерлік жүйелер мен желілердің ақпаратын қорғаудың бағдарламалық-аппаратт	Машықтар: 1. Ақпаратты қорғау саласындағы ғылыми-техникалық әдебиеттерді, нормативтік және әдістемелік материалдарды жинақтау 2. Қауіп модельдерін және компьютерлік жүйелердің қауіпсіздігін бұзушы модельдерін қалыптастыру 3. Компьютерлік жүйенің ақпаратын қорғауды қамтамасыз етудің ең орынды тәсілдерін анықтау 4. Компьютерлік жүйелердің жеке қауіпсіздік саясатын, соның ішінде қол жетімділік пен ақпараттық ағындарды басқару саясатын әзірлеу 5. Компьютерлік жүйенің қауіпсіздігін бағалау үшін ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттарды қолдану 6. Компьютерлік қауіпсіздікті қамтамасыз ету саласындағы қолданыстағы заңнамалық базаны қолдану 7. Киберқауіпсіздік жөніндегі нормативтік және әдістемелік құжаттарды ағылшын тілінде оқу және түсіну 8. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын пайдалану қажеттілігі туралы шешімдер қабылдауды жүзеге асыру
		Білімдер: 1. Ақпаратты қорғау жөніндегі жұмыстарды ұйымдастыру тәртібі

	ық құралдарына қойылатын талаптарды әзірлеу	2. Операциялық жүйелерде, мәліметтер базасын басқару жүйелерінде және компьютерлік желілерде ақпаратты алу, өңдеу және беру әдістері мен құралдары 3. Компьютерлік жүйелердің қауіпсіздігін талдау әдістері 4. Шабуылдардың түрлері және оларды компьютерлік жүйелерде іске асыру тетіктері 5. Ақпараттың ағып кету арналарын анықтау әдістері 6. Компьютерлік желілердегі, операциялық жүйелердегі және дерекқорды басқару жүйелеріндегі ақпаратты қорғау әдістері мен құралдары 7. Ақпаратты қорғау құралдарын компьютерлік жүйелерді құру принциптері 8. Қол жеткізуді басқарудың ресми модельдері 9. Криптографиялық Алгоритмдер және оларды бағдарламалық қамтамасыз етудің ерекшеліктері 10. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 11. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары 12. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық 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. ҚР СТ 34.030-2008 Ақпараттық технологиялар Ақпараттық қауіпсіздік менеджменті жүйелеріне аудит және сертификаттауды жүзеге асыратын органдарға қойылатын талаптар. Ұйымның ақпараттық қауіпсіздігін басқару жүйелерінің аудиті	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	5	Ақпаратты қорғау жөніндегі маман
	6	Ақпаратты қорғау жөніндегі маман
	7	Ақпаратты қорғау жөніндегі маман
11. 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:	1. Ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі I санатты маман: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білімі және ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі II санатты маман лауазымында кемінде 2 жыл жұмыс өтілі болуы тиіс		
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. Цифрлық криминалистика және ақпараттық қауіпсіздік инциденттерін талдау 2. Сандық деректерді талдау	
	Қосымша еңбек функциялары:		
	Дағды 1:	Машықтар: 1. Ұйымдағы ықтимал деректер көздерін анықтау 2. Деректерді жинау жоспарын жасаңыз 3. Деректерді алуды және алынған деректердің тұтастығын тексеруді жүзеге асыру 4. Процесте қолданылатын әрбір құрал туралы ақпаратты қоса алғанда, деректерді жинау үшін журнал жүргізуді жүзеге асыру 5. Белгілі бір дереккөзге жататындығын анықтауға мүмкіндік беретін ақпараттың қасиеттері мен белгілерін бөлектеңіз 6. Бағдарламалық жасақтаманы топтарға бөлу принциптерін анықтаңыз	
		Білімдер: 1. Ықтимал деректер көздерінің түрлері 2. Компьютерлік ақпарат тасымалдаушылар	

Еңбек функциясы 1: Цифрлық криминалистика және киберқауіпсіздік инциденттерін талдау	Әлеуетті ақпарат көздерінен деректерді алу	3. Алынған ақпараттың сақталуын, тұтастығын және құпиялылығын қамтамасыз ету әдістері 4. Ақпарат беру жүйелері мен желілерін құру және жұмыс істеу принциптері 5. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама 6. Есептеу жүйелерінің архитектурасы, құрылысы және жұмыс істеуі 7. Ақпаратты қорғауды қамтамасыз ету үшін қолданылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар 8. Компьютерлік қылмыстардың, құқық бұзушылықтар мен оқиғалардың іздерін іздеу және талдау технологиялары 9. Компьютерлік қылмыстардың, құқық бұзушылықтар мен инциденттердің іздерін тіркеу және құжаттау тәртібі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Компьютерлік қылмыстар кезінде жиналған ақпаратты (тасымалдаушы объектілерді) сараптамалық зерттеу	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: 1. Компьютерлік ақпарат құралдарынан деректерді алу/оқу әдістері 2. Алынған ақпараттың сақталуын, тұтастығын және құпиялылығын қамтамасыз ету әдістері 3. Деректерді зерттеу және сүзу бағдарламалық құралдары 4. Ақпаратты қорғауды қамтамасыз ету үшін қолданылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар 5. Ақпарат беру жүйелері мен желілерін құру және жұмыс істеу принциптері 6. Цифрлық криминалистика саласындағы нормативтік құқықтық актілер 7. Компьютерлік қылмыстардың, құқық бұзушылықтар мен оқиғалардың іздерін іздеу және талдау технологиялары

		8. Компьютерлік қылмыстарды, құқық бұзушылықтар мен инциденттерді тергеп-тексеруді жүргізу әдістері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Сандық деректерді талдау	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 жұмыс істеу принциптері 4. Ақпаратты өңдеудің бағдарламалық құралдары 5. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама 6. Талданатын компьютерлік жүйеде ақпаратты сақтау форматтары 7. Компьютерлік жүйелерде қолданылатын негізгі файл пішімдері 8. Компьютерлік жүйелердегі конфигурациялық және жүйелік ақпаратты сақтау ерекшеліктері 9. Компьютерлік жүйелер мен желілердің осалдығы 10. Компьютерлік қылмыстарды, құқық бұзушылықтар мен инциденттерді тергеп-тексеруді жүргізу әдістері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Ақпаратты ұсынудың заңнамалық талаптарына	Машықтар: 1. Талдау қорытындысы бойынша есепті материалдар жасау 2. Талдау бойынша ақпаратты өзектендіру 3. Компьютерлік инциденттер мен қылмыстардың алдын алу бойынша ұсыныстар әзірлеу
		Білімдер: 1. Алынған ақпараттың сақталуын, тұтастығын және құпиялылығын қамтамасыз ету әдістері 2. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама

	сәйкес талдау және зерттеу нәтижелерін ресімдеу	3. Есептеу жүйелерінің архитектурасы, құрылысы және жұмыс істеуі 4. Ақпарат беру жүйелері мен желілерін құру және жұмыс істеу принциптері 5. Ақпаратты өңдеудің бағдарламалық құралдары 6. Компьютерлік жүйелердің ақпараттық-талдамалық және техникалық сараптамасы бойынша орындалған жұмыстардың нәтижелері бойынша ғылыми-техникалық сараптамалық қорытындылар 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
12. 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:	Басшылар, мамандар және басқа да қызметшілер лауазымдарының біліктілік анықтамалығын бекіту туралы Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрінің 2020 жылғы 30 желтоқсандағы № 553 бұйрығы 3-параграф. Ақпаратты қорғау жөніндегі маманы	
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік Біліктілік: -
	1. 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;	

Жұмыс тәжірибесіне қойылатын талаптар:	2. 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; 3. 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:	Базалық (жоғары) АТ білімі болған кезде киберқауіпсіздік саласында біліктілікті арттырудың қосымша кәсіптік курстары	
Кәсіптің басқа ықтимал атаулары:		
Қызметтің негізгі мақсаты:	ЦЖ ақпаратты қорғау жүйелерін әкімшілендіру	
Еңбек функциялардың сипаттамасы		
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. ЦЖ ақпаратын қорғау жүйелерін әзірлеу 2. Ақпарат пен цифрлық жүйелерді қорғауды қамтамасыз ету
	Қосымша еңбек функциялары:	
	Дағды 1: Киберқауіпсіздік архитектурасын жобалау	Машықтар: 1. Қорғалатын ақпаратты құпия түрлері мен құпиялылық дәрежелері бойынша жіктеу 2. Цифрлық жүйеге талдау жүргізу және қауіпсіздік қатерлерін бағалау 3. Қол жеткізуді басқару әдістерін, қол жеткізу түрлерін және АЖ-да іске асырылуы тиіс қол жеткізу объектілеріне қол жеткізуді шектеу қағидаларын айқындау 4. ЦЖ ақпаратты қорғау жүйесінде іске асыруға жататын ақпаратты қорғау шараларын таңдау 5. Ақпаратты қорғау құралдарының түрлері мен түрлерін анықтау 6. Ақпаратты қорғау жүйесінің архитектурасын әзірлеу
		Білімдер: 1. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама 2. Құру және жұмыс істеу принциптері, заманауи жергілікті және ғаламдық компьютерлік желілерді және олардың компоненттерін іске асырудың мысалдары 3. Технологиялық процестерді басқару ЦЖ - дағы ақпаратты қорғау ерекшеліктері 4. ЦЖ бағдарламалық қамтамасыз ету ақпаратын қорғау құралдарының тиімділігі мен сенімділігін бағалау критерийлері 5. Ақпаратты қорғау жүйелерін ЦЖ бағдарламалық қамтамасыз етуді ұйымдастыру принциптері мен құрылымы 6. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар

		7. ЦЖ -да киберқауіпсіздік саясатын қалыптастыру принциптері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 1: ЦЖ ақпаратын қорғау жүйелерін әзірлеу	Дағды 2: ЦЖ ақпаратын қорғау жүйесіне пайдалану құжаттамасын әзірлеу	Машықтар: 1. ЦЖ -дағы ақпаратты қорғау үшін шараларды (қағидалар, рәсімдер, практикалық тәсілдер, басшылық қағидаттар, әдістер, құралдар) айқындау 2. ЦЖ киберқауіпсіздігінің ішкі жүйелерін құруға техникалық тапсырмалар әзірлеу 3. Қолданыстағы нормативтік және әдістемелік құжаттарды ескере отырып, ақпарат қауіпсіздігінің ішкі жүйелерін жобалау 4. ЦЖ модельдерін және ЦЖ ақпаратын қорғау жүйелерін әзірлеу 5. ЦЖ және қауіпсіздікті қорғау жүйелерінің модельдерін зерттеу 6. ЦЖ компоненттерінің бағдарламалық, архитектуралық-техникалық және схемалық шешімдерін талдау 7. ЦЖ -дағы ақпараттық тәуекелдерді бағалау және қорғалуға жататын ақпараттық инфрақұрылым мен ақпараттық ресурстарды анықтау 8. ЦЖ -да ақпаратты қорғауды қамтамасыз етудің бағдарламалық-аппараттық құралдарының жобалық шешімдерінің техникалық-экономикалық негіздемесін жүргізу 9. ЦЖ -да ақпаратты қорғауды қамтамасыз етудің бағдарламалық-аппараттық құралдарының жобалық шешімдерінің тиімділігін зерттеу 10. Ақпаратты қорғаудың аппараттық және бағдарламалық жүйелерін кешенді тестілеуді және жөндеуді жүргізу
		Білімдер: 1. Киберқауіпсіздікті басқарудың негізгі әдістері 2. Автоматтар теориясының, математикалық логиканың, Алгоритмдер теориясының және графиктер теориясының негізгі ұғымдары 3. Киберқауіпсіздік саласындағы жобаларды басқарудың негізгі әдістері 4. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар 5. АЖ-дағы ақпаратты қорғау жөніндегі негізгі шаралар 6. Технологиялық процестерді басқару ЦЖ - дағы ақпаратты қорғау ерекшеліктері 7. Қауіпсіздікке төнетін қатерлер, ақпараттық әсерлер, қауіпсіздікті бағалау критерийлері және АЖ-дағы ақпаратты қорғау әдістері 8. ЦЖ және ЦЖ ақпаратын қорғау жүйелерін әзірлеу кезеңдерінің әдістері, тәсілдері, құралдары, реттілігі және мазмұны

		9. ЦЖ бағдарламалық қамтамасыз етудегі ақпаратты қорғауды қамтамасыз етудің бағдарламалық-аппараттық құралдары 10. ЦЖ ақпаратын қорғау жүйелерін құрудың негізгі құралдары, тәсілдері мен принциптері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Ақпарат пен цифрлық жүйелерді қорғауды қамтамасыз ету	Дағды 1: ЦЖ ақпаратты қорғау жүйесінің архитектурасын әзірлеу	Машықтар: 1. ЦЖ -дағы киберқауіпсіздікті қамтамасыз ету үшін шаралар кешенін айқындау 2. ЦЖ ақпараттық-технологиялық ресурстарының осалдығын анықтау 3. ЦЖ ақпаратты қорғауды басқару жүйесін жетілдіру жөнінде ұсыныстар әзірлеу 4. ЦЖ құрамында пайдалану үшін ақпараттың қауіпсіздігін қамтамасыз ететін бағдарламалық-аппараттық құралдарды таңдау 5. ЦЖ үшін ақпарат қауіпсіздігіне төнетін қатерлерді жіктеу және бағалау 6. Қорғауға жататын ақпараттық инфрақұрылымды және ЦЖ ақпараттық ресурстарын айқындау 7. ЦЖ -да ақпараттың және бұзушылардың қауіпсіздігіне төнетін қатерлердің үлгілерін әзірлеу 8. Цифрландыру құралдарын қолданудың тиімділігін анықтау
		Білімдер: 1. ЦЖ - да қолданылатын негізгі ақпараттық технологиялар 2. Техникалық арналар бойынша ақпаратты "ағып кетуден" қорғау және ақпаратты қорғау тиімділігін бақылау тәсілдері мен құралдары 3. Киберқауіпсіздігін қамтамасыз етудің негізгі құралдары мен тәсілдері, ақпаратты қорғау жүйелерін құру принциптері 4. ЦЖ ақпаратын қорғауды қамтамасыз етудің бағдарламалық-аппараттық құралдары 5. Техникалық арналар бойынша "ағып кетуден" ақпаратты қорғау құралдарын құру қағидаттары 6. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар 7. Тестілеу және жөндеу әдістері, әзірлеуді құжаттауды ұйымдастыру принциптері, бағдарламалық қамтамасыз етуді сүйемелдеу процесі
	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:	
	6	Ақпаратты қорғау жөніндегі маман	
13. 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:	1. Ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі I санатты маман: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білімі және ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі II санатты маман лауазымында кемінде 2 жыл жұмыс өтілі болуы тиіс		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	АҚ аудитін жоспарлау және бақылау		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. КҚ аудитін жоспарлау 2. КҚ аудитін қамтамасыз ету 3. КҚ аудитін бақылау	
	Қосымша еңбек функциялары:		
		Машықтар:	

Еңбек функциясы 1: АҚ аудитін жоспарлау	Дағды 1: АҚ аудит бөлімшесінің жұмысын жоспарлау	1. КҚ 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 мен техникасы
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Аудиторлық тексеруді жоспарлау	Машықтар: 1. Аудиттің көлемін, ауқымын анықтау 2. Аудитті орындау үшін қажетті ресурстарды анықтаңыз 3. Аудиторлық топ мүшелерін іріктеу (тағайындау) 4. Аудиторлық тапсырмаларды бөлу және оларды орындаудың нақты мерзімдерін белгілеу 5. КҚ аудитін жүргізу жоспары мен бағдарламасын дайындау және келісу
		Білімдер: 1. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама 2. Аудитті жоспарлау әдістемелері, әдістемелері және технологиялары 3. Жобаларды басқару әдістері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: АҚ ұйымдық қамтамасыз ету	Машықтар: 1. КҚ аудиті мәселелері бойынша тексерілетін ұйымның (бөлімшенің) өкілдерімен өзара іс-қимылды ұйымдастыру 2. КҚ аудиторларын оқытуды және олардың біліктілігін арттыруды ұйымдастыру 3. Аудиторлық қызметті басқару
		Білімдер: 1. Іскерлік коммуникацияның кезеңдері мен формалары 2. Іскерлік ортадағы қарым-қатынас принциптері мен ережелері 3. Жұмыс орнында персоналды оқыту мен біліктілігін арттырудың нысандары мен әдістері 4. Персоналды оқыту және біліктілігін арттыру процесінің кезеңдері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Бизнес мақсаттары мен қауіптеріне сәйкес келетін ақпараттық қауіпсіздік стратегиясын қалыптастыру

Еңбек функциясы 2: АҚ аудитін қамтамасыз ету	Дағды 2: Киберқауіпсіздік процестерін стратегиялық басқару және үйлестіру	2. Ақпаратты қорғау процесіне инновациялық технологияларды интеграциялау жөніндегі жоспарларды әзірлеу 3. Ұзақ мерзімді қауіпсіздік қатерлерін бағалау және жауап беру сценарийлерін құру
		Білімдер: 1. Киберқауіпсіздік жөніндегі менеджмент жүйесіне қойылатын негізгі талаптар 2. Киберқауіпсіздік Тәуекелдерін басқару және азайту тәсілдері 3. Киберқауіпсіздік контекстінде тәуекелдерді басқару және оларды азайту принциптері 4. Цифрландыру саласындағы заңнама
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: АҚ аудиті мәселелері бойынша ұйым қызметкерлеріне кеңес беру және нұсқау беру	Машықтар: 1. Тексерілетін ұйымның (бөлімшенің) қызметкерлеріне КҚ аудитіне байланысты мәселелер бойынша консультация беру 2. Аудиторлық топтың қатысушыларына аудиторлық тапсырманы орындауға байланысты шешілмеген күрделі және даулы мәселелер бойынша кеңес беру 3. Тапсырма алдында аудиторлық топқа оның мүшелерінің мақсаттары мен міндеттерін түсіну және түсіну мақсатында нұсқау беру
		Білімдер: 1. Киберқауіпсіздік тәуекелдерін басқарудың ұлттық стандарты 2. Тәуекелдерді бағалау әдістемесі (OCTAVE) 3. Кәсіпорындағы АТ басқару және басқару моделінің сипаттамасы 4. Тәуекелдерді бағалауды және қауіптерді мониторингтеуді жүргізуге арналған технологиялар мен құралдар
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: Аудитордың кәсіби қасиеттерін бақылау	Машықтар: 1. КҚ аудиторларының аудиторлық тапсырмаларды орындау кезінде тәуелсіздік қағидалары мен әдеп қағидаттарын сақтауын бақылау 2. КҚ аудиторларының кәсіби білімі мен сапасын талдау және бағалау 3. Олардың кәсіби дағдыларын жетілдіру үшін КҚ аудиторларымен жұмыс істеу
		Білімдер: 1. Аудит сапасын бақылаудың ұлттық стандарттары 2. КҚ қамтамасыз ету бойынша аудиттің нормативтік-құқықтық актілері 3. КҚ бойынша аудит жүргізу жөніндегі талаптар

Еңбек функциясы 3: АҚ аудитін бақылау	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Аудиторлық тапсырманы бақылау	Машықтар: 1. Аудиторлық тапсырманы орындау мерзімдерін бақылау 2. Аудиторлық тапсырма рәсімдерінің орындалу сапасын бақылау 3. Аудиторлардың аудиторлық қызметті реттейтін ұйымдық-өкімдік құжаттардың сақталуын бақылау
		Білімдер: 1. Бұлтты қызметтердегі дербес деректерді қорғау әдістері 2. Деректерді қорғаудың криптографиялық принциптері мен стандарттары 3. Киберқорғаудың заманауи технологиялары: машиналық оқыту, жасанды интеллект, блокчейн
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: Жүйенің қауіпсіздігін бағалау үшін ену сынақтарын өткізу	Машықтар: 1. Осалдықтарды анықтау мақсатында қауіпсіздік жүйесіне кешенді тексерулер жүргізу 2. Жүйенің қауіпсіздігін бағалау үшін енуді тестілеу (penetration testing) әдістерін қолданыңыз 3. Ақпаратты қорғаудың тиімділігін үнемі қадағалап отыру 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
14. 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:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:	1. Ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі I санатты маман: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білімі және ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі II санатты маман лауазымында кемінде 2 жыл жұмыс өтілі болуы тиіс		
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:	Ұйымның КҚ басқару және қамтамасыз ету процесін бақылау		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. КҚ қамтамасыз ету процестерін үйлестіру 2. КҚ басқару және қамтамасыз ету жөніндегі іс-шараларды талдау және бақылау	
	Қосымша еңбек функциялары:		
	Дағды 1: Ұйымның КҚ басқару және қамтамасыз ету процестерін жоспарлау	Машықтар: 1. КҚ қамтамасыз ету процестерін реттейтін ҒТҚ-ның ағымдағы деңгейін бағалау 2. КҚ қамтамасыз ету процестерін реттейтін ТҚ әзірлеу (өзектендіру) 3. Цифрлық инфрақұрылымның ЦЖ және компоненттері үшін қорғау бейіндері мен қауіпсіздік жөніндегі тапсырмаларды әзірлеу	
		Білімдер: 1. Ұйымның бағдарламалық және аппараттық құралдарының қорғаныс механизмдерінің принциптері	

Еңбек функциясы 1: ҚҚ қамтамасыз ету процестерін үйлестіру		2. ҚҚ қамтамасыз ету саласындағы ғылыми зерттеулер 3. ЦЖ жобалау принциптері мен әдістемесі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: ҚҚ қамтамасыз ету саласында міндеттерді қою және олардың орындалуын бақылау	Машықтар: 1. ҚҚ басқару процестерінің ТҚ саясатын және ҚҚ қамтамасыз ету процестерін реттейтін құжаттарды әзірлеу (өзектендіру) жөніндегі қызметті үйлестіру 2. Ұйымның бекітілген (өзектендірілген) ҚҚ саясатын қызметкерлердің назарына жариялау және жеткізу 3. Ұйым қызметкерлерімен, мердігерлермен және үшінші тараптармен құпиялылық немесе ақпаратты жарияламау туралы келісімдерді әзірлеуге қатысу
		Білімдер: 1. Бизнес-процестерді реттеудің негізгі принциптері 2. ҚҚ қамтамасыз ету саласындағы заңнама 3. ҚҚ қамтамасыз ету саласындағы ұлттық стандарттар
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: ҚҚ басқару және қамтамасыз ету жөніндегі іс-шараларды талдау және бақылау	Дағды 1: Ұйымның ҚҚ қамтамасыз ету жөніндегі іс-шаралар жоспарын дайындау	Машықтар: 1. Ақпаратты автоматтандырылған өңдеумен байланысты бизнес - процестер мен активтердің қорғалуын талдау 2. ҚҚ қамтамасыз ету құралдары мен әдістерін таңдаңыз 3. Ұйымның ҚҚ саясатын іске асыруға бағытталған іс-шараларды әзірлеу 4. ҚҚ инциденттері мен форс-мажорлық жағдайлардан кейін бизнестің үздіксіздігін және қалпына келтіруді қамтамасыз ету бойынша жоспар құру
		Білімдер: 1. ҚҚ қамтамасыз ету құралдары мен құралдарының отандық және шетелдік нарығын дамытудың негізгі тенденциялары 2. Ақпараттың ағып кету арналарын анықтау және бұғаттау принциптері мен әдістері 3. ҒТҚ және ақпаратты өңдеуге байланысты активтерді жіктеу, есепке алу және таңбалау әдістері 4. Бизнес-процестердің үздіксіздігін қамтамасыз ету саласындағы ҒТҚ
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. ҚҚ қамтамасыз етудің сатып алынатын құралдарына техникалық ерекшеліктерді, тендерлік құжаттаманы әзірлеу

	Дағды 2: Жабдықтарды, бағдарламалық құралдар мен жүйелерді (кіші жүйелерді) сатып алуды жүзеге асыру үшін техникалық құжаттаманы дайындау	2. ЦЖ КҚ ішкі жүйелеріне қойылатын талаптарды, техникалық шарттарды әзірлеу 3. Ақпараттық-коммуникациялық инфрақұрылымның цифрлық жүйелері мен компоненттері үшін қауіпсіздік профильдері мен қауіпсіздік тапсырмаларын әзірлеу бойынша жұмыстарды ұйымдастыру және үйлестіру	
		Білімдер: 1. Сатып алынатын КҚ қамтамасыз ету құралдарына техникалық ерекшеліктерді, тендерлік құжаттаманы әзірлеу 2. ЦЖ КҚ ішкі жүйелеріне қойылатын талаптарды, техникалық тапсырмаларды әзірлеу 3. Ақпараттық-коммуникациялық инфрақұрылымның ЦЖ және компоненттері үшін қорғаныс бейіндерін және қауіпсіздік жөніндегі тапсырмаларды әзірлеу жөніндегі жұмыстарды ұйымдастыру және үйлестіру	
	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	
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:	7		
СБШ бойынша біліктілік ішкі деңгейі:	-		
БТБА, БА, үлгілік біліктілік сипаттамалары бойынша біліктілік деңгейі:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -

	магистратура, резидентура)		
Жұмыс тәжірибесіне қойылатын талаптар:	1. Ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі I санатты маман: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білімі және ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі II санатты маман лауазымында кемінде 2 жыл жұмыс өтілі болуы тиіс		
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 осалдықтарын іздеу және анықтау		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Сервистерді жобалау және енгізу кезіндегі қауіпсіздік тәуекелдерін бағалау және талдау 2. Киберқауіпсіздікке байланысты жаңа функционал бойынша кеңесші және тапсырыс беруші ретінде әрекет ету	
	Қосымша еңбек функциялары:		
Еңбек функциясы 1: Сервистерді жобалау және енгізу кезіндегі қауіпсіздік тәуекелдерін бағалау және талдау	Дағды 1: Осалдықтарға тестілеу жүргізу	Машықтар: 1. Осалдықты сканерлеу құралдарын қолданыңыз 2. Шабуылдарды анықтау үшін журналдар мен желілік трафикті талдаңыз 3. Деректер базасында және арнайы ресурстарда осалдықтар туралы ақпаратты іздеңіз 4. Осалдықтардың маңыздылығын анықтаңыз және олардың жүйенің қауіпсіздігіне әсерін бағалаңыз 5. Осалдықтарды жою бойынша есептер мен ұсыныстар дайындаңыз	
		Білімдер: 1. Шабуылдардың негізгі түрлерін түсіну 2. Осалдықтарды бағалау әдістемелері 3. Оқиғаларды логтау және талдау-SIEM жүйелерімен жұмыс 4. Қызметтердің хаттамалары мен архитектурасы 5. Бағдарламалау тілдері (Python, Bash, PowerShell, JS, SQL) 6. Қоғамдық осалдық базаларымен жұмыс	
	Дағдыны тану мүмкіндігі:	Талап етілмейді	
		Машықтар: 1. Әзірлеушілер мен әкімшілерге осалдықтарды жою бойынша нақты міндеттерді тұжырымдау 2. Түзетулерді қайта тестілеу жолымен тексеруге	

	Дағды 2: Сервистерге байланысты КҚ инциденттеріне мониторинг және ден қою	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)
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: Киберқауіпсіздікке байланысты жаңа функционал бойынша кеңесші және тапсырыс беруші ретінде әрекет ету	Дағды 1: Инциденттерді тергеуге және олардың алдын алу шараларын әзірлеуге қатысу	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. Киберқауіпсіздікке төнген қатерлер тұрғысынан жарияланымның ықтимал салдарын бағалау 6. Сервиске бағытталған дезинформациялық шабуылдарды анықтау және болдырмау
		Білімдер: 1. Киберқауіпсіздік 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: Аудитті ұйымдастыру және өткізу	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	
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	Сервистердің қауіпсіздігі жөніндегі маман
16. 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:	1. Ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі I санатты маман: кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білімі және ақпараттық инфрақұрылымның негізгі жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі II санатты маман лауазымында кемінде 2 жыл жұмыс өтілі болуы тиіс		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда ЦТ 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-аппараттық жүйелерін әзірлеу 2. Киберқауіпсіздік регламенттері мен талаптарына сәйкес деректерді шифрлауды және таратып жазуды жүргізу	
	Қосымша еңбек функциялары:		
	Дағды 1: Деректерді шифрлау жүйелеріне арналған жобалық шешімдерді әзірлеу	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 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. Киберқауіпсіздікті 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. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 1: Деректерді шифрлаудың бағдарламалық-аппараттық жүйелерін әзірлеу	Дағды 2: Деректерді шифрлаудың бағдарламалық, бағдарламалық-аппараттық жүйелерін іске асыру	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 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
Еңбек функциясы 2: Киберқауіпсіздік регламенттері мен талаптарына сәйкес деректерді шифрлауды	Дағды 1: 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 КҚ 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

және таратып жазуды жүргізу		6. Тестілік деректер жиынтығын, криптографиялық алгоритмдерді сақтау құрылымдары мен форматтары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Әзірленген деректерді шифрлау 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:	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. Талапта" 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	
17. 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:	Басшылар, мамандар және басқа да қызметшілер лауазымдарының біліктілік анықтамалығын бекіту туралы Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрінің 2020 жылғы 30 желтоқсандағы № 553 бұйрығы 2-параграф. Ақпаратты қорғау жөніндегі инженер		
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары оқу орнынан кейінгі білім (магистратура, резидентура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:	Кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білім, жұмыс өтіліне талаптар қойылмайды немесе тиісті мамандық (біліктілік) бойынша техникалық және кәсіптік, орта білімнен кейінгі (арнайы орта, кәсіптік орта) білім және I санатты ақпаратты қорғау жөніндегі техник лауазымында кемінде 3 жыл жұмыс өтілі.		
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:	Қолданбалы және жүйелік бағдарламалық қамтамасыз етудің ақпаратты қорғау құралдарымен жұмыс істеуін 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. Пайдалану барысында ақпаратты қорғау жүйесін сүйемелдеу	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Арнайы техникалық және технологиялық жабдықтарды жобалау және енгізу бойынша жұмыстарды орындайды. ақпаратты қорғаудың бағдарламалық-математикалық құралдары, цифрлық жүйелерді қорғаудың ұйымдастырушылық және техникалық шараларын қамтамасыз ету	

