БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
ҚАЗАҚСТАН РЕСПУБЛИКАСЫ

«Esil University» мекемесі

ESIL
UNIVERSITY

Бекітемін
«Esil University» мекемесінің ректоры
_____ А.А. Таубаев
«13» 02 _____2026ж.

БАҒДАРЛАМА

студенттерді қорытынды аттестаттау үшін кешенді емтихандар
6В06103 – «Ақпараттық технологиялар және деректерді қорғау» білім беру бағдарламасы бойынша «Компьютерлік желілердің қауіпсіздігі», «Қорғалған бағдарламалық қамтамасыз етуді жобалау», «Ақпаратты қорғаудың криптографиялық әдістері» пәндері бойынша

Астана, 2026

Кешенді емтихан бағдарламасы (қорытынды аттестаттау) 2022 жылғы 20 шілдедегі № 2 Жоғары және жоғары оқу орнынан кейінгі білімнің мемлекеттік жалпыға міндетті стандарты және ББББ 6В06103 – «Ақпараттық технологиялар және деректерді қорғау» модульдік білім беру бағдарламалары негізінде әзірленді.

Кешенді емтихан (қорытынды аттестаттау) бағдарламасы ақпараттық жүйелер және технологиялар кафедрасының отырысында талқыланды

Хаттама №6 «16» 01 2026 ж.

Кафедра меңгерушісі
«Ақпараттық жүйелер мен технологиялар» А.Ұ. Мұхиядин

Бағдарлама қолданбалы ғылымдар факультеті кеңесінің отырысында бекітілді

Хаттама №6 «19» 01 2026 ж.

Төраға А.А. Мухамеджанова

Бағдарлама «ESIL University» мекемесінің ғылыми-әдістемелік кеңесінің отырысында бекітілді

Хаттама №6 «20» 01 2026 ж.

Төреаға С.Б. Мақыш

Бағдарлама «ESIL University» мекемесінің Ғылыми кеңесінің отырысында бекітілді

Хаттама №8 «23» 02 2026 ж.

Кіріспе

6В06103 – «Ақпараттық технологиялар және деректерді қорғау» білім беру бағдарламасы бойынша студенттерді даярлау сапасы арнайы пәндер бойынша кешенді емтихан тапсыру нәтижелерімен куәландырылады. Студенттің оқу бағдарламасында қарастырылған теориялық материалды меңгеру деңгейін осы білім беру бағдарламасы бойынша жоғары және жоғары оқу орнынан кейінгі білім берудің мемлекеттік жалпыға міндетті стандартында қамтылған түлекке қойылатын жалпы талаптарды ескеретін кешенді емтихан айқындауы тиіс.

6В06103 білім беру бағдарламасы бойынша кешенді емтиханға – «Ақпараттық технологиялар және деректерді қорғау» үш пән бойынша сұрақтар енгізілген: «Компьютерлік желілердің қауіпсіздігі», «Қорғалған бағдарламалық қамтамасыз етуді жобалау», «Ақпаратты қорғаудың криптографиялық әдістері». Бағдарламада тақырыптардың мазмұны, сұрақтар тізімі және әр пән бойынша ұсынылатын әдебиеттер тізімі көрсетілген.

«Компьютерлік желілердің қауіпсіздігі» пәні бойынша бағдарлама

Тақырып 1. «Компьютерлік желілердің қауіпсіздігі» пәнінің негізгі түсініктері мен анықтамалары.

Ұғымдар: ақпарат, деректер, актив, қатер, осалдық, тәуекел. АҚ мақсаттары: құпиялық, тұтастық, қолжетімділік (CIA). Қауіпсіздік саясаты: мақсаты, құрылымы, талаптардың ұлгілері. Қорғау шаралары: ұйымдастырушылық, техникалық, физикалық. Негізгі қағидалар: ең аз артықшылық (minimal privileges), міндеттерді бөлу, тереңдетілген қорғаныс (defense-in-depth).

Тақырып 2. Желілер қауіпсіздігіне кіріспе. Желі мен деректер қауіпсіздігін жоспарлау.

Желі қауіпсіздігінің міндеттері және қолданылу саласы. Қорғауды жоспарлау кезеңдері: активтер → қатерлер → бақылаулар (контрольдер) → тексеру. Қолжетімділік саясатын және желіні пайдалану ережелерін жобалау. Defense-in-Depth моделі және қабатты қорғаныс. Инциденттерге дайындық: рөлдер, рәсімдер, хабарлау арналары.

