Зертханалық жұмыстар

Практикалық жұмыс №1. Пәнге қатысты соңғы 5 жыл ішінде басылып шыққан әдебиеттер туралы деректерді кестеге енгізу керек. Егерде .pdf форматта әдебиет табылса, кестеге енгізуге болады. Электронды нұсқасын кестемен бірге оқытушыға поштаға салып жібересіз. Кем дегенде 5-10 атаудан тұратын болсын кесте.

«Компьютерлік жүйелерде ақпаратты қорғау» пәнінің қамтылуы

№	Әдебиет атауы	Автор (лар)	Басылым түрі (оқулық, оқу құралы, әдістемелік нұсқаулар т.с.с.)	Шыққан жылы	Баспана атауы	Беттер саны	Шифр (кітапх.)	УДК	№ абонемента (№ корпуса)
1.									
2.									

Практикалық жұмыс №2. Курс негізінде қалыптасқан глоссарий

1. **АҚ қаупі (Threat)** – қорғау объектісіне (ақпараттық ресурстар), қарсы бағытталып, қандай да бір әрекеттерді жасайтын (әрекет немесе әрекетсіздік), өзіне, иеленушіге немесе пайдаланушыға зиян тигізу мүмкіндігі болатын ықтималдық.
2. **Ақпаратты қорғау** — ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені
3. **Ақпаратты қорғаудың тиімділігі** – ақпаратты қорғауға қойылған мақсаттар мен нәтижелердің сәйкесітігін көрсететін дәреже.
4. **Ақпаратты қорғаудың мониторингі** – Ақпаратты қорғау талаптарына сәйкесітігін орнату мақсатында ақпараттық жүйедегі ақпарат қауіпсіздігінің қамтамасыздандыру процесіне тұрақты жүргізілетін бақылау.
5. **Ақпаратты қорғаудың объектісі** – қорғаудың мақсатына сәйкес келетін қорғанысты талап ететін ақпарат, ақпарат тасымалдаушысы немесе ақпараттық процесс.
6. **Ақпараттың жариялануынан қорғау** – сол қорғаныстағы ақпаратқа қатынау құқығы жоқ, бірақ қызығушылық танытқан субъектілерге рұқсатсыз жолмен берілуін алдын алуға бағытталған ақпарат қорғанысы.
7. **Ақпаратты қағып алу (перехват)** – ақпараттанған сигналдарды табу, қабылдау және өңдеуді жүзеге асыратын техникалық жабыдықтарды қолдану арқылы ақпаратты заңсыз алу.
8. **Ақпараттанған сигнал** – параметрлері арқылы қорғаныстағы ақпараттың анықталуына жол беретін сигнал.
9. **Аутентификация** – субъект пен оның идентификаторының сәйкестігін тексеру және растау операциясы
10. **Ақпараттық қылмыс** (киберқылмыс) - ақпараттық технологияларды пайдаланумен жасалатын, қылмыстық-жазалау әрекетін көздейтін, қылмыс түрі.
11. **Ақпараттық терроризм** - ақпараттық ресурстар пайдаланылатын немесе (және) оларға ақпараттық кеңістікте әсер ететін террористік мақсатта жүзеге асырылатын қызмет.
12. **Есепберушілік** (немесе хаттамалау тетігі) қауіпсіздікті қамтамасыз етудің маңызды құралы болып табылады. Сенімді жүйе қауіпсіздікке байланысты барлық оқиғаларды тіркеп отыруы керек, ал хаттаманы жазу-жүргізу тексерумен (аудитпен - тіркелу ақпаратына талдау жасаумен) толықтырылады.
13. **Желілік қауіпсіздік сервистері** есептеуіш жүйелерде және желілерде өңделетін ақпараттың қорғау механизмдері
14. **Қауіп (threat)-** бүтіндіктің, қолжетімділіктің, конфиденциялдықтың бұзылуларына себеп болатын, шарттар мен факторлар жиынтығы.
15. **Қауіпсіздік саясаты** - мекеменің ақпаратты қалайша өңдейтінін, қорғайтынын және тарататынын анықтайтын заңдар, ережелер және тәртіп нормаларының жиыны. Бұл ережелер пайдаланушының қайсы кезде белгілі бір деректер жинағымен жұмыс істей алатынын көрсетеді. Қауіпсіздік саясатын құрамына мүмкін болатын қауіптерге талдау жасайтын және оларға қарсы әрекет шаралары кіретін қорғаныштың белсенді сыңары деп санауға болады
16. **Қатынасым мониторы** - пайдалынушының программаларға немесе деректерге әрбір қатынасының мүмкін болатын іс - әрекеттер тізімімен келісімдігі екендігін тексеретін монитор. Қатынасым мониторынан үш қасиеттің орындалуы талап етіледі:

- оңашаландық. Монитор өзінің жұмысы кезінде аңдудан қорғалуға тиісті;
- толықтық. Монитор әрбір қатынасу кезінде шақырылады. Бұл кезде оны орай өтуге мүмкіндік болмау керек;
- иландырылатындық. Мониторды талдауға және тестілеуге мүмкін болу үшін ол жинақы болуы керек.