	Дағды 1: Нормативтік реттеу, қатерлер, ақпаратты қорғаудың әдістері мен құралдары	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 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 тәртібі жөніндегі нұсқаулықтардың талаптарын сақтай отырып орындау
Еңбек функциясы 1: Ұйымда ақпаратты қорғау жүйесін құру		Білімдер: 1. Ақпаратты техникалық қорғауды қамтамасыз етуге байланысты мәселелер бойынша заңнамалық, өзге де нормативтік құқықтық актілер мен әдістемелік материалдар 2. Ұйымның мамандануы және оның қызметінің ерекшеліктері 3. Ақпаратты алу, өңдеу және беру әдістері мен құралдары 4. Ақпаратты қорғауды техникалық қамтамасыз ету жөніндегі ғылыми-техникалық және өзге де арнаулы әдебиеттер 5. Ақпаратты қорғаудың техникалық құралдары, Ақпаратты қорғаудың бағдарламалық-математикалық құралдары 6. Ақпаратты қорғау жөніндегі техникалық құжаттаманы ресімдеу тәртібі 7. Ақпараттың ағып кетуі мүмкін арналар 8. Ақпаратты талдау және қорғау әдістері 9. Ақпаратты қорғау жөніндегі жұмыстарды ұйымдастыру 10. Арнайы жұмыстарды жүргізу режимін сақтау жөніндегі нұсқаулықтар 11. Техникалық барлау және ақпаратты қорғау саласындағы отандық және шетелдік тәжірибе 12. Экономика, өндірісті ұйымдастыру, Еңбек және басқару негіздері 13. Еңбек заңнамасы, ішкі еңбек тәртібінің тәртібі, еңбек қауіпсіздігі және еңбекті қорғау, өндірістік санитария, өрт қауіпсіздігі талаптары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. КҚ қамтамасыз ету құралдарының ағымдағы жағдайын бағалау

	Дағды 2: Қол жетімділігі шектеулі ақпаратты өңдеудің техникалық құралдарының мақсаты, функциялары, жұмыс істеу шарттары туралы деректерді талдау	2. Ақпаратты өңдеуге (талқылауға, беруге, сақтауға) персоналдың қатысу дәрежесін айқындау 3. Негізгі техникалық құралдар мен жүйелердің мақсаты, функциялары, жұмыс істеу шарттары туралы деректерді талдау
		Білімдер: 1. КҚ техникалық құралдарының негізгі параметрлері 2. Ақпаратты қорғау жүйесіне арналған пайдалану құжаттамасы 3. Ақпараттың түрлері, санаттары, түрлері және градация (санаттау) деңгейлері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: Ұйымдағы ақпараттың қауіпсіздігіне төнетін қатерлер моделін әзірлеу	Машықтар: 1. Ұйымдағы киберқауіпсіздікке төнетін қатерлердің модельдерін әзірлеу 2. Қатерлер моделін әзірлеудің бағдарламалық құралдарын пайдалану 3. Ұйымда ақпаратты қорғау жүйесін құру қажеттілігінің аналитикалық негіздемесін әзірлеу 4. Техникалық тапсырмаға сәйкес объектінің киберқауіпсіздігін 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 тапсырманы әзірлеу	Машықтар: 1. Цифрландыру 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
Еңбек функциясы 2: Ұйымда ақпаратты қорғау жүйесін пайдалануға беру	Дағды 1: Ақпаратты қорғау жүйесін пайдалануға беру	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
	Дағды 2: Ақпаратты қорғау жүйесінің тиімділігін қамтамасыз ететін ұйымдастыру шараларын әзірлеу және іске асыру	Машықтар: 1. Қол жетімділігі 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 баптау 3. Ұйымдастырушылық-өкімдік құжаттарды әзірлеу
		Білімдер: 1. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама 2. Ақпаратты қорғау әдістері, құралдары және жүйелері 3. Ақпаратты қорғаудың техникалық құралдарының архитектурасы
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: Ақпаратты техникалық қорғау мәселелері бойынша басшы құрамға нұсқама беруді және персоналды оқытуды ұйымдастыру	Машықтар: 1. Персоналды ақпаратты қорғаудың техникалық, бағдарламалық (бағдарламалық-техникалық) құралдарын пайдалануға оқытуды ұйымдастыру 2. Ақпаратты техникалық қорғау мәселелері бойынша нұсқама жүргізу 3. Қызметкерлермен сабақ өткізу
		Білімдер: 1. Ұйымдастырушылық-өкімдік құжаттар 2. Персоналға нұсқау беру әдістемесі 3. Оқу сабақтарын өткізу қағидалары
	Дағдыны тану мүмкіндігі:	Талап етілмейді

	Дағды 4: Ақпаратты қорғау жүйесін тәжірибелік пайдалануды және пысықтауды ұйымдастыру	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
Еңбек функциясы 3: Пайдалану барысында ақпаратты қорғау жүйесін 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 күйін бақылау 3. Ақпаратты техникалық қорғау бойынша ұйымдастырушылық және техникалық іс-шараларды жетілдіру бойынша ұсыныстар әзірлеуді басқару 4. Ұйымдағы ақпаратты техникалық қорғау жүйесін жетілдіру және тиімділігін бағалау
		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: Цифрландыру жүйелерін техникалық қызмет көрсету және пайдаланудан шығару және олардың элементтерін кәдеге жарату жөніндегі іс шараларды ұйымдастыру	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 ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
	6	Ақпаратты қорғау жөніндегі инженер

18. Кәсіптің карточкасы "Тәуекелдерді басқару менеджері":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-026		
Кәсіптің атауы:	Тәуекелдерді басқару менеджері		
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) басқару білімі бар киберқауіпсіздік саласындағы кәсіби біліктілікті арттырудың қосымша бағдарламалары		
Кәсіптің басқа ықтимал атаулары:	1229-0-002 - Риск-менеджмент жөніндегі басшы		
Қызметтің негізгі мақсаты:	Киберқауіпсіздік тәуекелдерін анықтайды, бағалайды және азайтады		
Еңбек функциялардың сипаттамасы			
	Міндетті еңбек функциялары:	1. КҚ қамтамасыз ету және деректермен жұмыс 2. Киберқауіпсіздік саласындағы тәуекелдерді сәйкестендіру	

Еңбек функцияларының тізбесі:		3. Киберқауіпсіздік саласындағы тәуекелдерді бағалау
	Қосымша еңбек функциялары:	1. Киберқауіпсіздік саласындағы тәуекелдерді азайту
Еңбек функциясы 1: АҚ қамтамасыз ету және деректермен жұмыс	Дағды 1: Киберқауіпсіздікті кешенді қамтамасыз ету және қорғалған жүйелерді басқару	Машықтар: 1. Артефактілерді, журналдарды, жад қоқыстарын, жүйелік іздерді жинау және талдау 2. Құпия сөз саясатын, қауіпсіздік топтарын, көп факторлы аутентификацияны басқарыңыз 3. Топтық саясатты, пайдаланушы құқықтарын, брандмауэр ережелерін қолданыңыз 4. КҚ жүйелеріне аудит және тестілеу жүргізу
		Білімдер: 1. Цифрлық жүйелерді басқару және қорғау негіздері 2. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары 3. Қауіпсіздік жүйелерін талдау, аудит және тестілеу принциптері 4. Бағдарламалау тілдері
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 2: Киберқауіпсіздік оқиғаларының деректерін талдау және өңдеу	Машықтар: 1. Киберқауіпсіздік оқиғаларын анықтау және жіктеу 2. Оқиғалар журналдарын, желілік трафикті және басқа деректер көздерін талдаңыз 3. Оқиғаларды талдау нәтижелері бойынша есептер мен ұсынымдар қалыптастыру 4. Арнайы құралдарды қолданыңыз (SIEM, IDS / IPS , forensic-құралдар)
		Білімдер: 1. Киберқауіпсіздік оқиғаларын жіктеу негіздері және олардың ерекшеліктері 2. КҚ оқиғалары туралы деректерді жинау және корреляциялау әдістері 3. Инциденттерді тергеу және цифрлық криминалистика негіздері 4. КҚ инциденттерін тіркеуге және өңдеуге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 1:	Машықтар: 1. Осалдықтарды анықтау үшін жүйелер мен процестерге аудит жүргізу 2. Желілік трафиктегі ауытқуларды анықтау үшін бақылау құралдарын пайдаланыңыз 3. Тәуекелдер туралы деректерді жинау үшін қызметкерлер мен мүдделі тараптардан сұхбат алыңыз

Еңбек функциясы 2: Киберқауіпсіздік саласындағы тәуекелдерді сәйкестендіру	Ықтимал қауіптер туралы ақпаратты жинау және талдау	4. Тәуекелдер тізілімінде анықталған қауіптерді құжаттау
		Білімдер: 1. Киберқауіптердің негізгі түрлері (вирустар, фишинг, DDoS-шабуылдар) 2. Осалдықты талдау әдістері (CVSS, OWASP) 3. ҚР мен әлемдегі киберқауіпсіздікке қойылатын нормативтік талаптар 4. Осалдықтарды сканерлеу құралдары (Nessus, OpenVAS)
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Тәуекелдерді жіктеу және сұрыптау	Машықтар: 1. Әсер ету деңгейлері бойынша тәуекелдерді санаттау 2. Ықтималдық пен салдарды бағалау үшін тәуекел матрицаларын қолданыңыз 3. Сыртқы деректерді КҚ тәуекелдерін талдауға біріктіру 4. Жаңа деректер негізінде тәуекелдер тізілімін жаңарту
		Білімдер: 1. Тәуекелдерді жіктеу модельдері 2. Активтердің іскерлік сынына әсер ететін факторлар 3. Қауіптер туралы ақпарат көздері 4. Тәуекелдерді үздіксіз бақылау принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Киберқауіпсіздік саласындағы тәуекелдерді бағалау	Дағды 1: Тәуекелдерді сандық және сапалық бағалау	Машықтар: 1. Тәуекелдерден күтілетін шығындарды есептеңіз 2. Қауіптердің салдарын модельдеу үшін сценарийлік талдау жүргізу 3. Қолданыстағы бақылау шараларының тиімділігін бағалау 4. Ұсыныстармен есептер қалыптастыру
		Білімдер: 1. Сандық бағалау әдістері 2. Сапалы тәсілдер 3. Тәуекелдерді бағалау стандарттары (NIST SP 800-30, FAIR) 4. Тәуекелдердің экономикалық аспектілері
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Тәуекелдерді бағалауды басқа бөлімдермен үйлестіру 2. Ену тестілеу жоспарларын әзірлеу (pentesting)

	Дағды 2: Тәуекелдерді бағалауды бизнес-процестерге біріктіру	3. Тәуекелдердің бизнес мақсаттарына әсерін талдау 4. Тәуекелдерді бағалаудағы өзгерістерді бақылау
		Білімдер: 1. SDLC (Secure Software Development Lifecycle) тәуекелдерді басқару интеграциясы 2. Бағалаудағы мүдделі тараптардың рөлдері 3. Тәуекелдерді модельдеуге арналған құралдар 4. Бағалау үшін реттеуші негіздер
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Киберқауіпсіздік саласындағы тәуекелдерді азайту	Дағды 1: Тәуекелдерді азайту жөніндегі шараларды әзірлеу	Машықтар: 1. Тәуекелдерді азайту стратегияларын жобалау 2. КҚ саласында тәуекелдерді азайтудың техникалық шараларын енгізу 3. Қызметкерлерді киберқауіпсіздік мәселелері бойынша оқыту 4. Енгізілген шаралардың тиімділігін бағалау
		Білімдер: 1. КҚ тәуекелдерін азайту стратегиялары 2. Техникалық қарсы шаралар 3. Хабардарлықты арттыру бағдарламалары 4. Тиімділік көрсеткіштері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Мақсаткерлік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар ISO/IEC 27005: 2018 — Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік тәуекелдерін басқару (information security risk management) ISO 31000: 2018- Тәуекелдерді басқару. Принциптер мен нұсқаулық (тәуекелдерді басқару) ISO/ IEC 27001 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. АҚ менеджментімен байланыс ISO/IEC 27002 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Бақылау шаралары (практика кодексі) ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 27005-2013 ("Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік тәуекелін басқару") ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:

19. Кәсіптің карточкасы "Мақсат жасаушы":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-024		
Кәсіптің атауы:	Мақсат жасаушы		
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы базалық (жоғары) білімі бар киберқауіпсіздік және кибер барлау саласындағы біліктілікті арттырудың қосымша бағдарламалары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Мақсатты талдау жүргізеді және киберкеңістік операцияларының жоспарларын әзірлейді		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Киберкеңістіктегі мақсаттарды талдау және таңдау 2. Таргетингтік пакеттерді әзірлеу 3. Кибер операцияларды жоспарлауға және жүргізуге қолдау көрсету	
	Қосымша еңбек функциялары:	1. Жүргізілген кибер операцияның тиімділігін бағалау	
	Дағды 1:	Машықтар: 1. Мақсатты желі топологиясын құру және маңызды түйіндерді анықтау 2. Мақсаттың аппараттық және бағдарламалық жасақтамасын анықтау (ОЖ нұсқалары, ДҚБЖ, веб-серверлер және т.б.) 3. Осалдықтарды және ықтимал шабуыл векторларын анықтау 4. Мақсатты активтердің маңыздылығын бағалау	
		Білімдер: 1. Мақсатты жүйені және жоюдың кибер тізбегін талдау әдістемелері 2. Осалдық деректер базасы және оларды пайдалану	

Еңбек функциясы 1: Киберкеңістіктегі мақсаттарды талдау және таңдау	Желілік карта мен мақсатты профильді құру	3. Киберкеңістіктегі активтердің сыни деңгейін бағалау принциптері 4. Желілік визуализация құралдары барлаумен бірге
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 2: Мақсат туралы барлау ақпаратын жинау және өңдеу	Машықтар: 1. Нысананың желілік инфрақұрылымында OSINT және HUMINT жүргізу 2. Арнайы құралдарды пайдаланып пассивті және белсенді барлауды орындау 3. Нысанаға алынған деректерді құрылымдау және тексеру 4. Белгіленген форматта барлау есептерін дайындау
		Білімдер: 1. OSINT және HUMINT әдістері мен құралдары 2. Желілік хаттамалар мен корпоративтік желі архитектурасының принциптері 3. Барлау жүргізу кезіндегі операциялық қауіпсіздік негіздері 4. Желіде және нақты ортада анықтауға қарсы әрекет ету әдістері
	Дағдыны тану мүмкіндігі:	Қажет
Еңбек функциясы 2: Таргетингтік пакеттерді әзірлеу	Дағды 1: Мақсаттардың номенклатурасын қалыптастыру және таңдауды негіздеу	Машықтар: 1. Стратегиялық, операциялық және тактикалық маңыздылығына қарай мақсаттың басымдылығын анықтау 2. CARVER моделін немесе соған ұқсасты пайдалана отырып, мақсатты таңдауды негіздеу 3. Мақсатты белгілеу пакетін жоғары басшылықпен үйлестіру 4. Әзірленген мақсаттар бойынша презентациялар мен брифингтерді дайындау
		Білімдер: 1. CARVER матрицалары және мақсатты басымдықты анықтаудың басқа әдістері 2. Кибер операциялардың әсер ету принциптері 3. Мақсатты белгілеу пакетін жобалауға қойылатын талаптар 4. Киберкеңістікте күштерді қолдану бойынша әскери доктрина негіздері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2:	Машықтар: 1. Мақсаттың электрондық дерекқорын жасау 2. Осалдық уақыт терезелерін, тәуелділіктерді және байланысты тәуекелдерді деректемеге қосу 3. Ықтимал қол жеткізу жолдары мен пайдалану кезеңдерін модельдеу

	Егжей-тегжейлі мақсатты құжаттаманы әзірлеу	4. Жаңа барлау қол жетімді болған кезде деректі нақты уақытта жаңарту
		Білімдер: 1. Ақпаратты бөлісу стандарттары 2. Шабуылдарды модельдеу принциптері 3. Киберкепіл залалын бағалау әдістері 4. Ынтымақтастық құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Кибер операцияларды жоспарлауға және жүргізуге қолдау көрсету	Дағды 1: Іс-әрекет курстарын әзірлеуге қатысу	Машықтар: 1. Әзірленген мақсаттарға негізделген техникалық түрде орындалатын әрекет бағыттарын (ҚҚ) ұсыныңыз 2. Тәуекелдер мен әр әрекет бағытының табысты болу ықтималдығын бағалаңыз (ӘБ) 3. Кибер симуляторда соғыс ойындары мен жаттығуларына қатысыңыз 4. Таңдалған іс-әрекет бағытына (ҚҚ) мақсаттарды реттеңіз
		Білімдер: 1. Киберкеңістіктегі операцияларды жоспарлау процесі 2. Әрекет ету нұсқаларын талдау және салыстыру әдістемелері (ҚБ) 3. Кибер операциялардағы синхрондау матрицасының принциптері 4. Кибер қақтығыстардағы ойын теориясының негіздері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Нақты уақыттағы мақсатты белгілеуді қамтамасыз ету	Машықтар: 1. Операция кезінде мақсаттың күйін бақылаңыз 2. Инфрақұрылым өзгерген кезде қол жеткізу параметрлерін жылдам реттеңіз 3. Жаңартылған деректерді операцияларға/қатынау топтарына тасымалдау 4. Қол жеткізілген әсерлер мен қалдық осалдықтарды жазу
		Білімдер: 1. Киберопераціялардағы басқару және басқару принциптері 2. Нақты уақыт режимінде мақсатты белгілеуді беру хаттамалары мен форматтары 3. Кибер операциялардың әсерін өлшеу әдістері 4. Бірыңғай кибер операциялық ортаның құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Енгізілетін құрылғыларды пайдаланудан телеметрия мен журналдарды жинау

Қосымша еңбек функциясы 1: Жүргізілген кибер операцияның тиімділігін бағалау	Дағды 1: Кибер операцияның қол жеткізілген нәтижелері туралы мәліметтерді жинау және талдау	2. Қажетті нәтижелерге қол жеткізу дәрежесін бағалау 3. Нәтижелерге қол жеткізбеу себептерін анықтау 4. Киберзиянды бағалау (BDA) есептерін дайындау
		Білімдер: 1. Зиянды бағалау әдістемелері (BDA) және қайта шабуылдар бойынша ұсыныстар 2. Киберкеңістікте шабуыл нәтижелеріне қол жеткізу көрсеткіштері 3. Трафик пен журналды талдауға арналған құралдар 4. Кибер операцияларда алынған сабақтардың принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Тез шешім қабылдай білу Командада жұмыс істей білу Мақсаткерлік Тәртіптілік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 15408 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері ISO/IEC 27002 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары (практика кодексі) ISO/IEC 27033-Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Желінің қауіпсіздігі ISO/IEC 27005 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік тәуекелдерін басқару ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO / IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ 1073-2025 ("Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар") ҚР СТ 4009-2025 ("Ақпараттық технологиялар. Ақпаратты криптографиялық қорғау. Блоктық симметриялық шифрлау алгоритмі")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
20. Кәсіптің карточкасы "Киберопераций операторы":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-033	
Кәсіптің атауы:	Киберопераций операторы	

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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласында базалық (жоғары) білімі болған кезде киберқауіпсіздік және кибероперациялар саласындағы қосымша кәсіби біліктілікті арттыру бағдарламалары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Осалдықтарды анықтайтын және қауіптерді бейтараптандыратын шабуыл және қорғаныс кибершабуылдарын жүргізеді		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Цифрлық жүйелердегі осалдықтарды анықтау 2. Қорғаныс кибероперацияларын жүргізу 3. Шабуыл кибероперацияларын жүргізу	
	Қосымша еңбек функциялары:	1. Жүргізілген кибероперацияның тиімділігін бағалау	
Еңбек функциясы 1: Цифрлық жүйелердегі осалдықтарды анықтау	Дағды 1: Ену тестілеуі және осалдықтарды пайдалану	Машықтар: 1. Арнайы құралдарды пайдаланып осалдықтарды сканерлеуді орындаңыз 2. Қол жеткізу үшін анықталған осалдықтарды пайдалану 3. Компаның тереңдігін бағалау үшін пайдаланудан кейінгі жұмыстарды жүргізу 4. Анықталған осалдықтардың тәуекел деңгейін бағалау	
		Білімдер: 1. Осалдықтар туралы мәліметтер базасы 2. Ену тестілеу құралдары 3. Пентест кезеңдері 4. Осалдықтарды бағалау әдістері	
	Дағдыны тану мүмкіндігі:	Қажет	
		Машықтар: 1. Мақсат туралы ақпарат жинау үшін барлау жүргізу 2. Ашық порттар мен қызметтерді анықтау үшін Желіні сканерлеу құралдарын пайдаланыңыз	

	Дағды 2: Мақсат туралы ақпарат жинау	3. Құпия ақпараттың ағып кетуіне қоғамдық көздерді талдау 4. Барлау нәтижелерін есептерде құжаттау
		Білімдер: 1. Киберопераciяның мақсаты туралы барлау деректерін алу әдістері 2. Желілік хаттамалар мен сервистердің жұмыс принциптері 3. Кибер барлау құралдары 4. Желі пайдаланушысы туралы деректерді алуға нормативтік шектеулер
	Дағдыны тану мүмкіндігі:	Қажет
Еңбек функциясы 2: Қорғаныс кибероперацияларын жүргізу	Дағды 1: Қауіптерді бақылау және анықтау	Машықтар: 1. Интрузияны анықтау жүйелерін теңшеңіз 2. Аномалияларды анықтау үшін журналдар мен трафикті талдаңыз 3. Нақты уақыттағы дабылдарға жауап беру 4. Оқиғаларды әртүрлі көздерден корреляциялау
		Білімдер: 1. SIEM-жүйелердің жұмыс принциптері 2. Шабуыл үлгілері 3. Желіні бақылау құралдары 4. Қауіптерді анықтау әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Қауіпті бейтараптандыру және жүйені қалпына келтіру	Машықтар: 1. Желіде бұзылған түйіндерді оқшаулаңыз 2. Зиянды бағдарламаны жойыңыз және сақтық көшірмелерден жүйелерді қалпына келтіріңіз 3. Инциденттерге форензик-талдау жүргізу 4. Қауіп толық жойылғанға дейін уақытша қорғау шараларын енгізу
		Білімдер: 1. КҚ инциденттеріне ден қою процестері 2. Сандық криминалистика құралдары 3. КҚ қатерін жою және жою әдістері 4. Сақтық көшірме жасау және қалпына келтіру принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 1:	Машықтар: 1. Кибероперациялар үшін күш қолдану қағидаларын әзірлеу 2. Кибероперация шеңберінде команданың іс-қимылын үйлестіру 3. Мамандандырылған құралдарды дайындаңыз 4. Киберопераciяның ықтимал әсерін бағалау
		Білімдер:

Еңбек функциясы 3: Ш а б у ы л кибероперацияларын жүргізу	Кибер операцияларды жоспарлау және дайындау	1. Кибероперация кезеңдері 2. Шабуылдаушы кибероперациялардың құқықтық және этикалық аспектілері 3. Эксплуатация жасау құралдары 4. Шабуылдаушы кибероперациялардың тактикасы, техникасы және рәсімдері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Кибер операцияларды орындау және бақылау	Машықтар: 1. Мақсатты жүйелерге қол жеткізу және қолдау 2. Желі ішінде жылжытуды орындаңыз 3. Анықтаудан аулақ болу үшін әрекеттерді жасырыңыз 4. Нақты уақыттағы операцияның тиімділігін бағалау
		Білімдер: 1. Артықшылықтарды бекіту және арттыру әдістері 2. Анықтаусыз кибероперациялар жүргізу технигі 3. C2 Инфрақұрылым құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Жүргізілген кибероперацияның тиімділігін бағалау	Дағды 1: Операцияның қол жеткізілген нәтижелері туралы деректерді жинау және талдау	Машықтар: 1. Ендірілген эксплуатациялық құрылғылардан телеметрия мен журналдарды жинаңыз 2. Қажетті нәтижелерге қол жеткізу дәрежесін бағалау 3. Нәтижелерге қол жеткізбеу себептерін анықтаңыз 4. Киберкеңістікте келтірілген залалды бағалау (BDA) туралы есептерді дайындау
		Білімдер: 1. Келтірілген залалды бағалау әдістері (BDA) және қайта шабуыл жасау бойынша ұсыныстар 2. Киберкеңістіктегі шабуыл нәтижелеріне қол жеткізу көрсеткіштері 3. Трафикті талдау құралдары мен журналдар 4. Кибероперацияларда алынған тәжірибе принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Мақсаткерлік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
	Халықаралық стандарттар: ISO/IEC 15408 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	қауіпсіздігін бағалау критерийлері (Common Criteria) ISO/IEC 27033- Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Желілік қауіпсіздік ISO/IEC 27035 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік инциденттерін басқару (Incident management) ISO/IEC 27031 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Қызметтің үздіксіздігіне дайындық бойынша нұсқаулық (Continuity readiness) ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO / IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ 1073-2025 ("Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
21. Кәсіптің карточкасы "Кибер-нұсқаушы":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-020		
Кәсіптің атауы:	Кибер-нұсқаушы		
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: Педагогика және психология	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) педагогикалық білімі бар киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша бағдарламалары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Киберқауіпсіздік саласындағы дағдылар мен хабардарлықты арттыру үшін оқу бағдарламаларын әзірлейді және жеткізеді		
Еңбек функциялардың сипаттамасы			
		1. КҚ қамтамасыз ету және деректермен жұмыс 2. Киберқауіпсіздік бойынша білім беру бағдарламаларын құрастыру	

Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	3. Тренинг сабақтарын өткізу және оқушыларды бағалау
	Қосымша еңбек функциялары:	1. Жаңа қауіптерді іздеу негізінде оқу материалдарын жаңарту
Еңбек функциясы 1: АҚ қамтамасыз ету және деректермен жұмыс	Дағды 1: Кешенді киберқауіпсіздік және қорғалатын жүйелерді басқару	Машықтар: 1. Артефактілерді, журналдарды, жад демптерін, жүйелік жолдарды жинау және талдау 2. Құпия сөз саясаттарын, қауіпсіздік топтарын және көп факторлы аутентификацияны басқару 3. Топтық саясаттарды, пайдаланушы құқықтарын және брандмауэр ережелерін қолдану 4. Ақпараттық қауіпсіздік жүйелеріне аудит пен сынақ жүргізу
		Білімдер: 1. Цифрлық жүйелерді басқару және қорғау негіздері 2. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары 3. Қауіпсіздік жүйелерін талдау, аудит және тестілеу принциптері 4. Бағдарламалау тілдері
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 2: Киберқауіпсіздік инциденттерінің деректерін талдау және өңдеу	Машықтар: 1. Киберқауіпсіздік инциденттерін анықтау және жіктеу 2. Оқиғалар журналдарын, желілік трафикті және басқа деректер көздерін талдау 3. Оқиғаларды талдау нәтижелері бойынша есептер мен ұсыныстарды жасау 4. Арнайы құралдарды (SIEM, IDS/IPS, криминалистикалық құралдар) пайдалану
		Білімдер: 1. Киберқауіпсіздік инциденттерін жіктеу негіздері және олардың сипаттамалары 2. Киберқауіпсіздік инциденттері туралы деректерді жинау және өзара салыстыру әдістері 3. Инциденттерді тергеу және цифрлық криминалистика негіздері 4. Киберқауіпсіздік инциденттерін есепке алу мен өңдеуге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет
		Машықтар: 1. Киберқауіпсіздік бойынша білім беру модульдеріне қойылатын талаптарды талдау 2. Оқу мақсаттары мен нәтижелерін тұжырымдау 3. Аудитория деңгейін ескере отырып бағдарлама құрылымын құру 4. Сабақ жоспарларын әзірлеу

Еңбек функциясы 2: Киберқауіпсіздік бойынша білім беру бағдарламаларын құрастыру	Дағды 1: Оқу бағдарламасын әзірлеу	5. Тәжірибелік тапсырмалар мен зертханалық жұмыстардың сценарийлерін құрастыру.
		Білімдер: 1. Педагогикалық жобалау негіздері 2. Білім беру бағдарламаларының модульдік құрылысының принциптері 3. Білім беру бағдарламаларын әзірлеу әдістері 4. Киберқауіпсіздік саласындағы қажетті құзыреттер 5. Оқу құжаттамасына қойылатын талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Оқу материалдарын дайындау	Машықтар: 1. Оқу және әдістемелік жинақтарды әзірлеу 2. Нақты кибер инциденттерге негізделген кейстерді құру 3. Онлайн платформалар үшін мазмұнды дайындау 4. Тиімді визуализация құралдарын пайдалану 5. Материалды көрсетуде бейімделу тәсілдерін қолдану
		Білімдер: 1. Оқу материалдарының түрлері 2. Көрнекі коммуникация негіздері 3. Электрондық курстарды әзірлеу құралдары 4. Бейімделіп оқыту принциптері 5. Оқу және қолданбалы оқу материалдарына қойылатын талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: Оқу материалдарын бағалау	Машықтар: 1. Оқу материалдарына сараптамалық бағалау жүргізу 2. Бақылау-өлшеу әдістерін қолдану 3. Студенттердің кері байланысын талдау 4. Тәжірибелік зертханалық тапсырмалардың практикалық тиімділігін бағалау 5. Талдау нәтижелері бойынша материалдарды түзету
		Білімдер: 1. Педагогикалық сараптама әдістері 2. Оқу материалдарының сапасының критерийлері 3. Оқу материалын бағалау стандарттары 4. Білімді бақылаудың психометриялық әдістері 5. Оқушылардың білімін бақылау мен бағалаудың барлық түрлеріне тәсілдер
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Аудиториялық және онлайн сабақтарын өткізу 2. Топтық динамикасын басқару