Тақырып 3. Қауіпсіздік жүйелеріне арналған желілер: оңтайлы топологиялар.

Топологиялар: жұлдыз, сақина, ағаш, mesh, гибридті. Таңдау критерийлері: сенімділік, ақауға төзімділік, құны, масштабталуы. Желіні аймақтарға бөлу және сегментация (DMZ, VLAN, сенім аймақтары). Арналар/құрылғыларды резервтеу және жоғары қолжетімділік (HA). Критикалық сервистер және IoT/камералар үшін бөлек сегменттер бөлу.

Тақырып 4. Есептеу желісінің периметрі түсінігі. OSI моделі. Байланыс хаттамаларының стандартты стектері.

Периметр ұғымы: желі шекаралары, кіріс/шығыс трафикті бақылау. OSI моделі: деңгейлердің функциялары және деңгейлер бойынша типтік қауіптер. TCP/IP стекі және оны OSI-мен сәйкестендіру. Байланыс хаттамалары және деректерді тасымалдаудағы рөлі. Қорғаныс құралдары қай деңгейлерде қолданылады (фильтрация, шифрлау, қолжетімділікті басқару).

Тақырып 5. TCP/IP моделі. Желілік хаттама. TCP/IP, DNS, ICMP хаттамалары.

TCP/IP деңгейлері және олардың қызметі. TCP және UDP: ерекшеліктері, типтік қатерлер мен шабуылдар. DNS: мақсаты, негізгі қауіптер (ауыстыру, кэшті улау). ICMP: диагностика функциялары және теріс пайдалану тәуекелдері. Негізгі қорғаныс шаралары: ACL, ICMP-ті шектеу, DNS-ті қауіпсіз баптау.

Тақырып 6. Компьютерлік желілердің қауіпсіздігін қамтамасыз ету. Шабуыл түрлері және желілердің осалдығы.

Шабуылдарды жіктеу: пассивті/активті, сыртқы/ішкі. Типтік шабуылдар: MITM, spoofing, replay, session hijacking, DoS/DDoS. Ұғымдар: осалдық, эксплойт, шабуыл беті (attack surface). Қорғаныс әдістері: алдын алу, анықтау, әрекет ету (реагирование). Ұйымдастырушылық шаралар: оқыту, регламенттер, өзгерістерді бақылау.

Тақырып 7. Жергілікті және таратылған есептеу желілеріне қауіпсіздік қатерлері. Жергілікті желі қауіпсіздігін арттыру.

LAN және WAN қатерлерінің айырмашылығы (инсайдер тәуекелі). LAN-дағы арна деңгейі қатерлері (ARP/MAC/STP - кіріспе деңгейінде). LAN сегментациясы: VLAN, ACL, сервистер мен пайдаланушыларды бөлу. Желіге қолжетімділікті бақылау: 802.1X/NAC (жалпы түсінік). Желілік құрылғыларды қатайту (hardening), жаңарту, конфигурацияларды резервтік көшіру.

Тақырып 8. Желілік деңгейлердегі қауіпсіздік механизмдері.

L2 деңгейіндегі бақылаулар: Port Security, DHCP Snooping, Dynamic ARP Inspection, STP қорғанысы. L3 деңгейіндегі бақылаулар: anti-spoofing, ACL, маршрутизацияны қорғау. L4 деңгейіндегі бақылаулар: stateful inspection, порттар/қосылымдарды басқару. L7 деңгейіндегі бақылаулар: WAF, прокси, контентті фильтрациялау. Деңгейлер бойынша мониторинг және журналдау.

Тақырып 9. Желілік қауіпсіздік хаттамалары: ssh, ssl, tls, smtp, l2f, ipsec, l2tp, pptp, socks.

Әр хаттаманың мақсаты және қолданылу аймағы. SSH: қорғалған әкімшілендіру, қате баптаудан туатын тәуекелдер. SSL/TLS: арналарды шифрлау, сертификаттар, PKI-дің негізгі қағидалары. IPsec: tunnel/transport режимдері, IKE тағайындалуы (жалпы). L2TP/PPTP/L2F/SOCKS: қолдану сценарийлері және қауіпсіздік шектеулері.

Тақырып 10. Сымсыз желіні қорғау. Wi-Fi желілеріндегі қауіпсіздік.