17. **Қауіпсіздік өзегі** - қатынасым мониторының жүзеге асырылуы. Қауіпсіздік өзегі барлық қорғаныш тетіктерінің құрылу негізі болып табылады. Қатынасым мониторының аталған қасиеттерінен басқа қауіпсіздік өзегі өзінің өзгерместігіне кепілдік беруі керек.

18. **Қауіпсіздік периметрі** - сенімді есептеу базасының шекарасы. Оның ішіндегі сенімді, ал сыртындағы сенімсіз деп саналады. Сыртқы және ішкі әлемдер арасындағы байланыс ретқақпа арқылы жүзеге асырылады. Бұл ретқақпа сенімсіз немесе дұшпандық қоршауға қарсы тұра алуға қабілетті бар деп саналады.

19. **Қатынауды ерікті басқару** - жеке субъект немесе құрамына осы сцубъект кіретін топтың тұлғасын ескеру негізінде жасалған объектілерге қатынас құруды шектеу. Ерікті басқару - белгілі бір тұлға (әдетте, объектінің иесі) өзінің қарауынша басқа субъектілерге өзінің шешімі бойынша объектігі қатынас құру құқығын бере алады.

20. **Қауіпсіз жүйе** – белгілі бір тұлғалар немесе олардың атынан әрекет жасайтын үрдістер ғана ақпаратты оқу, жазу құрастыру және жою құқығына ие бола алатындай етіп ақпаратқа қол жеткізуді тиісті құралдар арқылы басқаратын жүйе.

21. **Құпиялылықты сақтау** –заңды түрде құқығы бар субъектілер ғана қатынай алатын ақпарттың күйі.

22. **Осалдық (Vulnerability)** – қауіптің пайда болуын мүмкін қылатын қорғау жүйесіндегі әлсіздік.

23. **Сенімді есептеу базасы** (СЕБ) - компьютерлік жүйенің қауіпсіздік саясаты жүзеге асыруға жауапты қорғаныш тектерінің жиынтығы. Компьтерлік жүйенің сенімділігіне баға беру үшін тек оның есептеу базасын қарастырып шықса жеткілікті болады. СЕБ негізгі міндеті - қатынасым мониторының міндетін орындау, яғни, объектілермен белгілі бір операциялар орындау болатындығын бақылау.

24. **Сенімді жүйе** - әр түрлі құпиялық дәрежелі ақпаратты қатынас құру құқығын бұзбай пайдаланушылар тобының бір уақытта өңдеуін қамтамасыз ету үшін жеткілікті аппаратық және бағдарламалық құралдарды қолданатын жүйе.

25. **Тәуекелдерді бағалау (Risk Assessment)** – тәуекелдердің теңестірулері, оларды сипаттайтын параметрлерді таңдау және осы параметрлермен бағаларды алу.

Практикалық жұмыс №3. Бақылау тапсырмалары

Берілген Тапсырма 1 және Тапсырма 2 орындап, 3-ші тапсырманы өз бетімен осы үлгілерге қатысты жаңа тапсырмалар түрінде әзірлеу

1 Тапсырма: төменде берілген жүйенің сипаттамаларына сүйеніп қауіпсіз критерийлер класын анықтаңыз

а) Қорғалған объекттің қауіпсіздік таңбасы бар (мысалы мына сипаттама B1 класының талабын білдіреді)

б) Қорғалған жүйеге кіру үшін идентификация мен аутентификация ұйымдастырылған

в) Жүйенің сырттан келген шабуылдарға қарсылық көрсету тиімді құралдары бар

г) Сенімді есептеуіш базасының құрылымы қауіпсіздікпен тиімді басқаруға бағытталған

2 Тапсырма: Жүйедегі қауіпсіздік жағдай сипатының қауіпсіз критерийінің сипаттамасына сәйкестігін орнатыңыз