Еңбек функциясы 3: Тренинг сабақтарын өткізу және оқушыларды бағалау	Дағды 1: Аудиториялық және онлайн сабақтарын өткізу	3. Күрделі материалды қолжетімді түрде түсіндіру 4. Оқушыларды белсенді қатысуға ынталандыру 5. Сабақ уақытын және құрылымын басқару
		Білімдер: 1. Белсенді оқыту әдістері 2. Қоғамдық коммуникация негіздері 3. Педагогикалық процестің психологиясы 4. Топтық жұмыс әдістері 5. Жеңілдетілген түсіндіру техникасы
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: АҚ саласында тәжірибелік сабақтарды өткізу	Машықтар: 1. Модельдеу платформаларында практикалық сабақтар ұйымдастыру 2. Кибершабуылдарды модельдеу 3. Киберқауіпсіздік инциденттеріне жауап беру тапсырмаларын құрастыру 4. Виртуалды практикалық орталарды орнату 5. Оқушылардың іс-әрекетін талдау
		Білімдер: 1. Кибергигиена 2. Кибершабуылдарды модельдеу әдістері 3. Кибер полигондарды құру принциптері 4. Сандық сот сараптамасының негіздері 5. Киберқауіпсіздік инциденттерін басқару құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: Оқыту нәтижелерін бақылау және бағалау	Машықтар: 1. Білімді тексеруге арналған материалдарды әзірлеу 2. Тәжірибелік тапсырмалардың орындалуын бағалау 3. Автоматтандырылған тестілеу жүйесін қолдану 4. Дағдыларды қорытынды бағалауды жүргізу 5. Бағалау нәтижелерін талдау және өңдеу
		Білімдер: 1. Бағалау стандарттары мен критерийлері 2. Бақылау түрлері мен тест тапсырмалары 3. Тест нәтижелерін талдау әдістері 4. Объективті бағалау принциптері 5. Тесттер өткізу мен нәтижелерді бағалаудың автоматтандырылған жүйелері
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Киберқауіптердің өзгерістерін бақылау 2. Компаниялар мен CERT орталықтарының есептерін талдау 3. Оқушылар үшін маңызды қауіптерді белгілеу

Қосымша еңбек функциясы 1: Жаңа қауіптерді іздеу негізінде оқу материалдарын жаңарту	Дағды 1: Ағымдағы қауіптерді талдау	4. Алынған деректерді оқу материалдарының мазмұнымен салыстыру 5. Аналитикалық құралдарды қолдану
		Білімдер: 1. Киберқауіптер туралы деректердің негізгі көздері 2. Шабуылдар мен осалдықтардың типтері 3. Киберқауіптерді талдау принциптері 4. Киберқауіпсіздіктің ағымдағы үрдістері 5. Тәуекелдерді бағалау әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Мақсаткерлік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 27001 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар ISO/IEC 27002 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары (практика кодексі) ISO/IEC 15408 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері (Common Criteria) ISO/IEC 27033- Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Қауіпсіз желіні құруды үйрету ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO / IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ 1073-2025 ("Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
22. Кәсіптің карточкасы "Зерттеу және әзірлеу жөніндегі маман":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-029	
Кәсіптің атауы:	Зерттеу және әзірлеу 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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Негізгі (жоғары) техникалық білімі бар киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша бағдарламалары		
Кәсіптің басқа ықтимал атаулары:	2153-2-009 - Телекоммуникациялар жөніндегі инженер-әзірлеуші 1233-0-001 - Бас конструктор (ғылыми зерттеулер және әзірлемелер жөніндегі)		
Қызметтің негізгі мақсаты:	Киберқауіпсіздік саласындағы инновацияларды әзірлейді, пайда болатын қауіптермен күресудің жаңа технологиялары мен әдістемелерін зерттейді.		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. КҚ және деректерді басқару 2. КҚ саласында ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарды жүргізу 3. Ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстар кезінде КҚ жүйесін сынақтан өткізу	
	Қосымша еңбек функциялары:		
Еңбек функциясы 1: АҚ және деректерді басқару	Дағды 1: Кешенді киберқауіпсіздік және қорғалатын жүйелерді басқару	Машықтар: 1. Артефактілерді, журналдарды, жад демптерін, жүйелік жолдарды жинау және талдау 2. Құпия сөз саясаттарын, қауіпсіздік топтарын және көп факторлы аутентификацияны басқару 3. Топтық саясаттарды, пайдаланушы құқықтарын және брандмауэр ережелерін қолдану 4. Киберқауіпсіздік жүйелеріне аудит пен сынақ жүргізу	
		Білімдер: 1. Цифрлық жүйелерді басқару және қорғау негіздері 2. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары 3. Қауіпсіздік жүйелерін талдау, аудит және тестілеу принциптері 4. Бағдарламалау тілдері	
	Дағдыны тану мүмкіндігі:	Қажет	
		Машықтар: 1. Киберқауіпсіздік инциденттерін анықтау және жіктеу 2. Оқиғалар журналдарын, желілік трафикті және басқа деректер көздерін талдау	

	Дағды 2: Киберқауіпсіздік инциденттерінің деректерін талдау және өңдеу	3. Оқиғаларды талдау нәтижелері бойынша есептер мен ұсыныстарды жасау 4. Арнайы құралдарды (SIEM, IDS/IPS, криминалистикалық құралдар) пайдалану
		Білімдер: 1. КҚ инциденттерін жіктеу негіздері және олардың сипаттамалары 2. КҚ инциденттері туралы деректерді жинау және өзара салыстыру әдістері 3. Инциденттерді тергеу және цифрлық криминалистика негіздері 4. КҚ инциденттерін есепке алу мен өңдеуге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет
Еңбек функциясы 2: КҚ саласында ғылыми-зерттеу және	Дағды 1: АҚ саласында патенттік зерттеулер жүргізу	Машықтар: 1. Патент тазалығын қамтамасыз ету шараларын негіздеу 2. Кедергісіз өндіру және сату шараларын негіздеу 3. Киберқауіпсіздік саласында жаңадан жасалған шешімдердің патенттік қабілеттілігін бағалау 4. Киберқауіпсіздік саласындағы зияткерлік меншік объектілеріне зерттеулердің қолданылуын талдау әдістерін қолдану 5. Шешімнің техникалық деңгейінің көрсеткіштерін анықтау
		Білімдер: 1. Қорғау құжаттары: патенттер, өтінімдер 2. Киберқауіпсіздік саласындағы қорғалатын объектілермен патент объектісін салыстырмалы талдау 3. Патент тазалығын анықтау әдістері 4. Зерттеу объектілерін қорғаудың құқықтық негіздері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Ғылыми-техникалық ақпаратты және зерттеу нәтижелерін өңдеу және талдау бойынша жұмыстарды жүргізу	Машықтар: 1. Ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарды жүргізудің жоспарлары мен әдістемелік бағдарламаларын әзірлеу 2. Ғылыми-техникалық ақпаратты жинау мен зерттеуді ұйымдастыру 3. Ғылыми мәліметтерді, эксперименттер мен бақылаулардың нәтижелерін талдауды жүргізу 4. Ғылыми деректерді, эксперименттер мен бақылаулардың нәтижелерін теориялық жалпылауды жүзеге асыру
		Білімдер:

тәжірибелік-конструкторлық жұмыстарды жүргізу		1. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер мен техникалық құжаттар 2. Ғылыми деректерді талдау әдістері 3. Ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарды жоспарлау және ұйымдастыру әдістері мен құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: АҚ саласында зерттеулер жүргізу кезінде жұмысшылар тобын басқару	Машықтар: 1. Ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарды жүргізудің жоспарлары мен әдістемелік бағдарламаларының элементтерін әзірлеу 2. Ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстардың нәтижелерін белгіленген өкілеттіктерге сәйкес енгізу 3. Қызметкерлер алған нәтижелердің дұрыстығын тексеру 4. Өз қызметкерлеріміздің біліктілігін арттыруды жүзеге асыру
		Білімдер: 1. Еңбек және басқару саласындағы қолданыстағы нормативтік құжаттама 2. Еңбекті ұйымдастыру және персоналды басқару әдістері 3. Ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстардың нәтижелерін енгізу әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстар кезінде КҚ жүйесін сынақтан өткізу	Дағды 1: Киберқауіпсіздікті кешенді тестілеу	Машықтар: 1. Пентесттерді өткізу 2. Бастапқы кодты талдау 3. Осалдықты сканерлеу 4. Осалдықты пайдалану
		Білімдер: 1. Пентестинг кезінде барлау, сканерлеу, пайдалану және пайдаланудан кейінгі пайдалану 2. Кодтағы типтік қателер 3. Осалдықты пайдалану әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: АҚ қолданылатын әлеуметтік инженерия	Машықтар: 1. Әлеуметтік инженерия әдістері арқылы адам факторларын сынау 2. Тестілеу процесін жоспарлау, үйлестіру және құжаттау 3. Уақыт пен ресурстарды басқару

	саласында зерттеулер жүргізу	Білімдер: 1. Әлеуметтік инженерия әдістері 2. Уақытты басқару 3. Зерттеу кезеңдерін жүргізу және басқару тәртібі	
	Дағдыны тану мүмкіндігі:	Қажет емес	
Жеке құзыреттерге қойылатын талаптар:	Дербестік және жауапкершілік Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Мақсаткерлік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық		
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 15408-1:2018 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Overview and general model ISO/IEC 15408-2/3 — функционалдық және қауіпсіздік талаптарын қамтитын бөліктер. ҚР Ұлттық стандарттары: ҚР СТ ISO/IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO/IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ 1073-2025 ("ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар") ҚР СТ 4009-2025 ("Ақпараттық технологиялар. Ақпаратты криптографиялық қорғау. Блоктық симметриялық шифрлау алгоритмі")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
23. Кәсіптің карточкасы "IT инвестициялары/портфолио менеджері":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-022		
Кәсіптің атауы:	IT инвестициялары/портфолио менеджері		
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:	Қажет емес		

Формалды емес және информалы біліммен байланыс:	Негізгі (жоғары) қаржылық білімі бар киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша бағдарламалары	
Кәсіптің басқа ықтимал атаулары:	2412-0-003 - Инвестиция жөніндегі консультант	
Қызметтің негізгі мақсаты:	АТ инвестицияларының ұйымның стратегиялық мақсаттарына сәйкес келуін және киберқауіпсіздік қажеттіліктерін қанағаттандыруын қамтамасыз етеді	
Еңбек функциялардың сипаттамасы		
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. КҚ қамтамасыз ету және деректермен жұмыс 2. ЦТ инвестицияларын стратегиялық басқару 3. ЦТ инвестицияларына қаржылық және аналитикалық қолдау көрсету
	Қосымша еңбек функциялары:	1. ЦТ инвестицияларындағы сәйкестікті басқару
Еңбек функциясы 1: АҚ қамтамасыз ету және деректермен жұмыс	Дағды 1: Кешенді киберқауіпсіздік және қорғалатын жүйелерді басқару	Машықтар: 1. Артефактілерді, журналдарды, жад демптерін, жүйелік жолдарды жинау және талдау 2. Құпия сөз саясаттарын, қауіпсіздік топтарын және көп факторлы аутентификацияны басқару 3. Топтық саясаттарды, пайдаланушы құқықтарын және брандмауэр ережелерін қолдану 4. Киберқауіпсіздік жүйелеріне аудит пен сынақ жүргізу
		Білімдер: 1. Цифрлық жүйелерді басқару және қорғау негіздері 2. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары 3. Қауіпсіздік жүйелерін талдау, аудит және тестілеу принциптері 4. Бағдарламалау тілдері
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 2: Киберқауіпсіздік инциденттерінің деректерін талдау және өңдеу	Машықтар: 1. Киберқауіпсіздік инциденттерін анықтау және жіктеу 2. Оқиғалар журналдарын, желілік трафикті және басқа деректер көздерін талдау 3. Оқиғаларды талдау нәтижелері бойынша есептер мен ұсыныстарды жасау 4. Арнайы құралдарды (SIEM, IDS/IPS, криминалистикалық құралдар) пайдалану
		Білімдер: 1. Киберқауіпсіздік инциденттерін жіктеу негіздері және олардың сипаттамалары 2. Киберқауіпсіздік инциденттері туралы деректерді жинау және өзара салыстыру әдістері 3. Инциденттерді тергеу және цифрлық криминалистика негіздері

		4. Киберқауіпсіздік инциденттерін есепке алу мен өңдеуге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет
Еңбек функциясы 2: ЦТ инвестицияларын стратегиялық басқару	Дағды 1: ЦТ инвестицияларының стратегиялық жоспарын құрастыру	Машықтар: 1. Ұйымның стратегиясын талдаңыз және ЦТ инвестициялары бойынша ұзақ мерзімді нұсқауларды тұжырымдаңыз 2. Бизнес талаптары мен тәуекелдер негізінде ЦТ бастамаларын қаржыландыру басымдықтарын анықтау 3. ЦТ инвестицияларының корпоративтік мақсаттарға қол жеткізуге әсерін бағалау 4. Басшылық пен мүдделі тараптарға инвестиция қажеттілігін негіздеу
		Білімдер: 1. Стратегиялық және қаржылық жоспарлау принциптері 2. Бизнес басымдықтары мен шығындар факторларын талдау әдістері 3. АТ-ның корпоративтік басқару негіздері 4. ЦТ стратегиясына киберқауіпсіздік талаптарын біріктіру принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: IT жоба портфолиосын басқару	Машықтар: 1. ЦТ бастамаларының портфолиосы мен инвестициялық қажеттіліктер туралы деректерді біріктіру 2. ЦТ жобаларының құнын, күрделілігін және тәуекелін бағалау 3. Инновациялық, операциялық және қорғаушы бастамалар арасындағы портфельді теңестіру 4. Портфель құрамы бойынша шешімдерді басшылықпен келісу
		Білімдер: 1. Жобалардың инвестициялық тартымдылығын бағалау тәсілдері 2. ЦТ -бастамаларды жіктеу әдістері 3. Инвестициялық және жобаларды басқару негіздері 4. Тәуекелдер мен киберқауіпсіздікті басқару тәсілдері
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Инвестициялық өнімділікті бағалау критерийлерін әзірлеу 2. ЦТ жобаларының нақты шығындары мен пайдасын талдауды жүргізу

	Дағды 3: ЦТ инвестициясының тиімділігін бағалау	3. ЦТ инвестицияларының тиімділігі туралы есептерді қалыптастыру 4. ЦТ инвестицияларының табыстылығын арттыру бағыттарын анықтау
		Білімдер: 1. Жобадан кейінгі талдау әдістері 2. Тиімділікті бағалаудың қаржылық үлгілері 3. KPI/KRI көрсеткіштерін жинау және талдау әдістері 4. Бюджеттің атқарылуын бақылау негіздері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: ЦТ инвестицияларына қаржылық және аналитикалық қолдау көрсету	Дағды 1: ЦТ инвестицияларын қаржылық модельдеу	Машықтар: 1. Инвестициялық сценарийлерді бағалаудың қаржылық үлгілерін әзірлеу 2. ЦТ инвестицияларының болжамды қаржылық нәтижелерін есептеу 3. Инвестицияларды құны мен құны бойынша салыстыру 4. Презентация материалдарын дайындау
		Білімдер: 1. Инвестициялық талдау және қаржылық модельдеу әдістері 2. Сценарийлік талдаудың негіздері 3. Қаржылық деректерге және олардың сапасына қойылатын талаптар 4. Болжалды ақша ағындарын қалыптастыру принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: ЦТ инвестицияларын бюджеттеу және жоспарлау	Машықтар: 1. АТ-инвестициялық бюджетті әзірлеу және жаңарту 2. Дисперсиялық талдауды және шығындарды болжауды жүргізу 3. Инвестициялық өтінімдер үшін қаржылық негіздемелерді дайындау 4. Бюджеттік өтінімдерді қаржы бөлімдерімен үйлестіру
		Білімдер: 1. Бюджеттеу әдістері 2. Басқару есебінің негіздері 3. ЦТ инвестицияларды бөлу принциптері 4. Инвестициялық жобаларды жобалауға қойылатын қаржылық талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Заңнамалық және салалық талаптарды талдау

Қосымша еңбек функциясы 1: Ц Т инвестицияларындағы сәйкестікті басқару	Дағды 1: ЦТ инвестицияларының нормативтік талаптарға сәйкестігін бақылау	2. ЦТ бастамаларының нормативтік стандарттарға сәйкестігін бағалау 3. Сәйкессіздіктерді жою бойынша ұсыныстарды әзірлеу 4. Нормативтік талаптарға сәйкестік туралы есептерді дайындау
		Білімдер: 1. ЦТ және киберқауіпсіздік саласындағы нормативтік құқықтық актілер 2. Дербес деректерді өңдеуге қойылатын талаптар 3. Сатып алулар мен инвестицияларды реттеу стандарттары 4. Сәйкестік процестерін құжаттандыру тәсілдері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 27001 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар ISO/IEC 27005 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік тәуекелдерін басқару ISO/IEC 27002 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары (практика кодексі) ISO 31000-тәуекелдерді басқару. Принциптер мен нұсқаулық ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ ISO / IEC 27005-2013 ("Ақпараттық технологиялар . Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік тәуекелін басқару") ҚР СТ 1073-2025 ("Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар") ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
24. Кәсіптің карточкасы "Бағдарлама менеджері":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-021	
Кәсіптің атауы:	Бағдарлама менеджері	
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) басқару білімі бар киберқауіпсіздік саласындағы кәсіби біліктілікті арттырудың қосымша бағдарламалары		
Кәсіптің басқа ықтимал атаулары:	2512-1-003 - АКТ жобалары менеджері		
Қызметтің негізгі мақсаты:	Ұйымдық мақсаттарға, мерзімдерге және бюджетке сәйкес келетініне көз жеткізу үшін киберқауіпсіздік жобаларын қадағалайды.		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. КҚ және деректерді басқару 2. Алынған жоспарлар негізінде КҚ жобаларын басқару 3. Келісімшарттық міндеттемелер негізінде КҚ жобаларын жоспарлау және аяқтау	
	Қосымша еңбек функциялары:	1. Қызметкерлерді басқару әдістеріне үйрету	
Еңбек функциясы 1: КҚ және деректерді басқару	Дағды 1: Кешенді киберқауіпсіздік және қорғалатын жүйелерді басқару	Машықтар: 1. Артефактілерді, журналдарды, жад демптерін, жүйелік жолдарды жинау және талдау 2. Құпия сөз саясаттарын, қауіпсіздік топтарын және көп факторлы аутентификацияны басқару 3. Топтық саясаттарды, пайдаланушы құқықтарын және брандмауэр ережелерін қолдану 4. КҚ жүйелеріне аудит пен сынақ жүргізу	
		Білімдер: 1. Цифрлық жүйелерді басқару және қорғау негіздері 2. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары 3. Қауіпсіздік жүйелерін талдау, аудит және тестілеу принциптері 4. Бағдарламалау тілдері	
	Дағдыны тану мүмкіндігі:	Қажет	
		Машықтар: 1. Киберқауіпсіздік инциденттерін анықтау және жіктеу 2. Оқиғалар журналдарын, желілік трафикті және басқа деректер көздерін талдау	

	Дағды 2: Киберқауіпсіздік инциденттерінің деректерін талдау және өңдеу	3. Оқиғаларды талдау нәтижелері бойынша есептер мен ұсыныстарды жасау 4. Арнайы құралдарды (SIEM, IDS/IPS, криминалистикалық құралдар) пайдалану
		Білімдер: 1. Киберқауіпсіздік инциденттерін жіктеу негіздері және олардың сипаттамалары 2. Киберқауіпсіздік инциденттері туралы деректерді жинау және өзара салыстыру әдістері 3. Инциденттерді тергеу және цифрлық криминалистика негіздері 4. Киберқауіпсіздік инциденттерін есепке алу мен өңдеуге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет
Еңбек функциясы 2: Алынған жоспарлар негізінде КҚ жобаларын басқару	Дағды 1: Алынған жоспарға сәйкес киберқауіпсіздік жүйелері жобаларында шарттардың орындалуын бақылау	Машықтар: 1. Құжаттарды әзірлеу 2. Байланыс жасау 3. Есептерді дайындау 4. Енгізілген деректерді талдау 5. Жеткізу және төлеу мерзімдері бойынша шарттық міндеттемелердің орындалуын бақылау
		Білімдер: 1. Іс жүргізу негіздері 2. Іскерлік өзара әрекеттесудегі тұлғааралық және топтық қарым-қатынас технологиялары, жанжалдарды басқару негіздері 3. Шарт бойынша міндеттемелердің орындалуын бақылау құралдары мен әдістері 4. Төлемдерді жүзеге асыру құралдары мен әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Алынған жоспарға сәйкес жобалық жұмыстың орындалуын ұйымдастыру	Машықтар: 1. Алынған жоба жоспарларына сәйкес жоба жұмысын орындау үшін жоба тобының мүшелерін тағайындау 2. Жобаны аяқтау үшін қажетті ресурстарды алыңыз және басқару 3. Жұмыс аяқталғаннан кейін жоба тобы мүшелерінен өнімділік есептерін алыңыз және бақылау 4. Жұмыстың аяқталуын растауды бақылау
		Білімдер: 1. Рөлді бөлуге арналған RACI матрицасы (жауапты, есеп беретін, консультацияланған, хабардар) 2. Түгендеу объектілерін алуды, сақтауды және пайдалануды ұйымдастыру тәртібі 3. Киберқауіпсіздік саласындағы есептілік құжаттамасы

		4. Келісімшарттық міндеттемелер саласындағы есептілік құжаттамасы
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: Алынған жоспарға сәйкес КҚ жүйесінің конфигурацияларының аудиті	Машықтар: 1. Киберқауіпсіздік жүйесінің конфигурациясының формальды физикалық аудитін жүргізу 2. Киберқауіпсіздік жүйесінің конфигурациясының ресми функционалдық аудитін жүргізу 3. Деректерді қорғау жүйесінің техникалық сипаттамаларын бағалау 4. Ақпаратты қорғау саласындағы кеңейтілген параметрлермен және терминологиямен жұмыс
		Білімдер: 1. Киберқауіпсіздік жүйесінің конфигурациясының физикалық аудитінің құралдары мен әдістері 2. Киберқауіпсіздік жүйесінің конфигурациясының функционалдық аудитінің құралдары мен әдістері 3. Техникалық шарттарды конфигурациялау 4. Деректерді қорғау жүйелерінің кеңейтілген терминологиясы мен техникалық параметрлері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Келісімшарттық міндеттемелер негізінде КҚ жобаларын жоспарлау және аяқтау	Дағды 1: Алынған тапсырмаға сәйкес жобаны жоспарлау	Машықтар: 1. Жобаны басқару жоспарын және оның қосалқы жоспарларын құрастырыңыз 2. Алынған тапсырмаға сәйкес жобалық жұмыстың иерархиялық құрылымын жасаңыз 3. Алынған тапсырмаға сәйкес жоба кестесін жасаңыз 4. Алынған тапсырмаға сәйкес жобаның сметасын жасаңыз 5. Алынған тапсырмаға сәйкес жобаны қаржыландыру жоспарын жасаңыз
		Білімдер: 1. Жобаны басқару жоспарының құрылымы мен мазмұнын білу 2. Құрылыс принциптерін және жұмыстарды бұзу ережелерін білу 3. Желіні жоспарлау әдістерін білу 4. Шығындарды бағалау әдістерін білу 5. Жобаның қаржылық ағындарын бөлу және жоспарлау принциптерін білу
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Шартқа және жобалық құжаттамаға сәйкес жоба нәтижелерін тапсырыс берушіге хабарлау 2. Жоба деректерін мұрағаттау 3. Жоба есебін әзірлеу

	Дағды 2: Алынған тапсырмаға сәйкес жобаны аяқтау	4. Жиналған тәжірибе негізінде басқару жүйесіне түзетулер енгізу
		Білімдер: 1. Коммуникация құралдары мен әдістері 2. Байланыс арналары 3. Коммуникациялық модельдер 4. Жобаны басқару пәндері 5. Қорытынды жобалық құжаттарды дайындау тәртібі
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Қызметкерлерді басқару әдістеріне үйрету	Дағды 1: Басқару әдістері бойынша оқу сабақтарын өткізу	Машықтар: 1. Қызметкерлердің дайындық деңгейін ескере отырып оқыту бағдарламасын жасау 2. Басқару әдістері бойынша тренингтер, лекциялар және практикалық сабақтар өткізу 3. Оқытудың интерактивті әдістерін қолдану
		Білімдер: 1. Заманауи басқару әдістемесі 2. Сабақты ұйымдастыру және өткізу принциптері 3. Оқушылардың белсенділігін бағалау әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements ISO/IEC 27002:2022 — Code of practice for information security controls ISO/IEC 27005:2018 — Information security risk management ҚР Ұлттық стандарттары: ҚР СТ ISO/IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ ISO/IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO/IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ 1073-2025 ("ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар") ҚР СТ 4009-2025 ("Ақпараттық технологиялар. Ақпаратты криптографиялық қорғау. Блоктық симметриялық шифрлау алгоритмі")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
25. Кәсіптің карточкасы "Қауіптер мен ескертулер талдаушысы":		

Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-023		
Кәсіптің атауы:	Қауіптер мен ескертулер талдаушысы		
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік бағыты бойынша базалық (жоғары) білім болған кезде киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Қарсыластың мүмкіндіктері мен ниеттерін талдау негізінде қауіп-қатерді бағалауды дамытады.		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Қауіптер мен ықтимал қарсыластар туралы деректерді жинау, өңдеу және жинақтау 2. Қарсыластың мүмкіндіктері мен ниеттерін талдау, қауіп-қатерді бағалау 3. Қауіптерге қарсы іс-қимыл бойынша ескертулерді , ұсынымдарды және есептілікті қалыптастыру	
	Қосымша еңбек функциялары:		
	Дағды 1: Нысаналы шабуылдарды дайындау және іске асыру белгілерін мониторингілеу және анықтау	Машықтар: 1. Шабуылдарды дайындау тізбегін анықтау үшін Siem-де корреляция ережелерін теңшеңіз 2. Қалыпты емес мінез-құлық үшін EDR/XDR телеметриясын талдаңыз 3. Барлау, шабуыл құралын құру және бастапқы қол жетімділік белгілерін анықтаңыз 4. Қарсыластың инфрақұрылымындағы өзгерістерді бақылау (C2, домендер, IP) 5. Тізімдерді қалыптастыру және жаңарту	
		Білімдер: 1. Att&CK моделі (Enterprise, Mobile, ICS қоса алғанда) 2. APT топтары мен киберқылмыскерлер қауымдастығының типтік TTPs	

Еңбек функциясы 1: Қауіптер мен ықтимал қарсыластар туралы деректерді жинау, өңдеу және жинақтау		3. Инфрақұрылымды белсенді және пассивті сканерлеу әдістері 4. Нөлдік күндік осалдықтарды пайдалану белгілері 5. Мінез-құлықты талдау және UEBA негіздері
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 2: Компаға келу индикаторларын және қауіп туралы деректерді жинау және бастапқы өңдеу	Машықтар: 1. Ашық, коммерциялық және жабық қауіп көздеріне сұраныстар қалыптастыру 2. Компаға келу индикаторларын талдауды және қалыпқа келтіруді жүзеге асыру 3. Алынған деректердің дұрыстығын бастапқы тексеруді және бағалауды жүргізу 4. Дереккөздерді сенім деңгейі мен өзектілігі бойынша жіктеңіз 5. API және сценарий құралдарын пайдаланып деректерді жинауды автоматтандыру
		Білімдер: 1. Threat intelligence негізгі платформалары мен арналары (MISP, OTX, STIX / TAXII, VirusTotal және т. б.) 2. Индикаторларды ұсыну форматтары (STIX 2.x, OpenIOC, YARA, Sigma) 3. Threat intelligence көздерінің жіктелуі (OSINT, HUMINT, коммерциялық, жабық) 4. Деректердің дұрыстығын бағалау принциптері 5. Өзекті қатерлер санаттары бойынша нормативтік құжаттар
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 1: Қауіп-қатер субъектісінің мүмкіндіктері мен уәждемесіне көп аспектілі талдау жүргізу	Машықтар: 1. Қауіп профильдерін құру 2. Жаудың техникалық және ресурстық мүмкіндіктерін бағалау 3. Шабуылдаушы субъектінің ықтимал мақсаттары мен басымдықтарын анықтаңыз 4. Әр түрлі топтардың TTPs салыстырмалы талдауын жүргізу 5. Жаудың келесі қадамдары туралы гипотезалар жасаңыз
		Білімдер: 1. Қауіп субъектілерінің жіктелуі (мемлекеттік, киберқылмыскерлер, хактивистер, инсайдерлер) 2. Бұзушының мүмкіндіктерін бағалау әдістері (ISO 27005) 3. КИБЕРҚАУІПТЕРДІҢ жетілу модельдері (APT үшін CMMI тәрізді) 4. Киберқылмыстың мотивациялық факторлары және экономикалық модельдері 5. Қауіптердің дамуын сценарийлік болжау әдістері