WEP, WPA, WPA2 шифрлау. Wi-Fi қатерлері: rogue AP, evil twin, sniffing, deauth. WEP: әлсіз тұстары және неге қолданудан бас тартылады. WPA/WPA2: PSK және Enterprise (жалпы айырмашылық). Wi-Fi саясаты: бөлек SSID (қызметкерлер/қонақтар/IoT), VLAN арқылы сегментация. Мониторинг және шабуылдарды анықтау (WIDS/WIPS - жалпы), журналдау.

Тақырып 11. Корпоративтік желілерді қорғаудың заманауи технологиялары. Желіаралық экрандар, шабуылдарды анықтау жүйелері және виртуалды жеке желілер.

Желіаралық экрандар: түрлері және архитектурадағы орны (периметр/сегментация). IDS/IPS: мақсаты, айырмашылығы, орналастыру нұсқалары (SPAN/TAP/inline). VPN: сценарийлер (remote access/site-to-site), қолжетімділік саясаты. Интеграция: firewall + IDS/IPS + VPN + журналдау (SIEM - жалпы). Тәжірибелер: deny-by-default, өзгерістерді басқару, ережелерді тұрақты аудиттеу.

Тақырып 12. Корпоративтік желілердегі ішкі бұзушылар. Әсер ету әдістері.

Ішкі бұзушылардың түрлері: кездейсоқ/абайсыз/қасақана. Әдістер: құқықтарды теріс пайдалану, деректердің сыртқа шығуы, саботаж, lateral movement. Бақылаулар: least privilege, рөлдерді бөлу, PAM (жалпы түсінік). Мониторинг: мінез-құлықты талдау, журналдар, деректерге қолжетімділікті бақылау. Тергеу, дәлелдемелерді бекіту, алдын алу.

Тақырып 13. Қорғалған виртуалды жеке желілер (VPN) құру тұжырымдамасы.

VPN мақсаттары: құпиялық, тұтастық, аутентификация. Архитектура: шлюздер, маршрутизация, қолжетімділік нүктелері. Саясаттар: MFA, рөлдер мен құқықтар, split tunneling және шектеулер. Кілттер/сертификаттарды басқару (жалпы). Тәуекелдер мен шектеулер: құрылғының компрометациясы, утечкалар, клиентке сенім.

Тақырып 14. Осалдық сканерлері. Желілік шабуылдар. Корпоративтік желілерді ішкі бұзушылардан қорғау.

Осалдық сканерлерінің мақсаты және типтік нәтижелері (есептер). Сканерлеу түрлері: ішкі/сыртқы, аутентификацияланған/аутентификациясыз. Түзетуді приоритизациялау: тәуекел және актив критикалдылығы бойынша. Remediation: түзету → қайта тексеру → өзгерістерді бақылау. Ішкі бұзушыдан қорғаныс: аудит, журналдау, сегментация, DLP (жалпы).

Тақырып 15. Пассивті әсер ету әдістеріне қарсы тұру. Желілік трафикті тыңдау қаупіне қарсы тұру.

Пассивті әсерлер: sniffing, трафикті талдау, жасырын перехват. Тәуекелдер: ашық сегменттер, Wi-Fi, портты айнаға түсіру (mirroring), TAP. Негізгі шара - шифрлау: TLS, VPN, IPsec. Қосымша шаралар: сегментация, коммутаторларды қорғау, порттарды бақылау. Анықтау: аномалиялар, мониторинг құралдары, IDS/IPS мүмкіндіктері (не істей алады/не істей алмайды).

«Компьютерлік желілердің қауіпсіздігі» пәні бойынша сұрақтар

1. OSI моделінің физикалық деңгейінде жүзеге асырылатын желілік шабуылдар
2. Коммутаторларға шабуылдар: CAM-кестесін толтыру, STP, MAC, ARP-spoofing
3. Ақпаратты қорғаудың желілік құралдарының жіктелуі / классификациясы
4. Қауіпсіздік жүйелеріне арналған желілер: оңтайлы топологиялар
5. Жергілікті және таратылған есептеу желілеріне қауіпсіздік қатерлері, LAN қауіпсіздігін арттыру
6. Брандмауэр (Firewall): анықтама, түрлері
7. Шабуылдарды анықтау жүйелері және VPN (IDS/IPS + VPN байланысы)
8. Желілік хаттамалар: TCP/IP, DNS, ICMP
9. Кәсіпорын желісінде VLAN орнату
10. Көп қолданушы жұмыс режимі
11. Қорғалған виртуалды жеке VPN желілерін құру тұжырымдамасы
12. Ақпараттандыру объектісінде мәлімделген және нақты алынған ақпарат айырмашылықтарын іздеу
13. Windows Server желілік қызметтері, Windows-та маршруттау (маршрутизация)
14. Желілік инфрақұрылымды рұқсатсыз қол жеткізуден қорғау
15. Microsoft Windows брандмауэрі, интернеттегі желілік экрандардың жұмыс істеу мәселелері
16. Осалдық сканерлері, желілік шабуылдар, корпоративтік желіні ішкі