Жүйедегі қауіпсіздік жағдай сипаттамасы	*Қауіпсіз критерийінің сипаттамасы*
Proxy сервері арқылы сіздің Интернет трафигіңіз бақылауда болады	Мекеменің қауіпсіздік саясаты болу керек
Пайдаланушы банкоматта пин код енгізгенде оны қағып әкетуден (перехват) қорғау ұйымдастырылады	Жүйенің қауіпсіздік администраторы үрдістермен тиімді басқару керек
Пайдаланушы жүйеде орындаған амалдарынан бас тарта алмайды	Аутентификациялауды тиімді қамтамасыз ету үшін сенімді байланыс арнасы болу керек
Мекеменің қызметкерлеріне ақпаратпен жұмыс жасау тәртібі анықталған, жауапкершілік бекітілген	Жүйеде үрдістерді тіркейтін журнал болу керек

Практикалық жұмыс №4.
Өзіндік қаскүнем үлгісін тұрғызу. Ұқсас үлгілерді келесі әдебиеттен көруге болады: Жантасова Ж.З. Сенім көрсетілген компьютерлік жүйелердің қауіпсіздік критерийлері. Оқу-әдістемелік құралы. Өскемен: Берел, 2015.-94 б.

Практикалық тапсырма №5.
Қажетті материалдарды келесі әдебиеттен көруге болады: Жантасова Ж.З. Сенім көрсетілген компьютерлік жүйелердің қауіпсіздік критерийлері. Оқу-әдістемелік құралы. Өскемен: Берел, 2015.-94 б.

Практикалық тапсрыма №6. Вирустан қорғау

Қажетті материалдарды келесі әдебиеттен көруге болады: Жантасова Ж.З. Сенім көрсетілген компьютерлік жүйелердің қауіпсіздік критерийлері. Оқу-әдістемелік құралы. Өскемен: Берел, 2015.-94 б.

Практикалық жұмыс №7. Ақпаратқа қатынауды шектеу үлгілері
Қажетті материалдарды келесі әдебиеттен көруге болады: Жантасова Ж.З. Сенім көрсетілген компьютерлік жүйелердің қауіпсіздік критерийлері. Оқу-әдістемелік құралы. Өскемен: Берел, 2015.-94 б.

Тапсырма 8. Тесттік бақылау. Үлгі түрінде берілген тесттік тапсырмалар
1) Техникалық программалық қорғау құралдары келесі қауіпсіздік қызметін (сервисін) қамтамасыз етпейді:
   A. Идентификациялау
   B. Экрандау
   C. Тунелдеу
   D. Бүтіндікті сақтау
   E. Кадрларды даярлау
2) Қауіпсіз жүйенің ішкі қамтамасыз ету жүйелеріне жатпайды:
   A. Криптографиялық
   B. Программалық
   C. Техникалық
   D. Желілік
   E. Ұйымдастырушылық
3) Қауіпсіз жүйенің ішкі қамтамасыз ету жүйелеріне жатпайды:
   A. Құқықтық
   B. Программалық
   C. Компьютерлік
   D. Ақпараттық
   E. Техникалық
4) Скремблер деп аталады:
   A. Дауыс сигналдарының құрылымын өзгертетін құралы
   B. Сенсорлық экран арқылы хабарлама таратушы құралы
   C. Көздің ішкі тор қабығы бойынша идентификациялау құралы
   D. Желіде қорғалған арнасын ұйымдастырушы құралы
   E. Вирусқа қарсы бағдарлама
5) Желіаралық терезенің (FireWall) негізгі қызметі:
   A. Вирустан қорғау
   B. Жұптылықты бақылау
   C. Желілік ақпараттық ағымдарды бақылау
   D. Бір желілік хаттаманы екінші хаттамаға енгізу
   E. Заңсыздық қатынауды анықтау