Еңбек функциясы 2: Қарсыластың мүмкіндіктері мен ниеттерін талдау, қауіп-қатерді бағалау	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Қауіптерді бағалауды әзірлеу және өзектендіру	Машықтар: 1. Белгілі бір ұйым / сала үшін қауіптердің өзектілігін анықтау 2. Қауіпті іске асырудың ықтималдығы мен ықтимал салдарын есептеңіз 3. Қауіп пен осалдық матрицаларын қалыптастыру (threat × vulnerability) 4. Қауіптердің басымдығы туралы негізделген қорытындылар дайындау 5. Қауіп моделін жаңарту үшін материалдар дайындаңыз
		Білімдер: 1. Қауіптерді бағалау әдістемесі 2. Тәуекелдерді сапалық және сандық бағалау тәсілдері 3. Әлемде қолданылатын ықтималдық пен зиян шкалалары 4. ГАЖ, КВОИКА үшін қауіп модельдеріне қойылатын талаптар 5. Қатерлерді бағалауды өзектендіруге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Қауіптерге қарсы іс-қимыл бойынша	Дағды 1: Ескертулерді дайындау және тарату (advisory / warning)	Машықтар: 1. Құрылымдық ескертулер жасаңыз (TLP форматы, Traffic Light Protocol) 2. Ескертудің сыни және шұғыл деңгейін анықтау 3. Мазмұнды әртүрлі мақсатты аудиторияға бейімдеу 4. Ақпаратты таратудың құпиялылығын қамтамасыз ету 5. Кері байланыс пен ескертулердің тиімділігін бақылау
		Білімдер: 1. TLP түсті таңбалау жүйесі (WHITE / green / AMBER / RED) 2. Ескертулерді ресімдеуге және таратуға қойылатын талаптар 3. КҚ саласындағы шектеулі ақпаратпен жұмыс істеу қағидалары 4. Хабарландыру арналары мен форматтары (email, мессенджерлер, порталдар) 5. КҚ бойынша коммуникациялар тиімділігінің көрсеткіштері
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар:

ескертулерді, ұсынымдарды және есептілікті қалыптастыру	Дағды 2: Қауіптерге қарсы іс-қимыл бойынша ұсынымдарды әзірлеу және негіздеу	1. Қарсы іс-қимыл шараларының басым тізбесін қалыптастыру 2. Ұсынылған шаралардың қолданылуы мен құнын бағалау 3. Ұсынымдарды іске асырудың Жол картасын дайындау 4. Ұсыныстарды нормативтік талаптармен және үздік тәжірибелермен негіздеу 5. Процестердің иелерімен шараларды келісуге қатысу
		Білімдер: 1. Қорғау шараларының иерархиясы (техникалық, ұйымдастырушылық, құқықтық) 2. Ең жақсы қарсы тәжірибелер (CIS Controls, NIST CSF) 3. Defence-in-depth және zero trust принциптері 4. Қорғау шараларының тиімділігін бағалау әдістері 5. Реттеушілердің анықталған қатерлерді өтеу шараларына қойылатын талаптары
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Тәртіптілік Аналитикалық ойлау Бастамашылық Көшбасшылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 27005 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік тәуекелдерін басқару (тәуекелдерді басқару) ISO/IEC 27035 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік инциденттерін басқару (information security incident management) ISO/IEC 15408 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Қауіпсіздік талаптарын талдау (Common Criteria) ҚР Ұлттық стандарттары: ҚР СТ ISO/IEC 27005-2013 ("Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік тәуекелінің менеджменті") ҚР СТ ISO/IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен іс-әрекеттері ерекшелігінің құрылымы") ҚР СТ ISO/IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
26. Кәсіптің карточкасы "Желілік операциялар жөніндегі маман":		
Топтың коды:	2524-0	
Қызмет атауының коды:	2524-0-031	
Кәсіптің атауы:	Желілік операциялар 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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) IT-білім болған кезде ақпараттық қауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Желілік инфрақұрылымды, соның ішінде маршрутизаторларды, коммутаторларды және брандмауэрлерді басқарады және қорғайды, желінің сенімді және қауіпсіз жұмысын қамтамасыз етеді		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Желілік инфрақұрылымды мониторингілеу және пайдалану 2. Желілік инфрақұрылымның қауіпсіздігін қамтамасыз ету 3. Ақаулықтарды жою және желіні оңтайландыру	
	Қосымша еңбек функциялары:	1. Тәуекелдерді бағалау және ЦТ архитектурасындағы нормативтік талаптарға сәйкестікті қамтамасыз ету	
Еңбек функциясы 1:	Дағды 1: Желілік жабдықты пайдалану	Машықтар: 1. Маршрутизаторлар мен қосқыштарды конфигурациялау 2. Виртуалды Жергілікті желілерді және коммутация механизмдерін басқарыңыз 3. Ендірілген бағдарламалық жасақтаманы жаңартыңыз және қауіпсіздік патчтарын қолданыңыз 4. Конфигурациялардың сақтық көшірмесін жасаңыз және қалпына келтіріңіз	
		Білімдер: 1. Жетекші өндірушілердің желілік жабдықтарының командалық интерфейстері 2. OSI анықтамалық моделі және TCP/IP моделі 3. Динамикалық бағыттау хаттамалары 4. Арналарды коммутациялау және агрегациялау хаттамалары мен тетіктері	

Желілік инфрақұрылымды мониторингілеу және пайдалану	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Желі күйін бақылау	Машықтар: 1. Желілік бақылау жүйелерін конфигурациялау және пайдалану 2. Желі өнімділігінің көрсеткіштерін талдау (өткізу қабілеттілігі, кідірістер, пакеттің жоғалуы) 3. Нақты уақыт режимінде желілік трафиктің ауытқуларын анықтаңыз 4. Желі жұмысындағы бұзушылықтар туралы ескертулер мен хабарламаларды теңшеу
		Білімдер: 1. Желілік мониторинг және телеметрия хаттамалары 2. Желілік инфрақұрылымды бақылау платформалары мен құралдары 3. Желі өнімділігінің негізгі көрсеткіштері 4. Проактивті мониторинг және оқиғаларды ерте анықтау принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 2: Желілік инфрақұрылымның қауіпсіздігін қамтамасыз ету	Дағды 1: Желілік қауіптерден қорғау	Машықтар: 1. Қызмет көрсетуден бас тарту шабуылдарын анықтаңыз және қарсы тұрыңыз 2. Желіні сегментациялау және микросегментациялауды жүзеге асыру 3. Қауіпсіздік оқиғаларының журналдарын талдау 4. Пайдаланушы рөлдеріне негізделген қол жетімділікті бөлуді теңшеңіз
		Білімдер: 1. Желілік шабуылдардың негізгі түрлері және оларды жүзеге асыру әдістері 2. Киберқауіпсіздіктің халықаралық және салалық стандарттары 3. КҚ саласындағы ҚР нормативтік талаптары 4. Желілік трафикті талдау және инциденттерді тергеу құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Желілік қорғаныс құралдарын орнату	Машықтар: 1. Жаңа буын брандмауэрлерін конфигурациялау 2. Желілік трафикті сүзу және мекен-жайларды аудару ережелерін әзірлеу және қолдану 3. Қорғалған виртуалды жеке желілерді енгізу 4. Интрузияны анықтау және алдын алу жүйелерін теңшеңіз
		Білімдер: 1. Байланыс күйлерін бақылай отырып, брандмауэрлердің жұмыс істеу принциптері 2. NGFW архитектурасы және функционалдығы

		3. Желілік қосылымдарды қорғаудың криптографиялық хаттамалары 4. Zero Trust тәсілдері және бақыланатын желіге қол жеткізу
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Ақаулықтарды жою және желіні оңтайландыру	Дағды 1: Желінің жұмысын диагностикалау және қалпына келтіру	Машықтар: 1. Байланыс және маршруттау диагностикасын жүргізу 2. Ақаулардың себептерін анықтау үшін желілік пакеттерді талдаңыз 3. Істен шыққан кезде желінің жұмысын қалпына келтіру 4. Оқиғалардың өршуі кезінде жабдықты жеткізушілермен өзара әрекеттесу
		Білімдер: 1. Желілік диагностика құралдары 2. Ақаулықтарды жою әдістемелері 3. Жоғары қолжетімділік және резервтеу принциптері 4. Қызмет көрсету деңгейлері және инциденттерге басымдық беру
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Желі өнімділігін оңтайландыру	Машықтар: 1. Желілік аудит және сыйымдылықты жоспарлау 2. Трафикке басымдық беру тетіктерін теңшеңіз 3. Маршруттауды және жүктемені теңестіруді оңтайландыру 4. Желіні жүктеме және стресс-тестілеуді жүргізу
		Білімдер: 1. Қызмет көрсету сапасын қамтамасыз ету технологиялары 2. Брондау және теңгерімдеу хаттамалары 3. Өткізу қабілетін басқару әдістері 4. Желілерді жүктемелік тестілеу құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Тәуекелдерді бағалау және ЦТ архитектурасындағы нормативтік талаптарға сәйкестікті қамтамасыз ету	Дағды 1: АҚ тәуекелдерін талдау	Машықтар: 1. Қауіптер мен бұзушыларды модельдеу 2. Тәуекелдерді сапалық және сандық бағалауды жүргізу 3. Архитектуралық шешімдер үшін тәуекелдерге басымдық беріңіз 4. Өтемдік бақылау шараларын әзірлеу
		Білімдер: 1. Тәуекелдерді басқару әдістемелері 2. Ақпаратты қорғау саласындағы ҚР НҚА 3. Халықаралық стандарттар

	Дағдыны тану мүмкіндігі:	Қажет емес	
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Мақсаткерлік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық		
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 27033-Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Желілік қауіпсіздік (Network security) ISO/IEC 27031 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Қызметтің үздіксіздігіне дайындық бойынша нұсқаулық (Continuity readiness) ISO/IEC 27001/ISO / IEC 27002 — ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері және ақпараттық қауіпсіздікті басқару құралдары ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO / IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ 1073-2025 (" Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
27. Кәсіптің карточкасы "Кибер операцияларды жоспарлаушы":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-032		
Кәсіптің атауы:	Кибер операцияларды жоспарлаушы		
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:	Қажет емес		

Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы базалық (жоғары) білімі бар киберқауіпсіздік және кибер барлау саласындағы біліктілікті арттырудың қосымша бағдарламалары	
Кәсіптің басқа ықтимал атаулары:		
Қызметтің негізгі мақсаты:	Ресурстардың стратегияға сәйкес келуін қамтамасыз ететін кибер операциялар жоспарларын әзірлейді және үйлестіреді	
Еңбек функциялардың сипаттамасы		
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Стратегиялық және операциялық деңгейде кибер операцияларды жоспарлау 2. Әрекет нұсқаларын әзірлеу және салыстыру (COA) 3. Кибер операциялар бойынша жоспарлар мен нормативтік құжаттарды әзірлеу 4. Кибер операцияларды үйлестіру және бақылау
	Қосымша еңбек функциялары:	1. Жүргізілген кибер операцияның тиімділігін бағалау
Еңбек функциясы 1: Стратегиялық және операциялық деңгейде кибер операцияларды жоспарлау	Дағды 1: Кибер операцияның тұжырымдамасы мен дизайнын әзірлеу	Машықтар: 1. Кибероперацияның мақсаттары мен қалаған әсерлерін тұжырымдау 2. Саяси және құқықтық шектеулерді ескере отырып , кибер операцияның жоспарын әзірлеу 3. Жоспарды жоғары басшылықпен және тиісті күштермен үйлестіру 4. Жоспарды кибер операция жүргізуге бұйрық түрінде ресімдеу
		Білімдер: 1. Қазақстан Республикасының және жаудың киберкеңістігінде күштер мен құралдарды қолдану жөніндегі доктриналар 2. Әсерге бағытталған әдіс (ЭБА) әдістемелері 3. Киберкеңістіктегі халықаралық құқықтың құқықтық негіздері 4. Операциялық жоспарларды әзірлеудің құрылымы мен тәртібі
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Кибер операциялар ресурстарының басымдықтары мен бөлінуі	Машықтар: 1. CARVER матрицасын немесе соған ұқсасты пайдалана отырып, мақсаттарға басымдық беру 2. Операциялар арасында шектеулі ресурстарды бөлу 3. Нәтижеге жету үшін күштер мен құралдардың қажетті мөлшерін есептеу 4. Қосымша техникалық құралдар мен персоналға сұраныстарды жасау
		Білімдер: 1. CARVER әдістемесі немесе оның аналогтары 2. Киберкеңістікте шектеулі ресурстарды басқару принциптері

		3. Киберқұралдардың ұлттық арсеналының құрылымы мен мүмкіндіктері 4. Белгісіздік жағдайында шешім қабылдау теориясының негіздері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 2: Әрекет нұсқаларын әзірлеу және салыстыру (СОА)	Дағды 1: Әрекет нұсқаларын әзірлеу (СОА)	Машықтар: 1. Бір мақсат/мақсаттар тобы үшін кемінде үш техникалық мүмкін болатын іс-қимыл курсын (СОА) әзірлеу 2. Кибер жою тізбегі шеңберіндегі әрбір әрекет курсының кезеңдерін модельдеу 3. Уақыт терезелерін, анықтау тәуекелдерін және кепілдік зақымдануды қарастыру 4. Әрекеттер бағыттарын (СОА) диаграммалар мен матрицалар түрінде ұсыну
		Білімдер: 1. Кибероперацияларға бейімделген жоспарлау процесі 2. Іс-әрекет нұсқаларын әзірлеу және салыстыру әдістемелері (СОА) 3. Әрекеттерді синхрондау матрицасын құру принциптері 4. Кибер операцияларды модельдеу құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Әрекет нұсқаларын талдау және салыстыру (СОА)	Машықтар: 1. Тиімділік/тәуекелдер/ресурстар/уақыт критерийлері негізінде іс-әрекет нұсқаларына салыстырмалы талдау жүргізу 2. Іс-әрекеттің әрбір нұсқасының табысты болу ықтималдығы мен тәуекелдерін есептеу 3. Талдау нәтижелерін шешім қабылдау үшін басшылыққа ұсыну 4. Таңдалған әрекет нұсқасын (ӘҚ) түзету
		Білімдер: 1. Көп критериалды талдау және әрекет ету нұсқаларын салыстыру әдістері (ҚҚ) 2. Ойын теориясының негіздері және киберкеңістіктегі қақтығыстарды модельдеу 3. Кибероперациялардағы тәуекелдерді бағалау критерийлері 4. Таңдалған іс-әрекет нұсқасын бекіту тәртібі (СОА)
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Фазаларға бөлінген егжей-тегжейлі кибер операция жоспарын жасау

Еңбек функциясы 3: Кибер операциялар бойынша жоспарлар мен нормативтік құжаттарды әзірлеу	Дағды 1: Кибер операция жоспарын және синхрондау матрицасын құру	2. Барлық тартылған күштер мен құралдардың әрекеттерін синхрондау үшін матрицаны құру 3. Резервтік және төтенше жағдайдағы әрекеттердің нұсқаларын әзірлеу 4. Жоспарға қосымшаларды дайындау (бақылау схемалары, күштерді қолдану ережелері және т.б.)
		Білімдер: 1. Кибер операция жоспарының құрылымы мен талаптары 2. Киберкеңістікте синхрондау матрицасын құру принциптері 3. Киберкеңістікте операцияларды жүргізу циклі 4. Әкімшілік құжаттарды дайындауға қойылатын талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Кибероперациялардағы командалық және басқаруды дамыту	Машықтар: 1. Операция үшін икемді командалық және басқару инфрақұрылымын жобалау 2. Бастапқы және резервтік командалық және басқару арналарын анықтау 3. Сақтық командалық және басқару схемаларына көшу ережелерін әзірлеу 4. Операция алдындағы командалық және басқару жүйесін тестілеуді жүргізу
		Білімдер: 1. Белсенді қарсы іс-шаралар жағдайында ақауларға төзімді командалық басқару жүйелерін құру принциптері 2. Эксплойттар мен енгізілген құрылғыларды басқарудың заманауи хаттамалары мен құралдары 3. Қарсыластың басқару мен басқаруды бұзуына қарсы тұру әдістері 4. Басқару және басқару арналарын қорғауға қойылатын талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 1: Операцияға қатысушылардың өзара әрекеттесуін үйлестіру	Машықтар: 1. Мақсатты әзірлеу, қол жеткізу, пайдалану және қолдау топтарының қызметін үйлестіру 2. Мақсатты тағайындау мен барлау деректерін уақтылы беруді қамтамасыз ету 3. Бірыңғай кибер операциялық ортада бірлескен жұмысты ұйымдастыру 4. Командалар арасындағы басымдықтар мен ресурстар бойынша қайшылықтарды шешу
		Білімдер: 1. Киберкеңістікте ведомствоаралық ынтымақтастық қағидаттары

Еңбек функциясы 4: Кибер операцияларды үйлестіру және бақылау		2. Бірыңғай кибер операциялық ортаның құрылымы және оны басқару құралдары 3. Басқа құрылымдармен әрекеттерді үйлестіру тәртібі 4. Ресурстарды бөлу кезіндегі мүдделер қақтығысын басқару әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Операция барысын бақылау және жоспарды түзету	Машықтар: 1. Нақты уақытта операцияның орындалу барысын үздіксіз бақылауды қамтамасыз ету 2. Бизнеске келтірілген залалды бағалауды (BDA) жүргізу 3. Операцияны түзету немесе тоқтату туралы шешім қабылдау 4. Басшылық үшін аралық және қорытынды есептерді дайындау
		Білімдер: 1. Операциялық бақылау және киберопераціяларды басқару әдістері 2. Киберкеңістікте келтірілген залалды бағалау тәртібі 3. Киберопераціяның сәтті/сәтсіздігі критерийлері 4. Кибероперація бойынша қорытындыларды дайындау тәртібі
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Жүргізілген кибер операцияның тиімділігін бағалау	Дағды 1: Операцияның қол жеткізілген нәтижелері туралы мәліметтерді жинау және талдау	Машықтар: 1. Енгізілетін құрылғыларды пайдаланудан телеметрия мен журналдарды жинау 2. Қажетті нәтижелерге қол жеткізу дәрежесін бағалау 3. Нәтижелерге қол жеткізбеу себептерін анықтау 4. Киберзиянды бағалау (BDA) есептерін дайындау
		Білімдер: 1. Зиянды бағалау әдістемелері (BDA) және қайта шабуылдар бойынша ұсыныстар 2. Киберкеңістікте шабуыл нәтижелеріне қол жеткізу көрсеткіштері 3. Трафик пен журналды талдауға арналған құралдар 4. Кибер операцияларда алынған сабақтардың принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Жүйелі ойлау Күйзеліске тұрақтылық Тез шешім қабылдай білу Командада жұмыс істей білу Мақсаткерлік	

Жеке құзыреттерге қойылатын талаптар:	Тәртіптілік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық		
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 15408 (жалпы критерий) — ат қауіпсіздігін бағалау критерийлері ISO/IEC 27031:2011 — Guidelines for ICT readiness for business continuity ISO/IEC 27033 (серия) - Network security ҚР Ұлттық стандарттары: ҚР СТ ISO/IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO/IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ 1073-2025 ("ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар") ҚР СТ 4009-2025 ("Ақпараттық технологиялар. Ақпаратты криптографиялық қорғау. Блоктық симметриялық шифрлау алгоритмі")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
28. Кәсіптің карточкасы "Корпоративтік инфрақұрылым сәулетшісі":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-028		
Кәсіптің атауы:	Корпоративтік инфрақұрылым сәулетшісі		
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) it-білім болған кезде киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары		
Кәсіптің басқа ықтимал атаулары:	2521-2-001 - АТ-инфрақұрылым сәулетшілері		
Қызметтің негізгі мақсаты:	Бизнес мақсаттарын қауіпсіз технологиялық шешімдермен үйлестіре отырып, ат, ұйым архитектурасына қауіпсіздік талаптарын біріктіруді қамтамасыз етеді		
Еңбек функциялардың сипаттамасы			
		1. АҚ-ны ескере отырып, талаптарды талдау және мақсатты архитектураны әзірлеу	

Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	2. Киберқауіпсіздік шешімдерін корпоративтік инфрақұрылымға жобалау және интеграциялау 3. Тәуекелдерді бағалау және ЦТ архитектурасындағы нормативтік талаптарға сәйкестікті қамтамасыз ету
	Қосымша еңбек функциялары:	1. КҚ архитектурасының тиімділігін мониторингтеу
Еңбек функциясы 1: КҚ-ны ескере отырып, талаптарды талдау және мақсатты архитектураны әзірлеу	Дағды 1: Корпоративтік инфрақұрылымның мақсаттары мен талаптарын талдау	Машықтар: 1. Бизнес қажеттіліктерін анықтау үшін сұхбат жүргізу 2. Қауіпсіздік тәуекелдерін ескере отырып, бизнес-процестерді модельдеу 3. ЦТ инфрақұрылымына қойылатын негізгі талаптарды анықтау 4. Бизнес мақсаттарын технология мүмкіндіктерімен үйлестіру
		Білімдер: 1. Корпоративтік архитектураны құру әдістемесі 2. Бизнесті талдау және процестерді модельдеу 3. Тәуекелдерді басқару негіздері 4. ЦТ және бизнесті интеграциялау принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Мақсатты архитектураны әзірлеу	Машықтар: 1. Корпоративтік сәулет үлгілерін әзірлеу 2. Жобалау кезеңінде қауіпсіздік талаптарын біріктіру 3. Ағымдағы архитектурадан мақсатты архитектураға көшудің жол картасын жасаңыз 4. Алынған деректерді визуализациялау
		Білімдер: 1. Корпоративтік Инфрақұрылым шеңберлері 2. IT-шешімдерді модельдеу стандарттары 3. Инфрақұрылымға КҚ жүйелерін енгізу қағидаттары 4. Корпоративтік Инфрақұрылым технологиялары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 1: Қорғалған IT инфрақұрылымын жобалау	Машықтар: 1. Интеграцияланған КҚ жүйесімен архитектураны әзірлеу 2. Қорғаныс құралдарын біріктіру 3. Қауіпсіз бұлтты және гибридті инфрақұрылымдарды жобалау 4. Қол жеткізуді басқаруды ескере отырып, деректер ағындарын модельдеу
		Білімдер: 1. Қауіп модельдері 2. КҚ стандарттары

Еңбек функциясы 2: Киберқауіпсіздік шешімдерін корпоративтік инфрақұрылымға жобалау және интеграциялау		3. Қауіпсіздік технологиялары 4. Қауіпсіз даму принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Технологиялық шешімдерді таңдау және негіздеу	Машықтар: 1. Қауіпсіздік критерийлері бойынша жеткізушілер мен шешімдерді салыстыру 2. Қауіпсіз шешімдердің құны мен кірістілігін негіздеу 3. Техникалық сипаттамаларды әзірлеу
		Білімдер: 1. КҚ қаражатының нарығы (өнімдер және жетекші өндірушілер) 2. Қорғау шараларының тиімділігін бағалау әдістері 3. Техникалық сипаттаманы әзірлеу принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: АҚ-ны қолданыстағы жүйелерге интеграциялау	Машықтар: 1. Ағымдағы инфрақұрылымды осалдықтар бойынша бағалау 2. Қауіпсіздік деңгейін сақтай отырып, көші-қонды жоспарлау 3. Жобаларға қорғау шараларын енгізуді үйлестіру 4. Сәйкестік интеграциясын тексеру
		Білімдер: 1. КҚ жүйелерін бағалау әдістері 2. Интеграция құралдары 3. КҚ жүйелеріне қойылатын нормативтік талаптар 4. Бұлтты қауіпсіздік шеңберлері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Тәуекелдерді бағалау және ЦТ архитектурасындағы нормативтік талаптарға сәйкестікті қамтамасыз ету	Дағды 1: IT-архитектураның реттеуші және нормативтік сәйкестігін қамтамасыз ету	Машықтар: 1. Нормативтік талаптарға сәйкестігіне талдау жүргізу 2. Киберқауіпсіздік саясаты мен рәсімдерін әзірлеу 3. Аудит жүргізу үшін құжаттаманы дайындау 4. Цифрлық жүйелерді сертификаттау процестерін үйлестіру
		Білімдер: 1. Киберқауіпсіздік саласындағы ҚР НҚА 2. КҚ аудит стандарттары 3. Аудит үшін құжаттарды дайындау процестері 4. КВОИКАҒА қойылатын талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Қауіптер мен бұзушыларды модельдеу 2. Тәуекелдерді сапалық және сандық бағалауды жүргізу

	Дағды 2: КҚ тәуекелдерін талдау	3. Архитектуралық шешімдер үшін тәуекелдерге басымдық беріңіз 4. Өтемдік бақылау шараларын әзірлеу
		Білімдер: 1. Тәуекелдерді басқару әдістемелері 2. Ақпаратты қорғау саласындағы ҚР НҚА 3. Халықаралық стандарттар
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Ақ архитектурасының тиімділігін мониторингтеу	Дағды 1: Ақ архитектурасының тиімділігін мониторингтеу	Машықтар: 1. Қауіпсіздік саласындағы көрсеткіштер мен тиімділік көрсеткіштерін (KPI) теңшеңіз 2. Қауіпсіздік оқиғаларын және олардың архитектураға әсерін талдау 3. Архитектураға мерзімді шолулар жүргізу 4. Мониторинг нәтижелері негізінде жақсарту бойынша ұсынымдар қалыптастыру
		Білімдер: 1. Киберқауіпсіздік көрсеткіштері (MITRE att&CK, CIS Controls) 2. Бақылау құралдары (SIEM, осалдық сканерлері) 3. Үздіксіз жақсарту принциптері (PDCA) 4. Қауіп трендтері (CVE, қауіп аналитикасы)
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Мақсаткерлік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 27033-Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Желілік қауіпсіздік ISO/IEC 27002 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары (практика кодексі) ISO/IEC 27001 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар ISO/IEC 15408 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Архитектуралық компоненттердің қауіпсіздігін бағалау мәселелері (Common Criteria) ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO / IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ 1073-	

	2025 ("Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
29. 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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік бойынша қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	АҚ жоспарлау, бақылау, мониторинг және қамтамасыз ету		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Ұйымның КҚ басқару процестерін қарау 2. КҚ қамтамасыз ету процестерін жоспарлау 3. КҚ -ны қамтамасыз ету жөніндегі іс-шараларды жүзеге асыру 4. КҚ басқару және қамтамасыз ету процестерін бақылау	
	Қосымша еңбек функциялары:		
		Машықтар: 1. КҚ бойынша аналитикалық жұмысты үйлестіру 2. Тәуекелдерді, активтерді, инциденттерді, техникалық осалдықтарды, қатерлерді, қауіптерге техникалық қарсы іс-қимылдарды, бизнестің үздіксіздігін басқару процестерін қамтитын КҚ басқару процестерін бағалау және іске асыру әдістемелері мен әдістерін талдау, таңдау 3. КҚ басқару процестерінің ҒТҚ келісу	

Еңбек функциясы 1: Ұйымның КҚ басқару процестерін қарау	Дағды 1: КҚ басқару процестерін регламенттейтін нормативтік-техникалық құжаттаманы әзірлеу (өзектендіру)	4. КҚ саясатын, КҚ басқару үдерістерінің ҒТҚ және КҚ қамтамасыз ету үдерістерін регламенттейтін құжаттарды әзірлеу (өзектендіру) жөніндегі қызметті үйлестіру 5. Ұйымның бекітілген (өзектендірілген) КҚ саясатын қызметкерлердің назарына жариялау және жеткізу
		Білімдер: 1. Бизнес-процестерді реттеудің негізгі принциптері 2. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама 3. КҚ саласындағы ұлттық стандарттар 4. ЦЖ жобалау және пайдалану принциптері мен әдіснамалары 5. Бизнес-процестерді реттеу принциптері 6. Жобаларды басқару әдістері 7. КҚ тәуекелдерін бағалау және басқару әдістемелері 8. ЦЖ қауіптері мен осалдықтарын талдау әдістемесі 9. Ақпаратты өңдеуге байланысты активтерді жіктеу , есепке алу және таңбалау әдістері
	Дағдыны тану мүмкіндігі :	Талап етілмейді
	Дағды 2: КҚ қамтамасыз ету процестерін реттейтін ҒТҚ әзірлеу (өзектендіру)	Машықтар: 1. КҚ қамтамасыз ету процестерін реттейтін ҒТҚ-ның ағымдағы деңгейін бағалау 2. КҚ қамтамасыз ету процестерін реттейтін ТҚ әзірлеу (өзектендіру) 3. Ақпараттық-коммуникациялық инфрақұрылымның ЦЖ және компоненттері үшін қорғау бейіндері мен қауіпсіздік жөніндегі тапсырмаларды әзірлеу
		Білімдер: 1. Ұйымның бағдарламалық және аппараттық құралдарының қорғаныс механизмдерінің принциптері 2. КҚ басқару жүйесін құру принциптері 3. ЦЖ жобалау принциптері мен әдістемесі
	Дағдыны тану мүмкіндігі :	Талап етілмейді
	Дағды 1:	Машықтар: 1. Ақпаратты автоматтандырылған өңдеумен байланысты активтерді түгендеуді, жіктеуді, таңбалауды жүргізу 2. Активтерді санаттау нәтижелері бойынша есепті құжаттама жасау 3. КҚ қамтамасыз ету активтеріндегі кемшіліктерді анықтау
		Білімдер:

Еңбек функциясы 2: АҚ қамтамасыз ету процестерін жоспарлау	Киберқауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды жоспарлау	1. КҚ қамтамасыз ету саласындағы заңнама 2. КҚ қамтамасыз ету саласындағы ұлттық стандарттар 3. Бизнестің үздіксіздігі, КҚ оқиғаларын тіркеу және есепке алу, сақтық көшірме жасау, вирусқа қарсы қорғау, қол жеткізуді бақылау, алынбалы құралдармен, мобильді құрылғылармен жұмыс істеу , қашықтан қол жеткізу, криптография мен олардың тасымалдаушыларын пайдалану, лицензиялар мен нұсқалар бойынша іс-шараларды айқындау кезінде КҚ -ны қамтамасыз ету қағидаттары, әдістері мен құралдары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Ақпаратты автоматтандырылған өңдеумен байланысты бизнес-процестер мен активтер үшін тәуекелдерді, қауіптерді және ағып кету арналарын анықтау	Машықтар: 1. Ақпаратты автоматтандырылған өңдеумен байланысты бизнес-процестер мен активтер үшін тәуекелдерді, қауіптерді және ағып кету арналарын анықтау 2. АТҚ шеңберінде іс-шараларды жүзеге асыру 3. ЕТҚ құралдарында ЖЭСЖК бар-жоғына зерттеу жүргізу
		Білімдер: 1. Ақпараттың ағып кету арналарын анықтау әдістемесі мен құралдары 2. ҒТҚ, КҚ тәуекелдері мен қауіптерін анықтау әдістемесі 3. ААКТА бойынша ақпаратты ұстау әдістері 4. ЖЭСЖК бар-жоғына ЕТҚ құралдарын зерттеу әдістемесі 5. Декларацияланбаған техникалық мүмкіндіктердің болуына ЕТҚ құралдарына зерттеулер жүргізу әдістемесі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Ақпаратты автоматтандырылған өңдеумен байланысты бизнес-процестер мен активтердің қорғалуын талдау 2. КҚ қамтамасыз ету құралдары мен әдістерін таңдау 3. Ұйымның КҚ саясатын іске асыруға бағытталған іс-шараларды әзірлеу 4. Бизнестің үздіксіздігін және КҚ оқыс оқиғаларынан және форс-мажорлық жағдайлардан кейін қалпына келтіруді қамтамасыз ету бойынша жоспар жасау 5. Сатып алынатын КҚ қамтамасыз ету құралдарына техникалық ерекшеліктерді, тендерлік құжаттаманы әзірлеу

Еңбек функциясы 3: АҚ-ны қамтамасыз ету жөніндегі іс-шараларды жүзеге асыру	Дағды 1: АҚ-ны қамтамасыз ету жөніндегі іс-шаралар жоспарын іске асыру	6. ЦЖ КҚ кіші жүйелеріне қойылатын талаптарды, техникалық тапсырмаларды әзірлеу 7. Ақпараттық-коммуникациялық жүйе компоненттері мен ЦЖ 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. КҚ қамтамасыз ету саласындағы заңнама 4. КҚ қамтамасыз ету құралдары, осалдықтар мониторингі жүйелері, КҚ мониторингі жүйелері және ақпараттың жылыстауын болдырмау жүйелері, жүйелердің қорғау тетіктері 5. КҚ қамтамасыз ету саласындағы ұлттық стандарттар 6. ЦЖ қауіпсіздігін бағалау және талаптарды қалыптастыру тәсілдері 7. ЦЖ жобалау принциптері мен әдіснамасы 8. Ұйымның бағдарламалық және аппараттық құралдарының қорғау тетіктерін қолдану тәсілдері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: ЦЖ және ЦИ компоненттерінің қауіпсіздік функциялары параметрлерінің белгіленген талаптарға сәйкестігін бақылау	Машықтар: 1. ЦЖ 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 ЦЖ үшін қауіпсіздік бойынша тапсырмалар мен қорғау бейіндерінің іске асырылуын бақылауды жүзеге асырады.
		Білімдер: 1. КҚ құралдары мен әдістерін әзірлеу, тестілеу және байқаудан өткізу бойынша жұмыстарды орындаудың базалық қағидаттары мен тәсілдері 2. Бағдарламалық құралдарды, қорғау тетіктерін, ЦЖ және ЦИ компоненттерін пайдалану қағидалары 3. Баптаулардағы бұзушылықтарды анықтау әдістері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. КҚ -ны қамтамасыз ету жөніндегі іс-шаралар жоспарының іске асырылуын бақылауды жүзеге асыру 2. Ұйымдағы КҚ басқару процестерін КҚ және ҒТҚ қамтамасыз ету процестерін реттейтін құжаттар

Еңбек функциясы 4: КҚ басқару және қамтамасыз ету процестерін бақылау	Дағды 1: Киберқауіпсіздік процестерінің сәйкестігін бағалау	талаптарының орындалуын тексеру нәтижелерін талдау 3. Ұйым қызметкерлерімен құпиялылық туралы келісімдерді әзірлеуге немесе ақпаратты жария етпеуге қатысу мердігерлер және үшінші тараптар
		Білімдер: 1. СЖ-да және оларға кіріктірілген қорғау тетіктерінде әкімшілік ету қағидаттары мен құралдары 2. КҚ қамтамасыз ету АЖЖ жұмыс істеу қағидаттары 3. Жасақтау және қолдану қағидаттары, осалдықтар мониторингі жүйелері, КҚ мониторингі жүйелері 4. Ақпараттың жылыстауын болдырмау жүйелері 5. КҚ инциденттерін, сыни (авариялық) жағдайларды анықтау, алдын алу және салдарын жою әдістері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: ҚББЖ және бейнебақылау жүйелерінің жұмыс істеуін әкімшілендіру және мониторингілеу	Машықтар: 1. Әкімшілендіру ҚББЖ және бейнебақылау жүйелері 2. Жұмыс істеуіне мониторинг жүргізу ҚББЖ және бейнебақылау жүйелері 3. Қабылданған шешімдердің КҚ-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	
	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:	
	7	Ақпараттық қауіпсіздік жөніндегі маман	
30. Кәсіптің карточкасы "Кибер заң кеңесшісі":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-019		
Кәсіптің атауы:	Кибер заң кеңесшісі		
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Негізгі (жоғары) заңгерлік білімі бар киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша бағдарламалары		
Кәсіптің басқа ықтимал атаулары:	2611 - Заңгерлер		
Қызметтің негізгі мақсаты:	Киберқауіпсіздіктің құқықтық және реттеуші аспектілері, заңдарды, саясаттарды және этикалық стандарттарды сақтау бойынша сараптаманы қамтамасыз ету		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. КҚ саласындағы құжаттарды әзірлеу және құқықтық сараптама жүргізу 2. КҚ мәселелері бойынша ұйымдар мен жеке тұлғалардың мүдделерін білдіру 3. КҚ саласындағы деректермен жұмыс	
	Қосымша еңбек функциялары:	1. Қызметкерлерді киберқауіпсіздік мәселелері бойынша құқықтық сауаттылыққа үйрету	
	Дағды 1:	Машықтар: 1. Құжаттардың дұрыстығын тексеру үшін заманауи технологияларды және ашық ресурстарды пайдалану 2. Құжаттар мен сұраныстарды қалыптастыру үшін заманауи технологияларды және ашық ресурстарды пайдалану	

	Заманауи электрондық ресурстарды пайдалану	3. Контрагенттерді тексеру үшін аналитикалық жүйелерді қолдану
		Білімдер: 1. Электрондық платформаларды пайдалану ережелері, сондай-ақ алынған деректерге шектеулер 2. Электрондық ресурстарды тиімді пайдалану үшін қажетті деректер 3. Әртүрлі құжаттар түрлерінің мазмұнына заңнамалық талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 1: КҚ саласындағы құжаттарды әзірлеу және құқықтық сараптама жүргізу	Дағды 2: Құқықтық қорытындылар мен құқықтық ұсыныстарды дайындау	Машықтар: 1. Құжаттардағы заңға қайшы келетін, оның ішінде киберқауіпсіздік саласындағы ережелерді анықтау 2. Құжаттардағы тараптардың мүдделерінің теңгерімін бұзатын ережелерді анықтау 3. Киберқауіпсіздікке қатысты құқықтық құжаттар мәтінінің нақты нәтижеге сәйкестігін бағалау 4. Мәмілелерді жасасу туралы келіссөздер кезінде келіспеушілік хаттамаларын жасау
		Білімдер: 1. Азаматтық заңнама және оны тұлғалар, мәмілелер, мүліктік құқықтар туралы ережелер, сондай-ақ міндеттемелер туралы жалпы ережелер бөлігінде қолдану тәжірибесі 2. Азаматтық заңнама және оны жасау, орындау, тоқтату туралы ережелер, сондай-ақ шарттарды бұзудың салдары бөлігінде қолдану тәжірибесі 3. Азаматтық заңнама және оның міндеттемелердің жекелеген түрлері бойынша ережелер бөлігінде қолдану тәжірибесі
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: Киберқауіпсіздік саласындағы құжаттарды әзірлеу	Машықтар: 1. Киберқауіпсіздік саласындағы қатынастарды ресімдейтін келісімдерді әзірлеу және қарау 2. Киберқауіпсіздікке және жеке деректерді қорғау заңнамасына қатысты жергілікті нормативтік құқықтық актілерді әзірлеу 3. Іскерлік хат алмасу
		Білімдер: 1. Киберқауіпсіздік саласын реттеу бөлігінде әкімшілік заңнама және оны қолдану тәжірибесі 2. Құқықтық құжаттарды әзірлеуге қойылатын талаптар; қажетті реквизиттер тізбесі 3. Құжаттардың әртүрлі түрлерінің мазмұнына қойылатын заңнамалық талаптар 4. Құжат айналымы ережелері
	Дағдыны тану мүмкіндігі:	Қажет емес

Еңбек функциясы 2: АҚ мәселелері бойынша ұйымдар мен жеке тұлғалардың мүдделерін білдіру	Дағды 1: Келіссөздер жүргізу функцияларын жүзеге асыру	Машықтар: 1. Келіссөздер кезіндегі құқықтық және техникалық тәуекелдерді анықтау 2. Өз ұстанымыңызды қорғау үшін келіссөздер жүргізу әдістерін қолдану 3. Келіссөздердің барысын жазып алу
		Білімдер: 1. Іс жүргізу заңнамасы және оның тәжірибеде қолданылуы 2. Талап қою мерзімдерін есептеу ережелері 3. Талап арыздар мен талап-арыздарға жауаптар беру ережелері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Киберқауіпсіздік саласындағы шағымдармен жұмыс	Машықтар: 1. Талаптарды, арыздарды, жауаптарды, шағымдарды және басқа да іс жүргізу құжаттарын дайындау 2. Өсімпұлдар мен залалды өтеу мөлшерін есептеу 3. Көрсетілген талаптардың негіздері мен сомасын растайтын құжаттарды жинау 4. Позицияны нығайту үшін ауызша баяндама дайындау
		Білімдер: 1. Талап қою ісін жүргізу қағидалары 2. Сот актілерін қайта қарау жөніндегі іс жүргізу қағидалары 3. Атқарушылық іс жүргізу және оны қолдану тәжірибесі туралы заңнама 4. Келіссөздер жүргізу және ауызша баяндау әдістемесі
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 1: Жеке және құпия деректердің қауіпсіздігін қамтамасыз ету	Машықтар: 1. Цифрлық жүйелердегі жеке және құпия деректерді анықтау 2. Заңнамаға және ішкі саясатқа сәйкес қауіпсіздік шараларын қолдану 3. Құпиялықты бұзу қаупін бағалау және оларды азайту жолдарын ұсыну 4. Деректерді қорғау жөніндегі ішкі ережелер мен саясаттарды әзірлеуге және қолдауға қатысу
		Білімдер: 1. Дербес деректерді қорғау туралы заңнама 2. Ақпаратты қорғау әдістері мен құралдары 3. Ақпаратты жіктеу және санаттау 4. Жеке және құпия деректердің қауіпсіздігіне қатер
	Дағдыны тану мүмкіндігі:	Қажет
		Машықтар:

Еңбек функциясы 3: АҚ саласындағы деректермен жұмыс	Дағды 2: Киберқауіпсіздік инциденттерінің деректерін талдау және өңдеу	1. Киберқауіпсіздік инциденттерін анықтау және жіктеу 2. Оқиғалар журналдарын, желілік трафикті және басқа деректер көздерін талдау 3. Оқиғаларды талдау нәтижелері бойынша есептер мен ұсыныстарды жасау 4. Арнайы құралдарды (SIEM, IDS/IPS, криминалистикалық құралдар) пайдалану
		Білімдер: 1. Киберқауіпсіздік инциденттерін жіктеу негіздері және олардың сипаттамалары 2. Оқиға деректерін жинау және корреляциялау әдістері 3. Оқиғаларды тергеу және сандық криминалистика негіздері 4. Оқиғаларды тіркеуге және өңдеуге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет
Қосымша еңбек функциясы 1: Қызметкерлерді киберқауіпсіздік мәселелері бойынша құқықтық сауаттылыққа үйрету	Дағды 1: Қызметкерлерді киберқауіпсіздік мәселелері бойынша құқықтық сауаттылыққа үйрету	Машықтар: 1. Құпия сөзді басқару, электрондық пошта қауіпсіздігі, фишингтік шабуылдар, әлеуметтік инженерия, зиянды бағдарламалардан қорғау және деректерді қорғау сияқты тақырыптар бойынша қызметкерлер үшін киберқауіпсіздік бойынша оқыту бағдарламаларын әзірлеу 2. Презентациялар, оқулықтар және практикалық жаттығулар сияқты әртүрлі әдістерді қолдана отырып, қызметкерлерді оқыту 3. Оқыту бағдарламаларының тиімділігін бақылау және бағалау
		Білімдер: 1. Презентацияларды өткізу әдістері мен принциптері 2. Әртүрлі оқыту әдістемелері 3. Кәсіби деңгейді бағалау, мамандарды аттестациялау әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
	Халықаралық стандарттар: ISO/IEC 27001 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар ISO/IEC 27002 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары (практика кодексі) ISO/IEC 27005 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	тәуекелдерін басқаруға қойылатын талаптар ISO/IEC 29100 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Privacy framework. Құпиялылық және дербес деректерді қорғау ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO / IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ 1073-2025 ("Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
31. Кәсіптің карточкасы "Уәкілетті өкіл/авторландыруға жауапты":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-027		
Кәсіптің атауы:	Уәкілетті өкіл/авторландыруға жауапты		
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) басқарушылық білім болған кезде киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Орналастыру алдында қауіпсіздік стандарттарына сәйкестігін қамтамасыз ете отырып, қолайлы тәуекел деңгейінде пайдалану үшін ЦТ жүйелерін бағалайды және бекітеді		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. КҚ қамтамасыз ету және деректермен жұмыс 2. Тәуекелдің қолайлы деңгейін қамтамасыз ету үшін IT жүйелеріндегі авторизация механизмдерін бағалау 3. Авторизацияны және қауіпсіздік стандарттарына сәйкестікті бағалау негізінде ЦТ жүйелерін бекіту	

	Қосымша еңбек функциялары:	1. Киберқауіпсіздік тәуекелдерін азайту
Еңбек функциясы 1: АҚ қамтамасыз ету және деректермен жұмыс	Дағды 1: Киберқауіпсіздікті кешенді қамтамасыз ету және қорғалған жүйелерді басқару	Машықтар: 1. Артефактілерді, журналдарды, жад қоқыстарын, жүйелік іздерді жинау және талдау 2. Құпия сөз саясатын, қауіпсіздік топтарын, көп факторлы аутентификацияны басқарыңыз 3. Топтық саясатты, пайдаланушы құқықтарын, брандмауэр ережелерін қолданыңыз 4. КҚ жүйелеріне аудит және тестілеу жүргізу
		Білімдер: 1. Цифрлық жүйелерді басқару және қорғау негіздері 2. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары 3. Қауіпсіздік жүйелерін талдау, аудит және тестілеу принциптері 4. Бағдарламалау тілдері
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 2: Киберқауіпсіздік оқиғаларының деректерін талдау және өңдеу	Машықтар: 1. Киберқауіпсіздік оқиғаларын анықтау және жіктеу 2. Оқиғалар журналдарын, желілік трафикті және басқа деректер көздерін талдаңыз 3. Оқиғаларды талдау нәтижелері бойынша есептер мен ұсынымдар қалыптастыру 4. Арнайы құралдарды қолданыңыз (SIEM, IDS / IPS , forensic-құралдар)
		Білімдер: 1. Киберқауіпсіздік оқиғаларын жіктеу негіздері және олардың ерекшеліктері 2. КҚ оқиғалары туралы деректерді жинау және корреляциялау әдістері 3. Инциденттерді тергеу және цифрлық криминалистика негіздері 4. КҚ инциденттерін тіркеуге және өңдеуге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 1:	Машықтар: 1. Авторизацияны жүзеге асыру кезінде жиі кездесетін қателіктерді анықтаңыз 2. Талаптардың өзгергіштігінің рұқсатсыз қол жеткізу тәуекелдеріне әсерін бағалау 3. Динамикалық авторизациясы бар жүйелерде қолжетімділік аудиті тетіктерінің болуын тексеру 4. Артық құқықтар болған кезде туындайтын ықтимал осалдықтарды талдау
		Білімдер:

Еңбек функциясы 2: Тәуекелдің қолайлы деңгейін қамтамасыз ету үшін IT жүйелеріндегі авторизация механизмдерін бағалау	Авторизацияны іске асырумен байланысты тәуекелдерді анықтау	1. Авторизацияны жобалау және іске асыру кезінде туындайтын қателер 2. Аудиттеуді қамтамасыз ету принциптері 3. Авторизация модельдерінің өнімділігі мен масштабталуына байланысты тәуекелдер 4. Тәуекелдерді азайту үшін минималды құқықтар мен есепке алу талаптары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Қол жеткізуді басқару модельдерін талдау	Машықтар: 1. Авторизация модельдерінің арасындағы айырмашылықтарды анықтаңыз (RBAC, ABAC, PBAC, MAC, DAC) 2. Таңдалған авторизация моделінің ЦТ жүйесінің нақты бизнес талаптарына сәйкестігін бағалау 3. Күрделі жүйелер үшін авторизация модельдерінің комбинацияларын анықтаңыз 4. Жүйені жобалау кезінде авторизация мен бизнес логикасының бөлінуін тексеріңіз
		Білімдер: 1. Авторизацияның негізгі модельдері және олардың принциптері (RBAC, ABAC/PBAC, MAC, DAC) 2. Динамикалық модельдердің артықшылықтары мен кемшіліктері 3. Құқықтардың ең аз жеткіліктілігіне және қол жеткізуді кері қайтарып алуға қойылатын талаптар 4. Авторизация модельдерінің жүйенің жұмысына әсері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Авторизацияны және қауіпсіздік	Дағды 1: Авторизацияның қауіпсіздік талаптарына сәйкестігін тексеру	Машықтар: 1. Авторизацияның бизнес және киберқауіпсіздік талаптарымен интеграциясын бағалау 2. Жүйені бекітпес бұрын қол жетімділіктің аудиті мен мониторингін тексеріңіз 3. Ұсынылған шешімдердегі икемділік (PBAC) мен өнімділік (ACL) арасындағы тепе-теңдікті анықтаңыз 4. Динамикалық авторизация модельдері үшін қосымша журналдардың қажеттілігін анықтаңыз
		Білімдер: 1. Авторизация модельдерін таңдау және біріктіру тәжірибесі 2. Авторизация жүйелеріндегі аудитке және мониторингке қойылатын талаптар 3. Авторизацияның ЦТ жүйесінің жалпы қауіпсіздігіне әсері 4. Жүйенің пайдалануға дайындығын бағалау стандарттары

стандарттарына сәйкестікті бағалау негізінде ЦТ жүйелерін бекіту	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Авторландыру тәуекелдерін ескере отырып, IT-жүйені пайдалануды бекіту туралы шешім қабылдау	Машықтар: 1. Авторизация механизмдерімен байланысты қалдық тәуекелдердің жарамдылығын бағалау 2. Қанауды бекіту шарттарын тұжырымдау 3. Тәуекелдерді азайту үшін авторизация механизмдеріндегі түзетулерді үйлестіру 4. Авторизацияны талдау негізінде тәуекелді қабылдаудың негіздемесін құжаттау
		Білімдер: 1. Қол жеткізуді басқару контекстіндегі қолайлы тәуекел деңгейін бағалау принциптері 2. ЦТ жүйесін бекіту процесінде авторизацияның рөлі 3. Авторизация тәуекелдерін азайту әдістері 4. Бекітілгеннен кейін ЦТ жүйесінің құжаттамасына және мониторингіне қойылатын талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Киберқауіпсіздік тәуекелдерін азайту	Дағды 1: Тәуекелдерді азайту жөніндегі шараларды әзірлеу	Машықтар: 1. Тәуекелдерді азайту стратегияларын жобалау 2. КҚ саласында тәуекелдерді азайтудың техникалық шараларын енгізу 3. Қызметкерлерді киберқауіпсіздік мәселелері бойынша оқыту 4. Енгізілген шаралардың тиімділігін бағалау
		Білімдер: 1. КҚ тәуекелдерін азайту стратегиялары 2. Техникалық қарсы шаралар 3. Хабардарлықты арттыру бағдарламалары 4. Тиімділік көрсеткіштері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Мақсаткерлік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
	Халықаралық стандарттар: ISO/IEC 27001 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар ISO/IEC 27002 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Қол жеткізуді бақылау және сәйкестендіру (ақпараттық қауіпсіздікті қамтамасыз ету шаралары бойынша практика кодексі) ISO/IEC 24760 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Сәйкестендіру және қол жетімділікті басқару ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ 1073-2025 ("Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар") ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
32. Кәсіптің карточкасы "Көлік инфрақұрылымы бойынша ақпараттық қауіпсіздік жөніндегі маман":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-016		
Кәсіптің атауы:	Көлік инфрақұрылымы бойынша 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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) ЦТ білімі бар киберқауіпсіздік саласындағы кәсіби біліктілікті арттырудың қосымша бағдарламалары		
Кәсіптің басқа ықтимал атаулары:	2524-0-007 - Ақпараттық қауіпсіздік жөніндегі маман		
Қызметтің негізгі мақсаты:	Рұқсат етілмеген араласуды болдырмау үшін көлік құралдарын қорғауды қамтамасыз ету. Әуе, құрлық және өзен көлігіндегі бұйрықтар мен тәртіп бұзушылықтар.		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Тасымалдау процестерін басқару және бақылау үшін қауіпсіздік жүйелері мен желілік құрылғыларды сынау 2. Көлік саласының маңызды ерекшеліктерін ескере отырып, киберқауіпсіздік стандарттарын әзірлеу және енгізу 3. Киберқауіпсіздік инциденттеріне жауап беру	
	Қосымша еңбек функциялары:	1. Қызметкерлерді киберқауіпсіздік саясаты мен процедуралары бойынша оқыту	
		Машықтар: 1. Ұйымның қауіпсіздік жүйесіндегі әлсіз жақтарды анықтау үшін тұрақты осалдықты және	

		эксплуаттарды сканерлеуді (SIEM құралдарын қоса) жоспарлаңыз және орындаңыз 2. Қауіпсіздік жүйелеріне ену сынақтарын жүргізу 3. Тәуекел деңгейлерін бағалау үшін осалдықты сканерлеу нәтижелерін пайдаланыңыз 4. Осалдықтарды немесе тәуекелдерді жою бойынша ұсыныстарды әзірлеу
	Дағды 1: Бағдарламалық құралды тексеру	Білімдер: 1. Python, BASH, Java, Ruby және Perl сияқты пентест және бағдарламалау тілдерінің негіздері 2. РК-ге ден қою жөніндегі ағымдағы ұйымдастыру саясаты мен рәсімдері 3. РК анықтау және алдын алудың стандартты салалық құралдары 4. Қалыпты емес белсенділіктің идентификациялық сипаттамалары 5. NIDS, NIPS, HIDS және HIPS қондырғылары мен параметрлері 6. РК анықтау туралы есептерді жасау үшін қажетті құжаттама 7. Белгілі осалдықтарды жоймас бұрын оның құпиялылығын сақтау үшін жаңа осалдықтар туралы ақпаратты басқару 8. Кәсіпорындардың архитектуралары мен желілерінде NIDS / nips өнімдерін жобалау кезінде датчиктерді дұрыс орналастыру 9. РК анықтау жүйелеріне қызмет көрсету және конфигурациялау 10. Siem құралдарын пайдаланып осалдықтарды сканерлеуді орындау 11. Қорғаныс мониторингін қолдана отырып, желідегі немесе жүйедегі қалыптан тыс әрекеттерді анықтау 12. Көлік саласындағы ерекшеліктерді ескере отырып, жүйелер мен осалдықтардың қауіпсіздігін талдаудың бағдарламалық құралдары мен әдістері 13. Көлік кешені объектілерінің жұмыс істеуінің құқықтық, инженерлік-техникалық, ұйымдастырушылық мәселелерін түсіну
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Қауіптерді анықтау үшін кешенді бақылау және мониторинг жүргізу 2. Ықтимал бұзушылықтарды табу және анықтау үшін қауіп деректерін талдау нәтижелерін пайдаланыңыз 3. Тәулік бойы қорғау мониторингін қоса алғанда, ҚҚ анықтау және алдын алу жүйелерін орнатуды, пайдалануды және оларға қызмет көрсетуді жүзеге асыру

Еңбек функциясы 1: Тасымалдау процестерін басқару және бақылау үшін қауіпсіздік жүйелері мен желілік құрылғыларды сынау	Дағды 2: Желіні бақылау, қауіпсіздік қатерлерін ерте анықтау	4. Желілік ресурстарға аномальды белсенділік пен ықтимал қауіптерді анықтау үшін желілік трафик деректерін талдау және сипаттау
		Білімдер: 1. РК анықтау және алдын алудың стандартты салалық құралдары 2. РК-ге ден қою жөніндегі ағымдағы ұйымдастыру саясаты мен рәсімдері 3. Қалыпты емес белсенділіктің идентификациялық сипаттамалары 4. Қорғаныс мониторингін қолдана отырып, желідегі немесе жүйедегі қалыптан тыс әрекеттерді анықтау 5. Белгілі осалдықтарды жоймас бұрын оның құпиялылығын сақтау үшін жаңа осалдықтар туралы ақпаратты басқару 6. Энергетика саласындағы ерекшеліктерді ескере отырып, жүйелер мен осалдықтардың қорғалуын талдаудың бағдарламалық құралдары мен әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: Көлік инфрақұрылымына тән осалдықтарды талдау және бағалау	Машықтар: 1. Көлік желілерін қорғау үшін брандмауэрлерді және IDS/IPS орнату және пайдалану 2. Мамандандырылған құралдарды қолдана отырып, желілік трафикті бақылау және талдау 3. Көлік объектілеріне бейімделген қол жеткізуді бақылау және Бейнебақылау жүйелерін басқару 4. Криптографиялық жабдықтар мен шифрлау технологияларын енгізу және сүйемелдеу 5. Деректерді қауіпсіз бөлісу үшін желілік сегменттеу мен VPN конфигурациясы және қолдауы 6. Киберқауіпсіздік оқиғаларын талдау және оларға жауап беру үшін SIEM жүйелерін пайдалану 7. Мамандандырылған жабдықтардың қауіпсіздігіне диагностика және тестілеу жүргізу 8. Көлік инфрақұрылымының қауіпсіздік жүйелерін резервтеуді және істен шығуға орнықтылықты қамтамасыз ету 9. Жабдыққа техникалық қызмет көрсету рәсімдері мен нәтижелерін құжаттау
		Білімдер: 1. Көлік жүйелеріне бейімделген өнеркәсіптік деңгейдегі брандмауэрлердің (firewalls) жұмыс принциптері мен архитектурасы 2. Көлік желілеріндегі интрузияны анықтау және алдын алу жүйелерінің (IDS/IPS) ерекшеліктері 3. Көлік объектілеріндегі қолжетімділікті бақылау және бейнебақылау технологиялары

		4. Көлік коммуникацияларының ерекшеліктерін ескере отырып, желілік трафикті бақылау және талдау хаттамалары (NetFlow, SNMP, Wireshark) 5. Көлік инфрақұрылымындағы деректерді шифрлауға арналған криптографиялық қорғау және жабдық принциптері 6. Қауіпсіздік оқиғаларын басқару жүйелерімен (SIEM) жұмыс істеу және оларды көлік жүйелеріне біріктіру 7. Бөлінген инфрақұрылымдардағы желілерді сегменттеу және оқшаулау әдістері (VLAN, VPN) 8. Сыни компоненттердің ақауларға төзімділігі мен резервтеуін қамтамасыз етуге арналған техникалық шешімдер 9. Көлік саласындағы КҚ стандарттары мен нормативтері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 1: РК алдын алуға арналған желілік қауіпсіздік жүйесін қашықтан орнату және жаңарту	Машықтар: 1. Жүйенің бағдарламалық жасақтамасы мен аппараттық құралдарын үнемі жаңартып отырыңыз 2. Вирусқа қарсы бағдарламалық құралды орнатыңыз және жаңартыңыз 3. Өнеркәсіптік желі түйіндері үшін желіаралық қалқандарды конфигурациялаңыз 4. Жаңартуларды енгізу алдында өнеркәсіптік бағдарламалық құралмен үйлесімділігін тексеріңіз
		Білімдер: 1. Өндірістік желі түйіндерінің жұмысы 2. Шифрлау және криптография 3. Саясат, талаптар, орнату принциптері және бағдарламалық құрал жаңартулары 4. Брандмауэр жұмысы, қолданбасы және конфигурациясы 5. Желіаралық қалқандағы рұқсат етілген трафикті анықтау үшін ACL критерийлерін конфигурациялау
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Киберқауіпсіздіктің ағымдағы ұйымдастырушылық рәсімдерін және көлік объектілеріне тән талаптарды анықтау 1. Ішкі және салалық стандарттарға сәйкес көлік инфрақұрылымының қолданыстағы кибер операцияларының тиімділігіне талдау жүргізу 2. Көлік саласында қолданылатын талаптар мен нормативтерді ескере отырып, талдау нәтижелерін құжаттау 3. Көлік құралдары мен желілерден қорғауды қамтамасыз ететін киберқауіпсіздік жүйелерін енгізу және сүйемелдеу