6) Қорғалған ішкі желілерді жобалауға жатады:
   A. Желілік ағымдарды сүзгілеу
   B. Аудит ұйымдастыру
   C. тунелдеу
   D. скремблерлеу
   E. биометриялық құралдарды қолдану
7) Идентификациялау, аутентификациялау әдістеріне жатпайды:
   A. Биометриялық құралдарын қолдану
   B. Турникеттер орнату
   C. логин мен пароль ұйымдастыру
   D. желіаралық терезе орналастыру
   E. электрондық цифрлық қолтаңба жасау
8) Жұптықты бақылау схемаларының негізгі функциясы:
   A. Вирусты зиянсыз ету
   B. Желі арқылы кедергілерден кездесетін қателерді анықтау
   C. Желі арқылы кедергілерден кездесетін қателерді түзету
   D. Вирустың шабуылын анықтау
   E. Дауыс сигналдарының құрылымын өзгерту
9) Келесі құрал скремблерлерге жатады:
   A. Scout
   B. TouchSafe TS-600
   C. Guard-Base
   D. FireWall
   E. PERCo-KTO2
10) Келесі құрал скремблерлерге жатады:
   A. Scout
   B. TouchSafe TS-600
   C. RFM
   D. FireWall
   E. Hands Free Voice Change
11) Деректердің конфиденциалдығы дегеніміз:
   A. Шифрлеу, деректердің қайта құру тәсілінің жиынтығы;
   B. Ашық мәтіннің қайта құрылуына қолданатын белгілер жиыны;
   C. Криптожүйенің параметрі;
   D. Көрсетілген деректердің құпия деңгейінің көрсеткіші;
   E. Ақпаратты қорғау мақсатында қайта құру алгоритмі;
12) Ақпараттық қауіпсіздікті бұзатын мүмкіндік:
   A. Шабуыл;
   B. Қауіптілік;
   C. Осалдылық;
   D. Әдейі істелмеген қателер;
   E. Ішкі құрылғылардың істен шығуы;
13) Апаттық жағдайлар қауіптіліктің қай түріне жатады?
   A. Ішкі;
   B. Әдейі істелген;
   C. Кездейсоқ;
   D. Статикалық;
   E. Динамикалық;
14) Қауіпсіздік дегеніміз не?
   A. Компьютерлік жүйенің компоненттерінің өзгерулерден, бұзылудан, қорғау жағдайы;
   B. Ақпараттың кездейсоқ және әдейі әртүрлі жағдайдағы өзгерулеруі;
   C. Ақпаратқа қатынауға құқы болмаса да қасақана қатынау;
   D. Объектінің шынайылығын тексеру;
   E. Ақпаратты қорғау мақсатын қайта құру алгоритмі.

15) Аутентификациялау дегеніміз:
   A. Ақпаратқа шабуыл жасалғанын анықтау процедурасы;
   B. Субъектінің объектке қатынауының заңдылығын анықтау;
   C. Ақпаратқа қатынау аймағын анықтау;
   D. Объектінің шынайылығын тексеру;
   E. Объектке заңды қатынаушыларының нақтылануы.
16) Идентификациялау дегеніміз:
   A. Ақпаратқа шабуыл жасалғанын анықтау процедурасы;
   B. Субъектінің объектке қатынауының заңдылығын анықтау;
   C. Ақпаратқа қатынау аймағын анықтау;
   D. Объектінің шынайылығын тексеру;
   E. Объектке заңды қатынаушыларының нақтылануы.
17) Авторизациялау немесе өкілеттік беру дегеніміз:
   A. Ақпаратқа шабуыл жасалғанын анықтау процедурасы;
   B. Субъектінің объектке қатынауының заңдылығын анықтау;
   C. Қолжетерлік ресурстарының аймағын анықтау;
   D. Объектінің шынайылығын тексеру;
   E. Объектке заңды қатынаушыларының нақтылануы.
18) Тұтастық дегеніміз:
   A. Саналы уақыт ішінде керекті ақпараттық қызмет алу мүмкіндігі;
   B. Ақпараттың шынайлылығы, бұзудан және заңсыз өзгертуден қорғанылуы;
   C. Ақпаратты заңсыз оқудан қорғау;
   D. Ақпаратқа шектеу қою;
   E. Ақпаратты ұрлаудан қорғау.
19) Конфиденциалдық дегеніміз:
   A. Саналы уақыт ішінде керекті ақпараттық қызмет алу мүмкіндігі;
   B. Ақпараттың шынайлылығы;
   C. Ақпаратты заңсыз қол жекізуден немесе оны оқудан қорғау;
   D. Ақпаратқа шектеу қою;
   E. Ақпаратты кездейсоқ бүрмалаудан қорғау;
20) Ақпаратты қорғау дегеніміз не?
   A. Ақпаратқа рұқсатсыз қатынаудың алдын алу;
   B. Ақпаратқа қатынау жолдарын шектеу;
   C. Ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені;
   D. Ақпараттың дер кезінде пайдаланылуын қамтамасыз етуге бағытталған шаралар кешені;
   E. Ақпаратты қосалқы сақтауыш құрылғыларға жазып қою.