Еңбек функциясы 2: Көлік саласының маңызды ерекшеліктерін ескере отырып, киберқауіпсіздік стандарттарын әзірлеу және енгізу	Дағды 2: Тәуекелдерді азайту үшін қауіпсіздік хаттамалары мен процедураларын әзірлеу, енгізу және қолдау	4. Көлік инфрақұрылымында кибер операцияларды тиімді жүзеге асыру үшін қауіпсіздік рәсімдерінің, қызмет көрсетуді бұзудың және міндеттердің қажетті жаңартуларын анықтау және құжаттау 5. Көлік саласының ерекшеліктерін ескере отырып, операциялық және талдамалық процестерді, сондай-ақ инциденттер бойынша есептілік рәсімдерін енгізу
		Білімдер: 1. Көлік объектілері мен жүйелеріне бейімделген техникалық, өндірістік және ұйымдастырушылық құжаттаманы дайындау және жүргізу 2. Көлік саласының белгіленген стандарттарына сәйкес ресімделген егжей-тегжейлі талдаумен, қорытындылармен және ұсынымдармен құжаттама жасау 3. Көлік жүйелері саласындағы терең салалық және техникалық білім, олардың ерекшелігі мен пайдалану ерекшеліктерін ескере отырып 4. Көлік шешімдері мен қауіпсіздік жүйелерін әзірлеу және қолдау үшін бағдарламалау тілдерін (C , C., PHP, Python, JavaScript) меңгеру
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: IoT жүйелері үшін қауіпсіздікті енгізу	Машықтар: 1. Стандартты шаблондар мен құралдарды қолдана отырып, КҚ оқиғаларын тіркеу, жіктеу және басымдықтарды анықтау 2. Қауіпсіздік инциденттері бойынша құжаттаманы жүргізу 3. IoT құрылғыларының инфрақұрылымы мен көлік құралдарына қосылуын анықтау 4. IoT қауіпсіздігінің ауытқулары мен оқиғаларын анықтаңыз 5. Ақпаратты жинау және IOT соңғы нүктелерінің қауіпсіздік мәселелерін терең талдау, диагностикалау және жою 6. IoT қауіпсіздік мәселелерін анықтау процестеріне тұрақты техникалық қызмет көрсетуді орындау 7. It бойынша мониторинг және есеп беру ақпараттық панельдерін жобалау және әзірлеу 8. Барлық IoT деңгейлеріндегі маңызды осалдықтарды сканерлеу 9. Қауіпсіздік құрылғыларының сақтық көшірмесін жасаңыз және шифрлау
		Білімдер: 1. Бақылау бақылау тақтасын әзірлеу 2. Деректерді бағдарламалау және визуализация тілдері (Python, R, SQL, NodeJS) 3. Шифрлау және криптография негіздері 4. АҚ-ны қолдау жөніндегі ұйымдастыру саясаты, рәсімдері мен нұсқаулықтары

		5. КҚ рәсімдерін құжаттау және енгізу үшін деректермен алмасу рәсімдері 6. Қауіпсіздікті бақылау үшін қол жетімді стандартты шаблондар мен құралдардың спектрі 7. IoT жүйелеріндегі желінің, құрылғылардың, конфигурацияның және қосылудың негізгі топологиялары 8. Құрылғыларды, бұлттарды, коммуникацияларды, дерекқорларды және қолданбаларды қоса алғанда, әртүрлі IoT қауіпсіздік контексттері мен деңгейлері, қамту 9. Киберқауіпсіздік инциденттеріне әрекет етудің әдеттегі операциялық процедуралары It 10. Киберқауіпсіздік осалдықтары мен оқиғаларын жою It 11. IoT жүйелерінде киберқауіпсіздік деңгейін арттыруды енгізу 12. IoT жүйелеріндегі ауытқуларды анықтау және талдау, жүйелік аудит хаттамалары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 1: Ұйымдық қауіпсіздік процедураларына сәйкес оқиғаларды тану және оларға әрекет ету	Машықтар: 1. Киберқауіпсіздік оқиғаларының пайда болуы мен сипатын анықтау және растау 2. Киберқауіпсіздік оқиғаларына қатысты заңнамалық талаптарды, ұйымдастырушылық саясатты, процедураларды және әрекет ету жоспарларын анықтау 3. Оқиғаның көздерін, әсері мен салдарын талдау және бағалау 4. Оқиғаға жауап беру жоспарын іске қосыңыз және кибер оқиғаның локализацияланғанын растау 5. Ұйымның маңызды жүйелік инфрақұрылымының зақымдануын немесе деректердің бұзылуын бағалау 6. Киберқауіпсіздік оқиғасын, қабылданған әрекеттерді, шешімдерді және нәтижелерді құжаттау
		Білімдер: 1. Киберқауіпсіздік оқиғаларына жауап беру жоспарларының негізгі ерекшеліктері және олардың көздері мен себептері 2. Шабуылдардың әртүрлі түрлері, соның ішінде қызмет көрсетуден бас тарту (DoS), SQL инъекциялары(Sql), сайтаралық сценарий шабуылдары (XSS), аппараттық шабуылдар, WiFi шабуылдары 3. Киберқауіпсіздік оқиғаларын анықтау әдістемесі, алдын алу шаралары және азайту әдістері 4. КҚ оқиғалар журналын құжаттау және талдау процестері 5. Киберқауіпсіздік инциденттеріне әрекет етудің ұйымдастырушылық саясаты мен рәсімдері (

		инциденттердің сипаты мен орналасқан жерін анықтау, инциденттерді оқшаулау, қауіпсіздік патчтарын орнату және желіге кіруді өшіру, хабарлау және қажетті персоналға есептер беру)
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Киберқауіпсіздік инциденттеріне жауап беру	Дағды 2: Ұйым үшін қолданыстағы киберқауіпсіздік стандарттарын, саясаттары мен нұсқауларын енгізу	Машықтар: 1. Ұйымның миссиясы мен мақсаттарына сәйкес келетін киберқауіпсіздік саясаты мен нұсқаулығын енгізіңіз 2. Ұйымның деректері мен жүйелерін зиянкестерден қорғау үшін қолданыстағы қауіпсіздік стандарттарын қолданыңыз 3. Оқиғаларды тиімді басқару үшін оқиғаларға жауап беру жоспарлары мен процедураларын әзірлеу және қолдау 4. Ұйымның киберқауіпсіздік тәуекелдерін бағалау және осы тәуекелдерді азайту стратегияларын әзірлеу 5. Ұйымның киберқауіпсіздік саясаты мен нұсқауларының өзектілігін қамтамасыз ету үшін қауіпсіздік тенденциялары мен туындайтын қауіптерді бақылау және талдау
		Білімдер: 1. Жетілдірілген желілік қауіпсіздік мүмкіндіктері 2. Энергетика саласының ерекшеліктерін ескере отырып, киберқауіпсіздік стандарттарын енгізуге қолданылатын ұйымдастырушылық бизнес-процестер 3. Белгіленген стандарттар мен талаптарды құжаттау 4. Желілік қауіпсіздік инфрақұрылымының талаптары мен сипаттамаларын белгілеу 5. Техникалық қызмет көрсету және хабарлау процестерін белгілеу 6. Желілік қауіпсіздік инфрақұрылымына жоспарлы тексерулер жүргізу 7. КҚ тестілеу әдістері мен процедуралары 8. Ұйымдағы қауіпсіздік тәуекелдері және тәуекелге төзімділік 9. Ұйымда желілік қауіпсіздік инфрақұрылымын енгізу бойынша салалық стандарттар мен ережелер 10. Энергетика объектілерінің жұмыс істеуінің құқықтық, инженерлік-техникалық, ұйымдастырушылық мәселелерін түсіну
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Кибершабуылға қатысты дәлелдерді, соның ішінде журналдарды, кэшті, файлдарды және басқа

	Дағды 3: Киберқауіпсіздік оқиғаларын бағалау және хабарлау	сандық артефактілерді жинау, тасымалдау және сақтау 2. Атқарушы басшылықты, кибер-криминалистерді және ЦТ командаларын қоса алғанда, ішкі мүдделі тараптармен жұмыс істеу 3. Кибершабуылдар туралы ақпаратты құқық қорғау органдарына беру
		Білімдер: 1. Құқық қорғау органдарына киберқауіпсіздік оқиғалары туралы хабарлауға арналған ішкі хаттамалар 2. Құпия деректерді өңдеу (кибершабуылдардың дәлелдемелерін жинау, шифрлау, сақтау және жіберу)
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Қызметкерлерді киберқауіпсіздік саясаты мен процедуралары бойынша оқыту	Дағды 1: Қызметкерлерді киберқауіпсіздік саясаты мен процедуралары бойынша оқыту	Машықтар: 1. Парольдерді басқару, электрондық пошта қауіпсіздігі, фишингтік шабуылдар, әлеуметтік инженерия, зиянды бағдарламалардан қорғау және деректерді қорғау тақырыптары бойынша қызметкерлерге арналған Киберқауіпсіздік бойынша оқыту бағдарламаларын әзірлеу 2. Презентация, оқыту бағдарламалары және практикалық сабақтар ретінде әртүрлі әдістерді қолдана отырып, қызметкерлерге арналған тренингтер өткізу 3. Оқу бағдарламаларының тиімділігін бақылау және бағалау
		Білімдер: 1. Презентацияларды өткізу тәсілдері мен принциптері 2. Оқытудың әртүрлі әдістері 3. Ақпаратты техникалық қорғау бойынша ғылыми зерттеулер, әзірлемелер жүргізу әдістері елде және шетелде техникалық барлау және ақпаратты қорғау саласындағы ғылым мен техниканың жетістіктері 4. Ақпараттың қауіпсіздігін қамтамасыз ету жөніндегі мамандарды аттестаттау, кәсіби деңгейін бағалау әдістері 5. Еңбек заңнамасының, ішкі еңбек тәртібінің, еңбек қауіпсіздігі және еңбекті қорғау, өндірістік санитария, өрт қауіпсіздігі талаптарының тәртібі
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Аналитикалық ойлау Бастамашылық	
	Халықаралық стандарттар: ISO/IEC 27033 - Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Желілік қауіпсіздік (Network security)	

Техникалық регламенттер мен ұлттық стандарттардың тізімі:	ISO/IEC 27031 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Қызметтің үздіксіздігіне дайындық бойынша нұсқаулық (Continuity readiness) ISO/IEC 27001/ISO / IEC 27002 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері және ақпараттық қауіпсіздікті басқару құралдары ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO / IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ 1073-2025 (" Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
33. 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-коммуникациялық технологиялар	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:	Қажет емес		
Формалды емес және информалы біліммен байланыс:			
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Оқиғаларды талдау және тергеу компьютерлік ақпарат қол сұғушылық объектісі ретінде, компьютер қылмыс жасау құралы ретінде, сондай-ақ кез-келген сандық дәлел ретінде		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Компьютерлік қылмыстарды тергеу 2. Сандық құрылғылар мен жабдықтардың криминалистикалық сараптамасы	

	Қосымша еңбек функциялары:	
Еңбек функциясы 1: Компьютерлік қылмыстарды тергеу	Дағды 1: Компьютерлік қылмыстарға алғашқы жауап	Машықтар: 1. Оқиғалардың көздері мен себептерін анықтаңыз 2. Анықталған оқиғалардың салдарын бағалау 3. Корпоративтік желіге енуді анықтау 4. Зиянкестердің ұйым желісіне кіруінің барлық белгіленген тәсілдерін жою 5. Оқиғаның пайда болу механизмі мен жағдайларының құрылымын талдау 6. Бағдарламалық жасақтаманың өзгеру себебі мен шарттарын анықтаңыз 7. Белгілі бір дереккөзге жататындығын анықтауға мүмкіндік беретін ақпараттың қасиеттері мен белгілерін бөлектеңіз 8. Қолда бар ақпараттың жүйеде орналасуына сәйкестьстігін анықтау
		Білімдер: 1. Компьютерлік қылмыстардың негізгі түрлері 2.Ұйымның желісіне зиянкестердің кіру жолдары 3. Ұйымның ЦЖ-дағы Ақпарат қауіпсіздігінің негізгі қауіптері және бұзушы модельдері 4. Ақпарат беру жүйелері мен желілерін құру және жұмыс істеу принциптері 5. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттар 6. Ақпараттың "ағып кетуінің" техникалық арналары 7. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 8. Ашық жүйелердің өзара әрекеттесуінің эталондық моделі, негізгі хаттамалар, заманауи жергілікті және ғаламдық компьютерлік желілердің құрылысы мен жұмыс істеу кезеңдерінің реттілігі мен мазмұны 9. Цифрландырудың техникалық құралдарына техникалық қызмет көрсетуді ұйымдастыру мен жүргізудің негізгі әдістері 10. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары 11. Анықталған оқиғаларды есепке алу регламенті 12. Талданатын компьютерлік жүйеде ақпаратты сақтау форматтары 13. Компьютерлік жүйелерде қолданылатын негізгі файл пішімдері 14. Компьютерлік қылмыстардың, құқық бұзушылықтар мен инциденттердің іздерін тіркеу және құжаттау тәртібі Компьютерлік ақпарат саласындағы қылмыстық және әкімшілік құқық нормалары
	Дағдыны тану мүмкіндігі:	Қажет емес

		Машықтар: 1. Бұзушылықтардың алдын алу және уақтылы анықтау шараларын әзірлеу 2. Компьютерлерде құмды ақпаратты іздеу 3. Қарсы криминалистиканың әдістері мен құралдарын анықтау: толық дискіні шифрлау, ақпаратты қашықтан сақтау және т. б. 4. Дәлелдемелік базаны жинауды және оны ресімдеуді/сақтауды жүзеге асыру 5. Ұйымға нақты шабуылды модельдеу және одан болатын зиянды азайту бойынша шаралар қабылдау дағдыларын үйрету
	Дағды 2: Бұзушылықтар мен рұқсатсыз кірудің алдын алу шараларын жоспарлау	Білімдер: 1. Ақпарат беру жүйелері мен желілерін құру және жұмыс істеу принциптері 2. Ашық жүйелердің өзара әрекеттесуінің эталондық моделі, негізгі хаттамалар, заманауи жергілікті және ғаламдық компьютерлік желілердің құрылысы мен жұмыс істеу кезеңдерінің реттілігі мен мазмұны 3. Ақпаратты қорғау саласындағы ұлттық, мемлекетаралық және халықаралық стандарттар 4. Ұйымның АЖ-дағы Ақпарат қауіпсіздігінің негізгі қауіптері және бұзушы модельдері 5. Қарсы криминалистиканың әдістері мен құралдары 6. Техникалық арналар бойынша "ағып кетуден" ақпаратты қорғау құралдарын құру қағидаттары 7. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 8. АЖ-да ақпаратты қорғау үшін қолданылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар 9. Компьютерлік техниканы алудың негізгі принциптері 10. Анықтамалық деректерді табудан жасыру әдістері. 11. Тергеу бойынша ақпаратты құжаттау
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Киберқауіпсіздік оқиғаларын тергеу 2. Оқиға уақытын белгілеңіз 3. Компьютерлік құрылғының бастапқы диагностикасын жүргізу 4. Аппараттық жазу блокаторларымен және ақпарат тасымалдағыштардың телнұсқаларымен жұмыс істеу 5. Криминалистикалық талдау үшін дистрибутивтермен жұмыс жасаңыз. 6. Қатты дискінің кескінін (бірдей көшірмесін) және басқа да ақпарат тасымалдағыштарын, соның ішінде

	Дағды 1: Компьютерлік криминалистикалық сараптама	кескінді қатты дискінің бөлімінен немесе жеке секторынан алып тастауды жүргізу 7. Қалыптасқан диск кескіндерін өңдеу 8. Қатты дискілерден деректерді жинауды жүзеге асыру 9. Қатты дискілерде табылған файлдарды талдаңыз. 10. Файлдардан деректерді шығару. 11. ЖЖҚ қоқыстарын зерттеу. 12. Қатты дискіде және периферияда артефактілерді іздеңіз 13. Операциялық жүйелер мен қолданбалы бағдарламалардың жүйелік журналдарымен және журналдарымен жұмыс істеу 14. Жойылған деректерді қалпына келтіріңіз 15. Дәлелдемелік базаны жинауды және оны ресімдеуді/сақтауды жүзеге асыру
		Білімдер: 1. Файлдық жүйелер туралы негізгі білім 2. Операциялық жүйелер туралы негізгі білім 3. Киберқауіпсіздіктің негізгі принциптері және қорғаныс құралдарының жұмыс әдістері 4. Компьютерлік криминалистика құралдары 5. Қатты дискілер мен басқа дискілердің құрылғысы 6. Операциялық жүйелердің архитектурасы және пайдаланушы интерфейстері 7. Есептеу жүйелерінің архитектурасы, құрылысы және жұмыс істеуі 8. Деректерді қалпына келтіруді қоса, файлдық жүйемен жұмыс істеуге арналған құралдар жинағы 9. Ақпаратты қорғауды қамтамасыз ету үшін қолданылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 2: Сандық құрылғылар мен жабдықтардың криминалистикалық сараптамасы	Дағды 2: Желілік құрылғылардың криминалистикалық сараптамасы	Машықтар: 1. Желілік стек пен браузерлерге талдау жасаңыз 2. Электрондық пошта хабарламаларына талдау жасаңыз және электрондық пошта мекен-жайының байланысын орнатыңыз 3. Желілік трафиктің қоқысын құруға арналған құралдармен жұмыс жасаңыз 4. Желілік трафикті ұстау және зерттеу 5. Веб-серверлердің журналдарын зерттеу 6. IP-мекен-жайға тиесілі және орналасқан жерді орнатыңыз 7. Домендік атаудың тиесілігін орнатыңыз
		Білімдер: 1. Ақпарат беру жүйелері мен желілерін құру және жұмыс істеу принциптері 2. Ашық жүйелердің өзара әрекеттесуінің эталондық моделі, негізгі хаттамалар, заманауи жергілікті және

		ғаламдық компьютерлік желілердің құрылысы мен жұмыс істеу кезеңдерінің реттілігі мен мазмұны 3. Компьютерлік желілердегі сәйкестендірудің, аутентификацияның және авторизацияның үлгілік әдістері мен хаттамалары 4. Желілік сот сараптамасын жүргізудің негізгі принциптері 5. Талдау жүргізу үшін барынша толық ақпарат алу мақсатында қызметкерлердің іс-қимыл регламенті 6.Желілік криминалистиканы жүргізуге арналған типтік деректер көздері және оларды зерттеу 7. Желілік трафик қоқысын құруға арналған құралдар жинағының ерекшеліктері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: Мобильді құрылғылардың криминалистикалық сараптамасы	Машықтар: 1. Ұялы байланыс құрылғысын сәйкестендіруді жүзеге асыру 2. Барлық деректерді сандық құрылғыдан, периферияльық жабдықтардан және ақпарат жинақтағыштардан клондауды жүзеге асыру 3. Ұялы телефондардан ақпарат алуды жүзеге асыру 4. SIM-картадан ақпарат алуды жүзеге асыру 5. Ішкі және сыртқы жад картасынан ақпарат алу 6. Пошта жөнелтілімдерін, телеграфтық және өзге де хабарламаларды бақылауды жүзеге асыру 7. 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 құралдар 3. Ақпаратты қорғауды қамтамасыз ету үшін қолданылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар 4. Мобильді операциялық жүйелер туралы негізгі білім 5. Мобильді құрылғылардың файлдық жүйелері туралы негізгі білім 6. Жады картасының құрылғысы
	Дағдыны тану мүмкіндігі:	Қажет емес
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:	
34. Кәсіптің карточкасы "Білім менеджері":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-030		
Кәсіптің атауы:	Білім менеджері		
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) педагогикалық білім болған кезде деректер базасын құру және әзірлеу саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Қызметкерлердің маңызды ақпаратқа қол жеткізуін қамтамасыз ете отырып, ұйым ішіндегі білімді жинау, бөлісу және басқару жүйелерін әзірлейді		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Компанияның негізгі білім базасын жинау және жаңарту 2. Білім қорын әзірлеу және қолдау және кіріс ақпаратын басқару 3. Білім беру мен алмасуды ұйымдастыру және үйлестіру	
	Қосымша еңбек функциялары:	1. Білімді басқару жүйесінің тиімділігін бақылау	
		Машықтар: 1. Әр түрлі көздерден негізгі ережелерді, шаблондар мен анықтамалықтарды анықтаңыз және жинаңыз 2. Негізгі құжаттарды өзектендіруді қамтамасыз ету	

Еңбек функциясы 1: Компанияның негізгі білім базасын жинау және жаңарту	Дағды 1: Негізгі білім қорын жинау және жаңарту	3. Байланыс деректері бар мердігерлер мен серіктестердің тізілімін жүргізу 4. Ақпараттың тұтастығын және қайталанбауын бақылау
		Білімдер: 1. Ұйымның негізгі білімдерін анықтау және жіктеу әдістері 2. Құжаттарды версиялау және өзгерістерді бақылау принциптері 3. Корпоративтік құжаттаманы сақтау стандарттары (ISO 15489) 4. Файлдарды өңдеу және сақтау құралдары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Динамикалық білім базасын жинау және жаңарту	Машықтар: 1. Динамикалық білімді үнемі жинау процестерін ұйымдастыру 2. Динамикалық ақпараттың өзектілігіне мерзімді аудит жүргізу 3. Ескірген материалдар туралы хабарлау тетіктерін енгізу 4. Пішіндер мен интеграциялар арқылы деректерді ішінара жинау мен жаңартуды автоматтандыру
		Білімдер: 1. Динамикалық білім алу әдістері 2. Білімнің өмірлік циклінің принциптері 3. Процестер мен рәсімдердегі өзгерістерді бақылау құралдары 4. Қызметкерлерді мазмұнды үнемі жаңартуға тарту тәсілдері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 2:	Дағды 1: Пайдаланудың қарапайымдылығы үшін білім қорының құрылымын әзірлеу және оңтайландыру	Машықтар: 1. Білім қорының бөлімдері мен бөлімдерінің логикалық құрылымын жобалау 2. Тегтер, метадеректер және толық мәтінді іздеу жүйелерін енгізу 3. Нысаналы бөлімдердің өкілдерімен ыңғайлылықты тестілеуді өткізу 4. Пайдалану аналитикасына негізделген құрылымды оңтайландыру
		Білімдер: 1. Ақпараттық архитектура және дерекқор принциптері; 2. Таксономияны, онтологияны және тегтеуді құру әдістері 3. Корпоративтік жүйелердегі навигация және іздеу стандарттары 4. Қызметкерлердің әртүрлі рөлдері үшін ақпараттың қолжетімділігіне қойылатын талаптар

Білім қорын әзірлеу және қолдау және кіріс ақпаратын басқару	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Білім қорындағы ақпараттың сапасы мен қолжетімділігін қамтамасыз ету	Машықтар: 1. Мазмұнды модерациялау және бекіту ережелерін әзірлеу және енгізу 2. Пайдаланушы рөліне байланысты кіру құқықтарын теңшеңіз 3. Үлгілерді анықтау үшін шолу және іздеу статистикасын талдаңыз 4. Білім жүйесінің ыңғайлылығы туралы Қызметкерлердің пікірлерін жинау және ескеру
		Білімдер: 1. Мазмұн сапасын басқару принциптері 2. Қол жетімділік пен құпиялылықты шектеу саясаты 3. Дерекқорды талдау құралдары 4. Білім жүйесін пайдаланушылардан кері байланыс әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Білім беру мен алмасуды ұйымдастыру және үйлестіру	Дағды 1: Білім беру процестерін ұйымдастыру	Машықтар: 1. Менторлық және жұптық оқыту бағдарламаларын әзірлеу 2. Қызметкерлерді ауыстыру кезінде білім беру сессияларын ұйымдастыру 3. Берілген білімді бекіту үшін шаблондар жасаңыз 4. Жаңадан бастаушыларға тәлімгерлерді тағайындауды үйлестіру
		Білімдер: 1. Білім беру модельдері 2. Бейімделу бағдарламаларын құру принциптері 3. Тәжірибелі қызметкерлерден жаңадан бастаушыларға білім беруді ынталандыру тәсілдері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Оқыту іс-шараларын өткізу	Машықтар: 1. Ақпараттық платформаларда сабақтар ұйымдастыру 2. Білімді тексеру үшін материал әзірлеу 3. Оқытудан кейінгі құзыреттілік деңгейінің өзгеруін бағалау 4. Бейне сабақтар мен интерактивті материалдар жасаңыз
		Білімдер: 1. Интерактивті оқыту платформалары 2. Оқыту нәтижелерін бағалау әдістері 3. Игерілетін материалды құру принциптері
	Дағдыны тану мүмкіндігі:	Қажет емес

Қосымша еңбек функциясы 1: Білімді басқару жүйесінің тиімділігін бақылау	Дағды 1: Ұйымның білімді басқару жүйесін бағалау және жетілдіру	Машықтар: 1. Білім қорын пайдалану нәтижелерін теңшеу және талдау 2. Жүйенің сапасы туралы қызметкерлерге тұрақты сауалнама жүргізу 3. Қиындықтарды анықтаңыз және жақсарту жоспарларын жасаңыз 4. Талдау негізінде жаңа функциялар мен құралдарды енгізу
		Білімдер: 1. Негізгі тиімділік көрсеткіштері 2. Кері байланыс жинау әдістері және пайдаланушылардың мінез-құлқын талдау 3. Білімді басқару модельдері 4. Білімді басқару және AI құралдары саласындағы заманауи трендтер
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Мақсаткерлік Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 27001 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. ISO/IEC 27002 талаптары - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару құралдары (ақпараттық қауіпсіздікті қамтамасыз ету шаралары бойынша тәжірибе кодексі) ISO/IEC 27004 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. ISO/IEC 27003 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік менеджменті жүйесін енгізу бойынша нұсқаулық (Implementation guidance) ҚР Ұлттық стандарттары: ҚР СТ ISO/IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ ISO/IEC 27002-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару құралдары") (егер бейімделген болса) ҚР СТ ISO/IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
35. Кәсіптің карточкасы "Құқық қорғау/сот сараптамасы және қарсы барлау талдаушысы":		
Топтың коды:	2524-0	
Қызмет атауының коды:	-	
Кәсіптің атауы:	Құқық қорғау/сот сараптамасы және қарсы барлау талдаушысы	

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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Негізгі (жоғары) заңгерлік білімі бар киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша бағдарламалары.		
Кәсіптің басқа ықтимал атаулары:	2611-1-003 - Заңгер		
Қызметтің негізгі мақсаты:	Заңды тергеулер мен қарсы барлау операцияларын қолдау үшін цифрлық дәлелдемелерді жинау және талдау		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Киберқауіпсіздік инциденттеріне сот сараптамасын жүргізу және талдау 2. Сандық деректер мен цифрлық жүйелерді техникалық және қарсы барлау талдауы 3. Киберқауіпсіздік саласындағы деректермен жұмыс	
	Қосымша еңбек функциялары:	1. Қызметкерлерді ақпараттық қауіпсіздік мәселелері бойынша құқықтық сауаттылыққа үйрету	
Еңбек функциясы 1:	Дағды 1: Цифрлық сараптаманың процессуалдық және құқықтық негіздері	Машықтар: 1. Сандық дәлелдемелердің тұтастығына нұқсан келтірмей жинау, жазу және сақтау 2. Сараптамалық қорытындыларды дайындау және тергеу нәтижелерін сотқа ұсыну 3. Цифрлық сараптама процедураларын әзірлеу және енгізу 4. Тергеу нәтижелерін логикалық және заңды түрде дұрыс нысанда ұсыну	
		Білімдер: 1. Қазақстан Республикасының қылмыстық, іс жүргізу және әкімшілік заңнамасы 2. Сот-сандық сараптаманың принциптері мен стандарттары 3. Цифрлық сот сараптамасындағы халықаралық стандарттар мен этикалық нормалар	
	Дағдыны тану мүмкіндігі:	Қажет	

Киберқауіпсіздік инциденттеріне сот сараптамасын жүргізу және талдау	Дағды 2: Киберқауіпсіздік инциденттерінің деректерін талдау және өңдеу	Машықтар: 1. Киберқауіпсіздік инциденттерін анықтау және жіктеу 2. Оқиғалар журналдарын, желілік трафикті және басқа деректер көздерін талдау 3. Оқиғаларды талдау нәтижелері бойынша есептер мен ұсыныстарды жасау 4. Арнайы құралдарды (SIEM, IDS/IPS, криминалистикалық құралдар) пайдалану
		Білімдер: 1. Киберқауіпсіздік инциденттерін жіктеу негіздері және олардың сипаттамалары 2. Оқиғалар туралы деректерді жинау және корреляциялау әдістері 3. Оқиғаларды тергеу және цифрлық криминалистика негіздері 4. Инциденттерді тіркеу және өңдеуге қойылатын нормативтік талаптар
	Дағдыны тану мүмкіндігі:	Қажет
Еңбек функциясы 2: Сандық деректер мен цифрлық жүйелерді техникалық және қарсы барлау талдауы	Дағды 1: Сандық тасымалдаушылар мен жүйелерді техникалық талдау	Машықтар: 1. Бағдарламалық және аппараттық құралдарды пайдаланып сандық медианы талдау 2. Мобильді құрылғылардан деректерді шығару 3. Оқиғалардың уақыт кестесін әзірлеу 4. Тасымалдаушыдан алынған деректерді талдау үшін құралдарды пайдалану
		Білімдер: 1. Криминалистика және құқықтық информатика негіздері 2. Операциялық жүйелердің жұмыс істеу принциптері (Windows, Linux, macOS, Android, iOS) 3. Файлдық жүйе құрылымдары (NTFS, FAT, ext4, APFS және т.б.) 4. Қатты дискілерді, мобильді құрылғыларды және желі деректерін талдау әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Сандық криминалистиканың көмегімен қарсы барлау қызметін жүзеге асыру	Машықтар: 1. Жойылған немесе шифрланған деректерді қалпына келтіру және түсіндіру 2. Зиянды файлдар мен сценарийлерді талдау 3. Криптоталдау және шифрды шешу құралдарымен жұмыс істеу 4. Сандық және физикалық кеңістіктегі кибершабуыл көздерін анықтау
		Білімдер: 1. Киберқауіпсіздік және қарсы барлау принциптері 2. Жойылған немесе шифрланған деректерді қалпына келтіру әдістері

		3. Кері инженерия және зиянды бағдарламаларды талдау негіздері 4. Криптографиялық қорғау және деректерді шифрды шешу әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 3: Аналитикалық және қарсы барлау қызметі	Машықтар: 1. Желі журналдары мен қауіпсіздік оқиғаларын талдау 2. Әртүрлі көздерден алынған деректерді салыстыру (журналдар, хат алмасу, метадеректер) 3. Субъектілер арасындағы байланыстарды анықтау үшін OSINT әдістерін қолдану 4. Қарсы барлау талдау әдістерін қолдану
		Білімдер: 1. Желілік хаттамалар және оларды талдау әдістері (TCP/IP, HTTP/S, DNS және т.б.) 2. Анонимизацияға және деректерді қорғауға қарсы әрекет ету әдістері 3. SIEM жүйелерінің жұмыс істеу принциптері 4. OSINT, HUMINT, TECHINT талдауының негіздері
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 3: Киберқауіпсіздік саласындағы деректермен жұмыс	Дағды 1: Деректермен жұмыс	Машықтар: 1. Әртүрлі көздерден деректерді жинау және өңдеу 2. Деректерді жою және түрлендіру 3. Талдау жүргізу және нәтижелерді түсіндіру 4. Деректерді визуализациялау және ұсыну
		Білімдер: 1. Статистика және математикалық деректерді талдау негіздері 2. Деректерді жинау, дайындау және жою әдістері 3. Талдау және визуализация құралдары 4. Мәліметтер базасы және деректер құрылымдары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Жеке және құпия деректердің қауіпсіздігін қамтамасыз ету	Машықтар: 1. Цифрлық жүйелердегі жеке және құпия деректерді анықтау 2. Заңнамаға және ішкі саясатқа сәйкес қауіпсіздік шараларын қолдану 3. Құпиялықты бұзу қаупін бағалау және оларды азайту жолдарын ұсыну 4. Деректерді қорғау жөніндегі ішкі ережелер мен саясаттарды әзірлеуге және қолдауға қатысу.
		Білімдер: 1. Дербес деректерді қорғау туралы заңнама 2. Ақпаратты қорғау әдістері мен құралдары

		3. Ақпаратты жіктеу және санаттау 4. Жеке және құпия деректердің қауіпсіздігіне қатер
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Қызметкерлерді киберқауіпсіздік мәселелері бойынша құқықтық сауаттылыққа үйрету	Дағды 1: Қызметкерлерді құқықтық сауаттылыққа үйрету	Машықтар: 1. Құпия сөзді басқару, электрондық пошта қауіпсіздігі, фишингтік шабуылдар, әлеуметтік инженерия, зиянды бағдарламалардан қорғау және деректерді қорғау сияқты тақырыптар бойынша қызметкерлер үшін киберқауіпсіздік бойынша оқыту бағдарламаларын әзірлеу 2. Презентациялар, оқулықтар және практикалық жаттығулар сияқты әртүрлі әдістерді қолдана отырып, қызметкерлерді оқыту 3. Оқыту бағдарламаларының тиімділігін бақылау және бағалау
		Білімдер: 1. Презентацияларды өткізу әдістері мен принциптері 2. Әртүрлі оқыту әдістемелері 3. Кәсіби деңгейді бағалау, мамандарды аттестациялау әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Дербестік және жауапкершілік Жүйелі ойлау Күйзеліске тұрақтылық Командада жұмыс істей білу Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 15408 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері (Common Criteria) ISO/IEC 27001 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. ISO/IEC 27037/ISO/IEC 27038 талаптары - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Сандық сот сараптамасы. Цифрлық дәлелдемелерді жинау, талдау және сақтау бойынша ұсыныстар ҚР Ұлттық стандарттары: ҚР СТ ISO/IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен іс-әрекеттері ерекшелігінің құрылымы") ҚР СТ ISO/IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала белгіленген пакеттері") ҚР СТ ISO/IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ 1073-2025 ("ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:

36. 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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік бойынша қосымша кәсіби біліктілікті арттыру курстары		
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:		
	Дағды 1: 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. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама 5. Қазіргі заманғы деректерді шифрлау жүйелерінің құрылысы және жұмыс істеуі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 1: Деректерді шифрлау жүйелерін пайдалану	Дағды 2: Деректерді шифрлау жүйелерінің жұмысын басқару	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 жетілдіру және арттыру жөнінде ұсыныстар әзірлеу 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 архитектурасы, құрылысы және жұмыс істеуі 2. Желілік протоколдар 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. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар 8. Қазіргі заманғы деректерді шифрлау жүйелерінің құрылысы және жұмыс істеуі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Деректерді шифрлау жүйесінің бағдарламалық-аппараттық құралдарының жұмыс істеу параметрлерін анықтау 2. Деректерді шифрлау жүйелерінің бағдарламалық-аппараттық құралдарының тиімділігін бағалау әдістемелерін әзірлеу

Еңбек функциясы 2: Деректерді шифрлау жүйелерінің қауіпсіздік деңгейін бағалау	Дағды 1: Деректерді шифрлау жүйелерінің жұмыс қабілеттілігі мен тиімділігіне бақылау тексерулерін жүргізу	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 жүйелерінің бағдарламалық-аппараттық құралдарын құру принциптері 3. Ақпаратты шифрлау алгоритмдерін бағдарламалық іске асырудың дұрыстығы мен тиімділігін бағалау әдістері мен құралдары 4. Ықтимал 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 талдау 2. КҚ 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 бойынша талдамалық есепті 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	
	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. 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	
37. 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:			
Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы қосымша кәсіби біліктілікті арттыру курстары		
Кәсіптің басқа ықтимал атаулары:			
Қызметтің негізгі мақсаты:	Қауіпсіздік деңгейлерін анықтау бойынша аудиторлық тексеру жүргізу		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Киберқауіпсіздік тәуекелдерін бағалау және талдау 2. Аудиторлық тапсырманың міндеттерін қамтамасыз ету 3. Аудиторлық тапсырманың міндеттерін орындау	
	Қосымша еңбек функциялары:		
		Машықтар: 1. Қауіптерді анықтау және бағалау үшін тәуекелдерді талдау әдістерін қолданыңыз 2. Цифрлық жүйелердегі тәуекелдерді азайту және осалдықтарды жою бойынша кешенді стратегияларды әзірлеу	

Еңбек функциясы 1: Киберқауіпсіздік тәуекелдерін бағалау және талдау	Дағды 1: Қауіптерді анықтау және бағалау үшін тәуекелдерді талдау әдістерін қолдану	3. Ықтимал қауіптердің ұйымға әсерін бағалау, тәуекелдерді азайту жоспарларын әзірлеу
		Білімдер: 1. Тәуекелдерді талдау әдістері, соның ішінде сапалық және сандық әдістер 2. Тәуекелдерді басқару және оларды азайту принциптері 3. Тәуекелдерді талдау және осалдықтарды бағалау құралдары мен технологиялары 4. Тәуекелдерді талдаудың заманауи әдістемелері, соның ішінде қауіптерді болжау үшін Big Data пайдалану
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2: Тәуекелдер мен қажеттіліктерді бағалау негізінде қауіпсіздік саясатын әзірлеу және енгізу	Машықтар: 1. Ұйым үшін қауіпсіздік саясатын, стандарттарын және ақпаратты қорғау процедураларын әзірлеу 2. Стандартталған қауіпсіздік процестерін енгізу, оларды ұйымның қажеттіліктеріне бейімдеу 3. Саясатты үнемі жаңарту арқылы ұйымдағы қауіпсіздік мәдениетін қалыптастыру және қолдау
		Білімдер: 1. Киберқауіпсіздік саясатын әзірлеу принциптері мен тәсілдері 2. Қауіпсіздік саясатын әзірлеу және енгізу саласындағы ұлттық стандарт 3. Корпоративтік инфрақұрылым деңгейіндегі ақпаратты қорғау технологиялары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: АҚ аудитін әдістемелік қамтамасыз ету	Машықтар: 1. Аудиторлық қызметті регламенттейтін әдістемелік және ұйымдастырушылық-өкімдік құжаттарды әзірлеуге (өзектендіруге) қатысу 2. Әдістемелік және ұйымдастырушылық-өкімдік құжаттардың тұсаукесерлерін өткізу 3. Қызметкерлерді регламенттеуші құжаттамамен таныстыруды жүргізу
		Білімдер: 1. Әдістемелік және ұйымдастырушылық-өкімдік құжаттарды әзірлеу, ресімдеу және бекіту тәртібі 2. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар 3. КҚ аудитін қамтамасыз етудің әдістемелік құжаттарымен персоналды таныстырудың тиімді әдістері
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар:

Еңбек функциясы 2: Аудиторлық тапсырманың міндеттерін қамтамасыз ету	Дағды 2: АҚ аудитін ұйымдастырушылық қамтамасыз ету	1. КҚ аудиті мәселелері бойынша тексерілетін ұйымның (бөлімшенің) өкілдерімен өзара іс-қимылды ұйымдастыруға қатысу 2. Ақпаратты сақтау, қол жеткізу және беру тәртібі мәселелері бойынша басшылық құжаттарды (бұйрықтар, өкімдер, нұсқаулықтар) жинауды жүзеге асыру 3. КҚ аудитін жүргізу
		Білімдер: 1. Іскерлік коммуникацияның кезеңдері мен формалары 2. Іскерлік ортадағы қарым-қатынас принциптері мен ережелері 3. КҚ аудитін жүргізу тәртібі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: Ұйымның барлық деңгейлерінде қауіпсіздік мәселелері бойынша кеңес беру	Машықтар: 1. Қызметкерлерді деректерді қорғау әдістеріне және қауіпсіз жұмыс ортасын құруға үйрету 2. Қауіпсіздік саясатын сақтау мәселелері бойынша кеңес беру, ақпараттық технологияларды қауіпсіз пайдалану бойынша ұсыныстар жасау 3. Ағымдағы қауіптер мен олардың алдын алу әдістері туралы басшылыққа үнемі кеңес беру
		Білімдер: 1. Деректерді қорғау принциптері, қауіпсіздік стандарттарының сақталуын бақылау әдістері 2. Қызметкерлерге арналған психология және қауіпсіздік талаптары 3. Ұйымдағы қауіпсіздік саясатын құру және қолдау процестері мен процедуралары
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 1: Есепті дайындау және нәтижелерді сыртқы және ішкі аудиторларға ұсыну	Машықтар: 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. Цифрландыру 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 КҚ аудит объектісінің КҚ қамтамасыз ету процестерінде КҚ ны қамтамасыз етуді тексеру және талдау	Машықтар: 1. АЖ-да жобалық-пайдалану құжаттамасын жинау және зерделеу, қызметкерлермен сұхбаттасу және ақпаратты тіркеу 2. КҚ аудит объектісіне НҚА мен НТҚ қолданылуын бағалау 3. Киберқауіпсіздікті 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. КҚ аудит объектісінің ресурстарына қатысты қауіпсіздікке төнетін қатерлерді жүзеге асыру мүмкіндігімен байланысты тәуекелдерді талдау 6. Киберқауіпсіздік аудиті объектісінің қорғаныс жүйесі мен архитектурасындағы қиындықтарды анықтау
		Білімдер: 1. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама 2. КҚ тәуекелдері мен қауіптерін анықтаудың әдістемелері, бағдарламалық құралдары 3. Аудиторлық куәліктерді жинау әдістері, рәсімдері мен тәртібі
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 3: АҚ аудит объектісінің ағымдағы қорғалу жағдайын тексеру және талдау	Машықтар: 1. Аудит объектісінің физикалық қауіпсіздігінің жай-күйін тексеру 2. Архитектурамен байланысты аудит объектісінің қауіпсіздік сипаттамаларын тексеріңіз 3. Аудит объектісінің серверлік және желілік жабдықтарының КҚ кіріктірілген механизмдерінің конфигурациясына байланысты қауіпсіздік сипаттамаларын тексеру 4. Пайдалану осалдықтарының бар-жоғын БҚ конфигурацияларын 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
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 3:		Машықтар:

Аудиторлық тапсырманың міндеттерін орындау		1. БҚ бастапқы кодына статикалық талдау жүргізу 2. Бастапқы кодқа динамикалық талдау жүргізу 3. Аудит объектісінің БҚ осалдықтарын анықтау
	Дағды 4: Аудит объектісінің бағдарламалық қамтамасыз етуінің осалдығын 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: Бағдарламалық қамтамасыз етуді әртүрлі жүктеме режимдерінде жұмысқа қабілеттілігіне тестілеу	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 желісінің жабдығының осалдығын 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. КҚ стандарттарына сәйкестігі туралы есептерді жасау және талдау
		Білімдер: 1. Қорғалу мен осалдықты талдаудың әдістері мен бағдарламалық құралдары

		2. Желі ресурстарын түгендеу техникасы 3. КҚ 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	
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:
	7	Ақпараттық қауіпсіздік жөніндегі аудитор
38. 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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда ЦТ 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. Анықталған осалдықтарды жою үшін әзірлеушілермен және қызмет менеджерлерімен өзара әрекеттесу 2. Киберқауіпсіздікке байланысты жаңа функционалдылықтың кеңесшісі және тапсырыс берушісі	
	Қосымша еңбек функциялары:		
Еңбек функциясы 1: Анықталған осалдықтарды жою үшін әзірлеушілермен және қызмет менеджерлерімен өзара әрекеттесу	Дағды 1: Қызметтердің анықталған осалдықтары туралы ақпаратты жинау және талдау	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	
		Машықтар: 1. Әзірлеушілер үшін осалдықтарды жою бойынша міндеттерді тұжырымдау 2. Осалдықтарды түзету бойынша ұсынымдар әзірлеу	

	Дағды 2: Сервистердің анықталған осалдықтарын жою жөніндегі міндеттерді қою және қабылдау	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: Киберқауіпсіздікке байланысты жаңа функционалдылықтың кеңесшісі және тапсырыс берушісі	Дағды 1: Бұқаралық ақпарат құралдарында және басқа да ашық қолжетімді көздерде сервистер туралы жарияланымдар мен хабарламаларды дайындау және орналастыру	Машықтар: 1. Киберқауіпсіздік 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:	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

	Өнімнің мүмкіндіктерін көрсету	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. Киберқауіпсіздікті 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	
39. Кәсіптің карточкасы "Көптілді талдау жөніндегі маман":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-025		
Кәсіптің атауы:	Көптілді талдау 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:	Қажет емес	
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) лингвистикалық білім болған кезде киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары	
Кәсіптің басқа ықтимал атаулары:		
Қызметтің негізгі мақсаты:	Киберқауіпсіздік операцияларын қолдау үшін, әсіресе халықаралық қауіптерді талдауда лингвистикалық және мәдени сараптаманы қолданады.	
Еңбек функциялардың сипаттамасы		
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Шетелдік ақпарат көздерін сәйкестендіру және өңдеу 2. Киберқауіпсіздік саласындағы лингвистикалық талдау 3. Көптілді талдау нәтижелері бойынша аналитикалық материалдар мен есептерді дайындау
	Қосымша еңбек функциялары:	1. Бағдарламалық кодты социолингвистикалық талдау
Еңбек функциясы 1: Шетелдік ақпарат көздерін сәйкестендіру және өңдеу	Дағды 1: Киберқауіпсіздік саласындағы материалдарды аудару және бейімдеу	Машықтар: 1. Киберқауіпсіздік бойынша техникалық мәтіндердің нақты аудармасын орындау 2. Мәтінмәнді ескере отырып аударманы бейімдеу 3. Аударманың дұрыстығын мағынаның бұрмалануын тексеріңіз (Пасха жұмыртқалары) 4. Арнайы терминология глоссарийлерімен жұмыс істеу
		Білімдер: 1. Киберқауіпсіздік саласындағы техникалық және мамандандырылған мәтіндерді аудару әдістері 2. Шет тілдеріндегі киберқауіпсіздік саласындағы ерекше лексика 3. Идиомалық өрнектерді аудару кезінде мағынаны сақтау принциптері 4. Аударма сапасының стандарттары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Шетелдік мәтіндер мен аудио материалдарды тану және жіктеу	Машықтар: 1. Ақпарат көзінің тілі мен диалектісін анықтаңыз 2. Шетелдік дереккөздердің КҚ саласындағы ақпараттан маңызды үзінділер алу 3. Тілдік деректерді өңдеу үшін арнайы құралдарды қолданыңыз
		Білімдер: 1. Негізгі шет тілдерінің фонетикасы, морфологиясы және синтаксисінің негіздері 2. Тілдер мен диалектілерді анықтау әдістері 3. Сөйлеуді және мәтінді автоматты тану құралдарымен жұмыс істеу принциптері

		4. Шет тілдеріндегі киберқауіпсіздік саласындағы терминологиялар
	Дағдыны тану мүмкіндігі:	Қажет емес
Еңбек функциясы 2: Киберқауіпсіздік саласындағы лингвистикалық талдау	Дағды 1: Шет тіліндегі дереккөздердің мәдени контекстін талдау	Машықтар: 1. Коммуникациядағы мәдени ерекшеліктерді анықтау 2. Шетелдік мәтіндердегі жасырын мағыналар мен ішкі мәтіндерді түсіндіру 3. Мәдени факторлардың киберқауіпсіздік саласына әсерін бағалау 4. Мәдени ерекшеліктерді кибершабуылдармен салыстыру
		Білімдер: 1. Әлеуетті қауіп төндіретін өңірлердің мәдени ерекшеліктері 2. Коммуникацияның әлеуметтік-лингвистикалық аспектілері 3. Мәдениеттің киберқауіпсіздік саласына әсері 4. Мәтіндерді мәдени талдау әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Геосаяси және өңірлік қауіп көзін бағалау	Машықтар: 1. Деректерді геосаяси оқиғалармен байланыстыру 2. Тілдік белгілері бойынша қауіптің шығу индикаторларын анықтау 3. Кибершабуылдардағы аймақтық ерекшеліктерді талдау 4. Мәдени-лингвистикалық деректер негізінде қауіптердің дамуын болжау
		Білімдер: 1. Киберқауіпсіздіктің геосаяси ерекшеліктері 2. Киберқауіпсіздік саласындағы тілдік жаңғыртудың өңірлік ерекшеліктері 3. Халықаралық қатынастар бойынша ашық ақпарат көздері 4. Киберқауіпсіздік саласындағы мәдени контекстті түсіндіру әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 1: АҚ қатерлеріне қарсы іс-қимыл бойынша	Машықтар: 1. Көптілді деректер негізінде талдамалық есептер жасау 2. Қауіптерді бейтараптандыру бойынша ұсыныстарды тұжырымдау 3. Талдау нәтижелерін мүдделі тараптарға таныстыру 4. Есептерді аудиторияның әртүрлі деңгейлеріне бейімдеу
		Білімдер:

Еңбек функциясы 3: Көптілді талдау нәтижелері бойынша аналитикалық материалдар мен есептерді дайындау	есептер мен ұсынымдар дайындау	1. Киберқауіпсіздік саласындағы аналитикалық есептердің құрылымдары 2. КҚ қатерлеріне қарсы іс-қимыл бойынша ұсынымдарды тұжырымдау әдістері 3. Аналитикалық ақпаратты ұсыну принциптері 4. Киберқауіпсіздік саласындағы есептерді ресімдеуге қойылатын талаптар
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Аналитикалық деректерді жинау және жүйелеу	Машықтар: 1. Лингвистикалық талдау нәтижелерін жүйелеу 2. Көптілді қауіп көздері бойынша мәліметтер базасын қалыптастыру 3. Аналитикалық есептер үшін деректерді визуализациялау 4. Өңделген ақпараттың құпиялылығын қамтамасыз ету
		Білімдер: 1. Аналитикалық деректерді жүйелеу және сақтау әдістері 2. Қауіптер бойынша деректер базасын құруға арналған құралдар 3. Киберқауіпсіздіктегі ақпаратты визуализациялау принциптері 4. Деректерді өңдеу кезінде ақпаратты қорғау нормаларын
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Бағдарламалық кодты социолингвистикалық талдау	Дағды 1: Бағдарламалық кодтың әлеуметтік лингвистикалық ерекшеліктерін анықтау және бағалау	Машықтар: 1. Түсініктемелер мен Код айнымалыларындағы лингвистикалық ерекшеліктерді анықтаңыз 2. Кодта идиомалық өрнектердің қолданылуын талдау 3. Бағдарламалық код құрылымындағы мәдени сілтемелерді анықтаңыз 4. Әр түрлі бағдарламалау тілдерінде кодты салыстырмалы талдау жүргізу
		Білімдер: 1. Әлеуметтік лингвистиканың негіздері және оны цифрлық деректерге қолдану 2. Лингвистикалық ерекшеліктерді ескере отырып бағдарламалау терминологиясы 3. Код жазу стиліндегі мәдени айырмашылықтар 4. Жасырын әлеуметтік лингвистикалық индикаторларды анықтау әдістері
	Дағдыны тану мүмкіндігі:	Қажет емес
	Жүйелі ойлау Күйзеліске тұрақтылық Тәртіптілік	

Жеке құзыреттерге қойылатын талаптар:	Аналитикалық ойлау Зейінді шоғырландыру және бақылау Бастамашылық Көшбасшылық		
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 15408 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін қамтамасыз ету критерийлері (Common Criteria) ISO/IEC 27001 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар ISO/IEC 27002 - ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Бақылау шараларын басқару (ақпараттық қауіпсіздікті қамтамасыз ету шаралары бойынша практика кодексі) ISO/IEC 2382 & ISO/IEC 2383 — Ақпараттық технологиялар. Терминология және жалпы ұғымдар (2382), деректерді талдау (2383). АКТ саласындағы қолдау стандарттары ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ ISO / IEC 15408-5-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 5 бөлім. Қауіпсіздік талаптарының алдын ала анықталған пакеттері") ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар")		
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:	
40. Кәсіптің карточкасы "Денсаулық сақтау саласындағы ақпараттық қауіпсіздік жөніндегі маманы":			
Топтың коды:	2524-0		
Қызмет атауының коды:	2524-0-017		
Кәсіптің атауы:	Денсаулық сақтау саласындағы ақпараттық қауіпсіздік жөніндегі маманы		
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:	Қажет емес		
Формалды емес және информалы біліммен байланыс:	Базалық (жоғары) ЦТ білімі бар киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша бағдарламалары		
Кәсіптің басқа ықтимал атаулары:	2524-0-007 - Ақпараттық қауіпсіздік жөніндегі маман		

Қызметтің негізгі мақсаты:	Медициналық мекемелерге және олармен байланысты медициналық жабдықтар жүйелеріне рұқсатсыз кіруді болдырмау үшін оларды қорғауды қамтамасыз ету. Медициналық жүйедегі командалар мен байланыс үзілістері.	
Еңбек функциялардың сипаттамасы		
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Денсаулық сақтау жүйесін басқару мен бақылауда қауіпсіздік жүйелерін, желілік құрылғыларды, медициналық жабдықтарды тестілеу, сондай-ақ осалдықтарды анықтау 2. Денсаулық сақтау жүйесінің ерекшеліктерін ескере отырып киберқауіпсіздік стандарттарын әзірлеу және енгізу 3. Киберқауіпсіздік инциденттеріне жауап беру
	Қосымша еңбек функциялары:	1. Қызметкерлерді киберқауіпсіздік саясаты мен процедуралары бойынша оқыту
	Дағды 1: Электрондық медициналық құжаттарды және зертханалық жүйелерді қоса алғанда, денсаулық сақтаудың цифрлық жүйелерінің ерекшеліктері	Машықтар: 1. Электрондық медициналық карталарды (ЭМК) және зертханалық жүйелерді баптау мен қорғауды қоса алғанда, денсаулық сақтаудың цифрлық жүйелерімен (иск) жұмыс істеу 2. Медициналық ақпаратты қорғау кезінде ҚР заңнамасы мен денсаулық сақтау министрлігі стандарттарының талаптарын сақтауды қамтамасыз ету 3. Шифрлауды және қолжетімділікті шектеуді қоса алғанда, дербес деректерді және құпия медициналық ақпаратты қорғау жөніндегі шараларды іске асыру 4. Медициналық цифрлық жүйелердегі пайдаланушылардың қол жетімділігі мен аутентификациясын бақылау жүйелерін конфигурациялау және басқару 5. VPN, антивирустық шешімдер және деректерді шифрлау құралдарын қоса алғанда, желілік қорғаныс құралдарын енгізу және қолдау 6. Интрузияны анықтау жүйелерін (IDS/IPS) конфигурациялау және пайдалану, қауіптерді уақтылы анықтау үшін қауіпсіздік мониторингін жүргізу 7. Жүйелердің үздіксіздігін қамтамасыз ету үшін медициналық деректердің сақтық көшірмесін жасау және қалпына келтіру процестерін ұйымдастыру 8. Денсаулық сақтау саласындағы нақты киберқауіптерді, соның ішінде медициналық жабдықтар мен жүйелерге жасалған шабуылдарды талдау және оларға қарсы тұру
		Білімдер: 1. Денсаулық сақтаудағы нормативтік-құқықтық талаптар ("Қазақстан Республикасы азаматтарының денсаулығын сақтау туралы" Қазақстан Республикасының Заңы (2009 жылғы 18 қыркүйектегі № 193-V ҚР Заңы), "Дербес деректер және оларды қорғау туралы" Қазақстан

		Республикасының Заңы (2013 жылғы 21 мамырдағы № 94-V ҚР Заңы) 2. Дербес деректерді және құпия медициналық ақпаратты қорғау әдістері 3. Медициналық жүйелердегі қол жетімділікті бақылау және аутентификация технологиялары 4. Денсаулық сақтаудың цифрлық жүйелерінің желілік қауіпсіздігінің айрықша негіздері 5. Интрузияны анықтау (IDS/IPS) және қауіпсіздік мониторингі жүйелерінің жұмыс принциптері 6. Медициналық деректердің сақтық көшірмесін жасауды және қалпына келтіруді ұйымдастыру 7. Денсаулыққа тән киберқауіптер (мысалы, медициналық жабдыққа шабуыл)
	Дағдыны тану мүмкіндігі:	Қажет
Еңбек функциясы 1: Денсаулық сақтау жүйесін басқару мен бақылауда қауіпсіздік жүйелерін, желілік құрылғыларды, медициналық жабдықтарды тестілеу, сондай-ақ осалдықтарды анықтау	Дағды 2: Бағдарламалық қамтамасыз етуді тексеру	Машықтар: 1. Ұйымның қауіпсіздік жүйесіндегі әлсіз жақтарды анықтау үшін тұрақты осалдықты және эксплуатациялық сканерлеуді (SIEM құралдарын қоса) жоспарлау және орындау 2. Қауіпсіздік жүйелеріне ену сынақтарын жүргізу 3. Тәуекел деңгейлерін бағалау үшін осалдықты сканерлеу нәтижелерін пайдалану 4. Осалдықтарды немесе тәуекелдерді жою бойынша ұсыныстарды әзірлеу
		Білімдер: 1. Python, BASH, Java, Ruby және Perl сияқты пентест және бағдарламалау тілдерінің негіздері 2. РК ден қою жөніндегі ағымдағы ұйымдастыру саясаты мен рәсімдері 3. РК анықтау және алдын алудың стандартты салалық құралдары 4. Қалыпты емес белсенділіктің идентификациялық сипаттамалары 5. NIDS, NIPS, HIDS және HIPS қондырғылары мен параметрлері 6. РК анықтау туралы есептерді жасау үшін қажетті құжаттама 7. Белгілі осалдықтарды жоймас бұрын оның құпиялылығын сақтау үшін жаңа осалдықтар туралы ақпаратты басқару 8. Кәсіпорындардың архитектуралары мен желілерінде NIDS / nips өнімдерін жобалау кезінде датчиктерді дұрыс орналастыру 9. РК анықтау жүйелеріне қызмет көрсету және конфигурациялау 10. Siem құралдарын пайдаланып осалдықтарды сканерлеуді орындау 11. Қорғаныс мониторингін қолдана отырып, желідегі немесе жүйедегі қалыптан тыс әрекеттерді анықтау

		12. Энергетика саласындағы ерекшеліктерді ескере отырып, жүйелер мен осалдықтардың қорғалуын талдаудың бағдарламалық құралдары мен әдістері 13. Энергетика объектілерінің жұмыс істеуінің құқықтық, инженерлік-техникалық, ұйымдастырушылық мәселелерін түсіну
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 3: Желіні бақылау, қауіпсіздік қатерлерін ерте анықтау	Машықтар: 1. Қауіптерді анықтау үшін кешенді бақылау және мониторинг жүргізу 2. Ықтимал бұзушылықтарды табу және анықтау үшін қауіп деректерін талдау нәтижелерін пайдаланыңыз 3. Тәулік бойы қорғау мониторингін қоса алғанда, ҚҚ анықтау және алдын алу жүйелерін орнатуды, пайдалануды және оларға қызмет көрсетуді жүзеге асыру 4. Желілік ресурстарға аномальды белсенділік пен ықтимал қауіптерді анықтау үшін желілік трафик деректерін талдау және сипаттау
		Білімдер: 1. РК анықтау және алдын алудың стандартты салалық құралдары 2. РК-ға ден қою жөніндегі ағымдағы ұйымдастыру саясаты мен рәсімдері 3. Қалыпты емес белсенділіктің идентификациялық сипаттамалары 4. Қорғаныс мониторингін қолдана отырып, желідегі немесе жүйедегі қалыптан тыс әрекеттерді анықтау 5. Белгілі осалдықтарды жоймас бұрын оның құпиялылығын сақтау үшін жаңа осалдықтар туралы ақпаратты басқару 6. Энергетика саласындағы ерекшеліктерді ескере отырып, жүйелер мен осалдықтардың қорғалуын талдаудың бағдарламалық құралдары мен әдістері
	Дағдыны тану мүмкіндігі:	Қажет
	Дағды 1: РК алдын алуға арналған желілік қауіпсіздік жүйесін қашықтан орнату және жаңарту	Машықтар: 1. Жүйенің бағдарламалық жасақтамасы мен аппараттық құралдарын үнемі жаңартып отыру 2. Вирусқа қарсы бағдарламалық құралды орнатыңыз және жаңарту 3. Өнеркәсіптік желі түйіндері үшін желіаралық қалқандарды конфигурациялау 4. Жаңартуларды енгізу алдында өнеркәсіптік бағдарламалық құралмен үйлесімділігін тексеру
		Білімдер: 1. Кәсіпорынның өнеркәсіптік желілік тораптарының жұмысы

		2. Шифрлау және криптография 3. Саясаттар, орнату принциптерінің талаптары және жаңартулар 4. Брандмауэрдің жұмыс істеуі, қолданылуы және конфигурациясы 5. Орнату ACL критерийі брандмауэрдегі рұқсат етілген трафикті анықтау үшін
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Қауіпсіздік тәуекелдерін азайту үшін қауіпсіздік хаттамалары мен процедураларын әзірлеу, енгізу және қолдау	Машықтар: 1. Қолданыстағы ұйымдастырушылық қауіпсіздік операциялары мен талаптарын анықтау 2. Ұйымның талаптарымен салыстырғанда ұйымның қолданыстағы киберопераciяларының тиімділігіне талдау жүргізу 3. Ұйымдастырушылық талаптарға сәйкес талдау нәтижелерін құжаттау 4. ICS жүйелерін енгізу және қызмет көрсету 5. Қолданыстағы ұйымдық операциялардың, қызмет көрсетудің бұзылуының және кибер операцияларды жүзеге асыру міндеттерінің қажетті жаңартуларын анықтау және құжаттау 6. Қажетті операциялық және аналитикалық процестерді, оқиғалар туралы есеп беру рәсімдерін енгізу
		Білімдер: 1. Техникалық, өндірістік және ұйымдастырушылық құжаттама 2. Қажетті құрылымды пайдалана отырып, егжей-тегжейлі талдау, қорытындылар және ұсыныстар бар құжаттаманы жазу 3. Энергетика саласының ерекшеліктерін ескере отырып, өнеркәсіптік басқару жүйесі (ӨБЖ) саласындағы салалық-техникалық білім 4. C, C++, PHP, Python және JavaScript сияқты бағдарламалау тілдері
Еңбек функциясы 2: Денсаулық сақтау жүйесінің ерекшеліктерін ескере отырып киберқауіпсіздік стандарттарын әзірлеу және енгізу	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Стандартты шаблондар мен құралдарды қолдана отырып, КҚ оқиғаларын тіркеу, жіктеу және басымдықтарды анықтау 2. Қауіпсіздік инциденттері бойынша құжаттаманы жүргізу 3. Кәсіпорынның электр желілеріне IoT құрылғыларының инфрақұрылымы мен қосылымдарын анықтаңыз 4. IoT қауіпсіздігінің ауытқулары мен оқиғаларын анықтау

	Дағды 3: IoT жүйелері үшін қауіпсіздікті енгізу	5. Ақпаратты жинау және IOT соңғы нүктелерінің қауіпсіздік мәселелерін терең талдау, диагностикалау және жою 6. IoT қауіпсіздік мәселелерін анықтау процестеріне тұрақты техникалық қызмет көрсетуді орындаңыз 7. It бойынша мониторинг және есеп беру ақпараттық панельдерін жобалау және әзірлеу 8. Барлық IoT деңгейлеріндегі маңызды осалдықтарды сканерлеу 9. Қауіпсіздік құрылғыларының сақтық көшірмесін жасаңыз және шифрлау
		Білімдер: 1. Бақылау бақылау тақтасын әзірлеу 2. Деректерді бағдарламалау және визуализация тілдері (Python, R, SQL, NodeJS) 3. Шифрлау және криптография негіздері 4. АҚ-ны қолдау жөніндегі ұйымдастыру саясаты, рәсімдері мен нұсқаулықтары 5. КҚ рәсімдерін құжаттау және енгізу үшін деректермен алмасу рәсімдері 6. Қауіпсіздікті бақылау үшін қол жетімді стандартты шаблондар мен құралдардың спектрі 7. IoT жүйелеріндегі желінің, құрылғылардың, конфигурацияның және қосылудың негізгі топологиялары 8. Құрылғыларды, бұлттарды, коммуникацияларды, дерекқорларды және қолданбаларды қоса алғанда, әртүрлі IoT қауіпсіздік контексттері мен деңгейлері, қамту 9. Киберқауіпсіздік инциденттеріне әрекет етудің әдеттегі операциялық процедуралары It 10. Киберқауіпсіздік осалдықтары мен оқиғаларын жою It 11. IoT жүйелерінде киберқауіпсіздік деңгейін арттыруды енгізу 12. IoT жүйелеріндегі ауытқуларды анықтау және талдау, жүйелік аудит хаттамалары
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 1: Киберқауіпсіздік оқиғаларын бағалау және хабарлау	Машықтар: 1. Журналдарды, кэштерді, файлдарды және басқа сандық артефактілерді қоса, кибершабуылға қатысты дәлелдемелерді жинау, тасымалдау және сақтау 2. Ішкі мүдделі тараптармен, соның ішінде атқарушы менеджмент, киберкриминалистика және IT командаларымен жұмыс 3. Кибершабуылдар туралы ақпаратты құқық қорғау органдарына жіберіңіз
		Білімдер:

		1. Құқық қорғау органдарына киберқауіпсіздік оқиғалары туралы хабарлауға арналған ішкі хаттамалар 2. Құпия деректерді өңдеу (кибершабуылдардың дәлелдемелерін жинау, шифрлау, сақтау және жіберу)
	Дағдыны тану мүмкіндігі:	Қажет емес
	Дағды 2: Ұйымдық қауіпсіздік процедураларына сәйкес инциденттерді тану және әрекет ету	Машықтар: 1. Киберқауіпсіздік оқиғаларының пайда болуы мен сипатын анықтау және растау 2. Киберқауіпсіздік оқиғаларына қатысты заңнамалық талаптарды, ұйымдастырушылық саясатты, процедураларды және әрекет ету жоспарларын анықтау 3. Оқиғаның көздерін, әсері мен салдарын талдау және бағалау 4. Оқиғаға жауап беру жоспарын іске қосыңыз және кибер оқиғаның локализацияланғанын растау 5. Ұйымның маңызды жүйелік инфрақұрылымының зақымдануын немесе деректердің бұзылуын бағалау 6. Киберқауіпсіздік оқиғасын, қабылданған әрекеттерді, шешімдерді және нәтижелерді құжаттау
Еңбек функциясы 3: Киберқауіпсіздік инциденттеріне жауап беру		Білімдер: 1. Киберқауіпсіздік оқиғаларына жауап беру жоспарларының негізгі ерекшеліктері және олардың көздері мен себептері 2. Шабуылдардың әртүрлі түрлері, соның ішінде қызмет көрсетуден бас тарту (DoS), SQL инъекциялары(Sql), сайтаралық сценарий шабуылдары (XSS), аппараттық шабуылдар, WiFi шабуылдары 3. Киберқауіпсіздік оқиғаларын анықтау әдістемесі, алдын алу шаралары және азайту әдістері 4. КҚ оқиғалар журналын құжаттау және талдау процестері 5. Киберқауіпсіздік инциденттеріне әрекет етудің ұйымдастырушылық саясаты мен рәсімдері (инциденттердің сипаты мен орналасқан жерін анықтау, инциденттерді оқшаулау, қауіпсіздік патчтарын орнату және желіге кіруді өшіру, хабарлау және қажетті персоналға есептер беру)
	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Ұйымның миссиясы мен мақсаттарына сәйкес келетін киберқауіпсіздік саясаты мен нұсқаулығын енгізіңіз 2. Ұйымның деректері мен жүйелерін зиянкестерден қорғау үшін қолданыстағы қауіпсіздік стандарттарын қолданыңыз

	Дағды 3: Ұйым үшін қолданыстағы киберқауіпсіздік стандарттарын, саясаттары мен нұсқауларын енгізу	3. Оқиғаларды тиімді басқару үшін оқиғаларға жауап беру жоспарлары мен процедураларын әзірлеу және қолдау 4. Ұйымның киберқауіпсіздік тәуекелдерін бағалау және осы тәуекелдерді азайту стратегияларын әзірлеу 5. Ұйымның киберқауіпсіздік саясаты мен нұсқауларының өзектілігін қамтамасыз ету үшін қауіпсіздік тенденциялары мен туындайтын қауіптерді бақылау және талдау
		Білімдер: 1. Жетілдірілген желілік қауіпсіздік мүмкіндіктері. 2. Энергетика саласының ерекшеліктерін ескере отырып, киберқауіпсіздік стандарттарын енгізуге қолданылатын ұйымдастырушылық бизнес-процестер. 3. Белгіленген стандарттар мен талаптарды құжаттау 4. Желілік қауіпсіздік инфрақұрылымының талаптары мен сипаттамаларын белгілеу 5. Техникалық қызмет көрсету және хабарлау процестерін белгілеу 6. Желілік қауіпсіздік инфрақұрылымына жоспарлы тексерулер жүргізу 7. КҚ тестілеу әдістері мен процедуралары 8. Ұйымдағы қауіпсіздік тәуекелдері және тәуекелге төзімділік 9. Ұйымда желілік қауіпсіздік инфрақұрылымын енгізу бойынша салалық стандарттар мен ережелер
	Дағдыны тану мүмкіндігі:	Қажет емес
Қосымша еңбек функциясы 1: Қызметкерлерді киберқауіпсіздік саясаты мен процедуралары бойынша оқыту	Дағды 1: Қызметкерлерді киберқауіпсіздік саясаты мен процедуралары бойынша оқыту	Машықтар: 1. Парольдерді басқару, электрондық пошта қауіпсіздігі, фишингтік шабуылдар, әлеуметтік инженерия, зиянды бағдарламалардан қорғау және деректерді қорғау тақырыптары бойынша қызметкерлерге арналған Киберқауіпсіздік бойынша оқыту бағдарламаларын әзірлеу 2. Презентация, оқыту бағдарламалары және практикалық сабақтар ретінде әртүрлі әдістерді қолдана отырып, қызметкерлерге арналған тренингтер өткізу 3. Оқу бағдарламаларының тиімділігін бақылау және бағалау
		Білімдер: 1. Презентацияларды өткізу тәсілдері мен принциптері 2. Оқытудың әртүрлі әдістері 3. Ақпаратты техникалық қорғау бойынша ғылыми зерттеулер, әзірлемелер жүргізу әдістері

		елде және шетелде техникалық барлау және ақпаратты қорғау саласындағы ғылым мен техниканың жетістіктері 4. Ақпараттың қауіпсіздігін қамтамасыз ету жөніндегі мамандарды аттестаттау, кәсіби деңгейін бағалау әдістері 5. Еңбек заңнамасының, ішкі еңбек тәртібінің, еңбек қауіпсіздігі және еңбекті қорғау, өндірістік санитария, өрт қауіпсіздігі талаптарының тәртібі
	Дағдыны тану мүмкіндігі:	Қажет емес
Жеке құзыреттерге қойылатын талаптар:	Жүйелі ойлау Күйзеліске тұрақтылық Аналитикалық ойлау Бастамашылық	
Техникалық регламенттер мен ұлттық стандарттардың тізімі:	Халықаралық стандарттар: ISO/IEC 27001 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар ISO/IEC 27799 - Денсаулық сақтаудағы ақпараттық технологиялар (Health informatics). Денсаулық сақтаудағы ақпараттық қауіпсіздікті басқару (in health Information Security management) ISO/IEC 27002 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары (практика кодексі) ISO/IEC 27005 - Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік тәуекелдерін басқару (Risk management) ҚР Ұлттық стандарттары: ҚР СТ ISO / IEC 27001-2023 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар") ҚР СТ ISO / IEC 15408-4-2025 ("Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 4 бөлім. Бағалау әдістері мен әрекеттерінің спецификациясының құрылымы") ҚР СТ 1073-2025 ("Ақпаратты криптографиялық қорғау құралдары. Ақпараттық қауіпсіздік пен өмірлік цикл процестеріне қойылатын талаптар")	
СБШ -нің ішіндегі басқа кәсіптермен байланыс:	СБШ-нің деңгейі:	Кәсіптің атауы:
41. 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:	Басшылар, мамандар және басқа да қызметшілер лауазымдарының біліктілік анықтамалығын бекіту туралы Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрінің 2020 жылғы 30 желтоқсандағы № 553 бұйрығы 2-параграф. Ақпаратты қорғау жөніндегі инженер	

Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -

Жұмыс тәжірибесіне қойылатын талаптар:	Кадрларды даярлаудың тиісті бағыты бойынша жоғары (немесе жоғары оқу орнынан кейінгі) білім, жұмыс өтіліне талаптар қойылмайды немесе тиісті мамандық (біліктілік) бойынша техникалық және кәсіптік, орта білімнен кейінгі (арнайы орта, кәсіптік орта) білім және I санатты ақпаратты қорғау жөніндегі техник лауазымында кемінде 3 жыл жұмыс өтілі.	
Формалды емес және информалы біліммен байланыс:	Киберқауіпсіздік саласындағы біліктілікті арттырудың қосымша кәсіби бағдарламалары базалық (жоғары) білімі болған жағдайда ЦТ 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. Ұйымда ақпаратты қорғау жүйесін құру 2. Ұйымда ақпаратты қорғау жүйесін пайдалануға беру
	Қосымша еңбек функциялары:	
		Машықтар: 1. Ақпаратты қорғаудың арнайы техникалық және бағдарламалық-математикалық құралдарын жобалау және енгізу, цифрлық 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 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

Еңбек функциясы 1: Ұйымда ақпаратты қорғау жүйесін құру	Дағды 1: Ұйымда қорғалуға жататын қол жетімділігі шектеулі ақпараттың (мәліметтердің) тізбесін айқындау	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. Цифрландыру 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: Ұйымда ақпаратты қорғау жүйесін пайдалануға беру	Дағды 1: Ақпаратты қорғау жүйесінің тиімділігін қамтамасыз ететін ұйымдастыру шараларын әзірлеу және іске асыру	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. ҚҚ қамтамасыз ету саласындағы нормативтік-құқықтық актілер 2. Ақпаратты қорғау әдістері, құралдары және жүйелері 3. Ақпаратты қорғаудың техникалық құралдарының архитектурасы 4. ҚҚ қамтамасыз ету саласындағы ұлттық стандарттар
	Дағдыны тану мүмкіндігі:	Талап етілмейді
	Дағды 2:	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

	Берілген үлгілер бойынша бағдарламалық қамтылым ақпаратын қорғаудың кіріктірілген құралдарын баптау	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
42. 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:	Басшылар, мамандар және басқа да қызметшілер лауазымдарының біліктілік анықтамалығын бекіту туралы Қазақстан Республикасы Еңбек және халықты әлеуметтік қорғау министрінің 2020 жылғы 30 желтоқсандағы № 553 бұйрығы 3-параграф. Ақпаратты қорғау жөніндегі маманы	

Кәсіптік білім деңгейі:	Білім деңгейі: жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -

Жұмыс тәжірибесіне қойылатын талаптар:	1. 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; 2. 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; 3. 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:	ЦЖ 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:	
	Дағды 1: ЦЖ ақпаратты қорғау жүйелерінің диагностикасы	Машықтар: 1. Киберқауіпсіздікке қатерлерді жіктеу және бағалау 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 ЦЖ және ЦЖ қауіпсіздігінің кіші жүйелерін пайдалану жөніндегі персонал қызметінің мазмұны мен тәртібі 2. Цифрлық жүйедегі ақпарат қауіпсіздігіне және бұзушының моделіне негізгі қатерлер 3. ЦЖ ақпаратты қорғау үшін пайдаланылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар

Еңбек функциясы 1: АЖ-да оларды пайдалану процесінде ақпараттың қорғалуын қамтамасыз ету		4. ЦЖ 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
	Дағды 2: ЦЖ ақпаратты қорғау жүйелерін әкімшілендіру	Машықтар: 1. ЦЖ пайдаланушыларының тіркелгілерін жасау, жою және өзгерту 2. ЦЖ бағдарламалық құрамдас бөліктерінің қауіпсіздік саясатын жоспарлау 3. Операциялық жүйелерді, деректер базасын басқару жүйелерін, компьютерлік желілер мен бағдарламалық жүйелерді орнату және баптау 4. ЦЖ -да ақпаратты қорғаудың криптографиялық әдістері мен құралдарын пайдалану 5. ЦЖ -да ақпаратты қорғауға байланысты оқиғаларды тіркеу және талдау
		Білімдер: 1. ЦЖ КҚ саясатын қалыптастыру қағидаттары 2. ЦЖ ақпаратын қорғаудың бағдарламалық-аппараттық құралдары 3. ЦЖ ақпаратты қорғау үшін пайдаланылатын негізгі криптографиялық әдістер, алгоритмдер, хаттамалар 4. Техникалық арналар бойынша ақпаратты " жылыстаудан" қорғау тиімділігін бақылау әдістері 5. ЦЖ бағдарламалық қамтамасыз етуді қорғау құралдарының тиімділігі мен сенімділігін бағалау критерийлері 6. Ақпаратты қорғау шараларының тиімділігін бақылаудың техникалық құралдары 7. ЦЖ бағдарламалық қамтамасыз етуді қорғау жүйелерін ұйымдастыру қағидаттары мен құрылымы 8. Персоналдың қорғалған автоматтандырылған жүйелерді және ЦЖ қауіпсіздік жүйелерін пайдалану жөніндегі қызметінің мазмұны мен тәртібі 9. ЦЖ -да ақпаратты қорғау жөніндегі негізгі шаралар
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. ЦЖ -дағы ақпараттық тәуекелдерді бағалау 2. Киберқауіпсіздікке төнетін қатерлерді жіктеу және бағалау 3. Автоматтандырылған жүйелердің қорғалуға жататын ақпараттық ресурстарын анықтау

	Дағды 3: ЦЖ -да ақпаратты қорғауды басқару	4. ЦЖ ақпаратын қорғауды басқару жүйесін жетілдіру бойынша ұсыныстар әзірлеу 5. ЦЖ ақпаратын қорғау жүйесінің параметрлерін конфигурациялау 6. Ақпаратты қорғау шараларының тиімділігін бақылаудың техникалық құралдарын қолдану
		Білімдер: 1. Ақпаратты қорғауды басқарудың негізгі әдістері 2. Киберқауіпсіздіктің негізгі қатерлері және АЖ-дағы бұзушының модельдері 3. Ақпаратты техникалық арналар арқылы "ағып кетуден" қорғау әдістері 4. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 5. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар
	Дағдыны тану мүмкіндігі:	Талап етілмейді
Еңбек функциясы 2: АЖ-да ақпаратты қорғау жүйелерін енгізу	Дағды 1: АЖ-да ақпаратты қорғау жүйелерін енгізу АЖ-да ақпаратты қорғау бойынша ұйымдастырушылық-өкімдік құжаттарды әзірлеу	Машықтар: 1. Киберқауіпсіздік қатерлерін жіктеу және бағалау 2. Техникалық барлауға қарсы іс-қимыл жөніндегі нормативтік құжаттарды қолдану 3. ЦЖ ақпаратты қорғау жүйесінің бағдарламалық жасақтамасын баптау параметрлерін анықтау 4. АЖ-да ақпаратты қорғау бойынша қабылданған шаралардың тиімділігін бақылау
		Білімдер: 1. Қорғалған ЦЖ 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. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		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 ЦЖ персоналын шаралар кешеніне (ережелер, рәсімдер, практикалық тәсілдер, басшылық қағидаттар, әдістер, құралдар) оқыту

	Дағды 2: Енгізу автоматтандырылған жүйелердегі ақпаратты қорғаудың ұйымдастырушылық шаралары	4. Ақпаратты қорғау жөніндегі талаптарды ескере отырып, ЦЖ персоналының жұмысын жоспарлауды және ұйымдастыруды жүзеге асыру 5. Аттестатталған ЦЖ және ЦЖ ақпаратын қорғау жүйесін конфигурациялау
		Білімдер: 1. Киберқауіпсіздікті қамтамасыз ету саласындағы нормативтік құқықтық актілер 2. Автоматтандырылған жүйелерді қорғау жүйелері мен ЦЖ 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 цифрлық 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
43. 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:		
	Білім деңгейі:	

Кәсіптік білім деңгейі:	жоғары білім (бакалавриат, маман дәрежесі, ординатура)	Мамандық: Ақпараттық қауіпсіздік	Біліктілік: -
Жұмыс тәжірибесіне қойылатын талаптар:	Қажет емес		
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, элементтері мен арналарына бағдарламалық-техникалық әсердің зиянды ықпалына қарсы іс-қимыл		
Еңбек функциялардың сипаттамасы			
Еңбек функцияларының тізбесі:	Міндетті еңбек функциялары:	1. Компьютерлік жүйелер мен желілердегі ақпаратты қорғау құралдарын басқару 2. Киберқауіпсіздік саласындағы тәуекелдерді бағалау және басқару	
	Қосымша еңбек функциялары:		
	Дағды 1: Ақпаратты қорғау құралдарын қолданбалы	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 киберқауіпсіздікке 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. Компьютерлік желілерді құру принциптері	

	және жүйелік бағдарламалық қамтамасыз етуді әкімшілендіру	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 киберқауіпсіздікке 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
		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

Еңбек функциясы 1: Компьютерлік жүйелер мен желілердегі ақпаратты қорғау құралдарын басқару	Дағды 2: Операциялық жүйелердегі ақпаратты қорғаудың ішкі жүйелерін басқару	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
		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 төнетін қатерлерді бағалау 2. Компьютерлік желілерде пакеттерді сүзу ережелерін теңшеңіз 3. Компьютерлік желілерде қолданылатын ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын таңдау 4. Компьютерлік желілерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын конфигурациялау және дұрыс конфигурациялау 5. Компьютерлік желілердегі ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс режимдерін таңдау

	Дағды 3: Компьютерлік желілерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын әкімшілендіру	6. Компьютерлік желілерде ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының жұмыс істеуіне мониторинг жүргізу 7. Компьютерлік желілердегі ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының тиімділігіне талдау жүргізу 8. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарын және олардың компьютерлік желілерде жұмыс істеу режимдерін таңдаудың оңтайлылығын бағалау
		Білімдер: 1. Компьютерлік желілерді құру принциптері 2. Операциялық жүйелердің желілік протоколдарының стегі 3. Желілік жабдық хаттамаларының стегі 4. Желіаралық экрандау әдістері мен құралдарын іске асыру тәртібі 5. Криптографиялық алгоритмдерді қамтитын желілік хаттамалардың жұмыс істеу принциптері 6. Компьютерлік желілердегі қол жетімділік пен ақпараттық ағындарды басқару саясатының түрлері 7. Компьютерлік желілердегі киберқауіпсіздік қатерлерінің көздері және олардың алдын алу шаралары 8. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының үлгілік 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 принциптері мен пайдалану қағидалары 11. Компьютерлік желілердегі ақпаратты қорғаудың бағдарламалық-аппараттық құралдары мен әдістері 12. Киберқауіпсіздік саласындағы нормативтік құқықтық актілер
	Дағдыны тану мүмкіндігі:	Талап етілмейді
		Машықтар: 1. Бағдарламалық жасақтама ақпаратының қауіпсіздігіне төнетін қатерлерді талдау 2. Бағдарламалық жасақтаманы қауіпсіз пайдалану ережелерін тұжырымдау 3. Бағдарламалық жасақтаманы қауіпсіз пайдалану ережелерін негіздеу 4. Ықтимал зиянды әсерді анықтау үшін бағдарламалық жасақтаманың жұмысын талдау 5. Ақпаратты қорғаудың бағдарламалық-аппараттық құралдарының техникалық құжаттамасында

		мәлімделген нақты сипаттамаларының сәйкестігіне тексеру жүргізу 6. Бағдарламалық қамтамасыз етуді пайдалану кезінде туындайтын ақпарат қауіпсіздігіне төнетін қатерлерге қарсы іс-шараларды жүзеге асыру 7. Ақпаратты қорғауды қамтамасыз ету мақсатында бағдарламалық қамтамасыз етудің жұмыс істеу тәртібін айқындау 8. Бағдарламалық жасақтаманың кіріктірілген ақпаратты қорғау құралдарына қойылатын талаптардың тиімділігін талдау
	Дағды 1: Ақпаратты қорғау құралдарын қолданбалы және жүйелік бағдарламалық қамтамасыз етуді әкімшілендіру	Білімдер: 1. Операциялық жүйелердегі ақпаратты қорғау ішкі жүйелерінің архитектурасы 2. Мәліметтер базасын басқару жүйелерін құру принциптері 3. Бағдарламалық жасақтаманы талдаудың негізгі құралдары мен әдістері 4. Антивирустық бағдарламалық жасақтаманы құру принциптері 5. Қолданбалы бағдарламалық жасақтамаға қатысты қол жетімділік пен ақпараттық ағындарды басқару саясатының түрлері 6. Бағдарламалық қамтамасыз етудің киберқауіпсіздігіне қатер көздері және олардың алдын алу жөніндегі шаралар 7. Қолданылатын бағдарламалық жасақтаманың осалдығы және оларды пайдалану әдістері 8. Зиянды бағдарламалық қамтамасыз етудің түрлері мен жұмыс істеу нысандары 9. Зиянды бағдарламалық жасақтаманың сипаттамалық белгілері 10. Бұрын белгісіз зиянды бағдарламалық жасақтаманы анықтау құралдары мен әдістері 11. Ақпаратты криптографиялық қорғаудың бағдарламалық құралдарының жұмыс істеу принциптері 12. Бағдарламалық қамтамасыз етуді пайдалану кезінде ақпараттың қауіпсіздігін қамтамасыз ету тәртібі 13. Ақпаратты қорғау саласындағы нормативтік құқықтық актілер 14. Ақпаратты қорғау жөніндегі ұйымдастыру шаралары
Еңбек функциясы 2: Киберқауіпсіздік саласындағы тәуекелдерді бағалау және басқару	Дағдыны тану мүмкіндігі:	Қажет емес
		Машықтар: 1. Қауіп-қатерлерді, осалдықтар мен салдарларды қоса алғанда, АКТ-ны пайдалануға байланысты әлеуетті тәуекелдерді анықтау және талдау

	Дағды 2: АКТ-ны пайдалануға байланысты тәуекелдерді бағалау әдістемелерін әзірлеу және енгізу	2. Ұйымның және оның цифрлық 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. Киберқауіпсіздік негіздері 2. Тәуекелдерді бағалау әдіснамасы 3. Киберқауіпсіздікті қамтамасыз ету саласындағы ұлттық стандарттар 4. Киберқауіпсіздікті қамтамасыз ету саласындағы заңнама
	Дағдыны тану мүмкіндігі:	Қажет емес
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	Қауіпсіздік мәселелері жөніндегі маман (АКТ)

4-ші тарау. Кәсіптік стандарттың техникалық деректері

44. Мемлекеттік органның атауы:
Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігі
Орындаушы:
Калим Ерболат Темирулы, +7 (700) 007 03 33, e.kalim@mdai.gov.kz
45. Әзірлеуге қатысатын ұйымдар (кәсіпорындар):
"Ақпараттық қауіпсіздік мәселелері институты" ЖШС
Жоба жетекшісі:
Косяков Игорь Олегович
E-mail: heimmdal@topmail.kz
Телефон нөмірі: +7 (702) 359 14 90

Қазақстан Республикасының Жасанды интеллект және цифрлық даму министрлігі
Орындаушылар:
Советханова Ақжарқын Бақдәулетқызы, +7(705) 508 72 05, a.sovetkhanova@mdai.gov.kz
"Қазақстандық ақпараттық қауіпсіздік қауымдастығы" ЗТБ
Орындаушылар:
Покусов Виктор Владимирович, +7 (771) 716 18 16, v@viktor.kz
"Каспий қоғамдық университеті"
Орындаушылар:
Сулейменов Нариман Сапарович, +7 (777) 827 33 31, narimanS1991@yandex.kz
"Әл-Фараби атындағы Қазақ ұлттық университеті" КЕАҚ
Орындаушылар:
Мусиралиева Шынар Женисбековна, +7 (708) 010 03 72, mussiraliyevash@gmail.com
"Л. Н. Гумилев атындағы еуразия ұлттық университеті" КЕАҚ
Орындаушылар:
Сатыбалдина Дина Жагыпаровна, +7 (701) 538 40 75, satybaldina_dzh@enu.kz
"Astana IT University" ЖШС
Орындаушылар:
Аманжолова Сауле Токсановна, +7 (777) 362 22 37, s.amanzholova@astanait.edu.kz
46. Кәсіптік біліктілік жөніндегі салалық кеңес: 10.03.2026 жыл.
47. Кәсіптік біліктілік жөніндегі ұлттық орган: 28.05.2026 жыл.
48. "Атамекен" Қазақстан Республикасының Ұлттық кәсіпкерлер палатасы: -
49. Нұсқа нөмірі және шығарылған жылы: Нұсқа , жыл.
50. Болжамды қайта қарау күні: -

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