зиянкестерден қорғау
17. STP негізінде ақауға төзімді LAN құру, арна деңгейіндегі шабуылдардан қорғау
18. Корпоративтік желілердегі ішкі зиянкестер: әсер ету әдістері
19. Пассивті әсер етуге қарсы тұру: желілік трафикті тыңдау (sniffing) қаупі
20. VPN протоколдарын салыстыру: SSH, IPsec, L2TP, PPTP
21. VPN протоколын таңдау критерийлері
22. Домен орнату және Group Policy (топтық саясат)
23. Кәсіпорын желісінде IP протоколын орнату
24. IPSec желілік қауіпсіздік протоколы және VPN пайдалану
25. Деректерді беру арналарын криптографиялық қорғау (рұқсатсыз қол жеткізуден)
26. Веб-қосымшалардың осалдығын анықтау ерекшеліктері
27. Microsoft Windows желісінде қолжетімділікті шектеу және желілік ресурстарды басқару
28. Қазіргі корпоративтік желілердің қауіпсіздік мәселелері
29. Желінің аппараттық және бағдарламалық қамтамасыз етуі
30. Келесі буын желілік экраны (NGFW)
31. Желінің жүйелік бағдарламалық қамтамасыз етуі
32. TCP/IP протоколдары (TCP/UDP) қауіптері
33. DNS қауіптері: cache poisoning, spoofing, туннелдеу - анықтау және қорғаныс (DNSSEC/DoT/DoH).
34. ICMP: толық бұғаттау дұрыс па? Қауіп/пайда балансы, қандай типтерді рұқсат ету керек?
35. IP spoofing: желіде қалай байқалады және anti-spoofing (uRPF, ACL) қалай құрылады?
36. Control Plane Protection: маршрутизатордың басқару жазықтығын қорғау тәсілдері.
37. DDoS түрлері (volumetric, protocol, application): әрқайсысына қарсы қорғаныс шаралары.
38. Firewall анықтамасы: функциялары, желідегі орны (perimeter/segmentation) және саясат құру қағидасы.
39. Application firewall және WAF: айырмашылығы, веб-қосымшаға қатысты қандай қауіптерді жабады?
40. NGFW: DPI, App-ID, IPS, URL filtering, SSL inspection - қайсысы қандай қауіпке жауап береді?
41. SIEM жүйесі
42. IDS/IPS + VPN бірге қолдану: VPN трафигін қай жерде тексеру керек (tunnel before/after decrypt).
43. IPsec: AH vs ESP және transport vs tunnel mode — айырмашылығы, қолдану мысалы.
44. VPN протоколын таңдау критерийлері: қауіпсіздік, қолдау, NAT traversal, өнімділік, масштабтау.
45. Криптографиялық алгоритм таңдау: AES, ChaCha20, RSA/ECDSA, DH/ECDH

46. ҚР-ның «Ақпараттандыру туралы» Заңы аясында ақпараттық жүйе иесі/операторының негізгі жауапкершіліктерін желілік қауіпсіздік тұрғысынан талдаңыз (қорғау, қолжетімділік, инциденттерге әрекет).
47. «Дербес деректер және оларды қорғау туралы» Заң талаптарын желіде іске асыру: деректерді жинау/өңдеу/сақтау, қолжетімділікті шектеу, журналдау, үшінші тұлғаға беру тәуекелі. (Практикалық саясат пен техникалық бақылаулар ұсыныңыз.)
48. «Мемлекеттік құпиялар туралы Заң» контекстінде желі архитектурасын қалай өзгертесіз? (оқшаулау, сегментация, рұқсат деңгейі, тасымалдау арнасы, құпия ақпаратпен жұмыс станциялары).
49. «Ақпаратқа қол жеткізу туралы» Заң талаптары мен ақпараттық қауіпсіздік арасында қайшылық туған кезде (ашықтық VS қауіпсіздік) шешім қабылдау алгоритмін ұсыныңыз.
50. Бұзушыны ішкі және сыртқы деп бөлудің критерийлерін атаңыз. Әрқайсысына тән мақсат, мүмкіндіктер және тәуекел деңгейін салыстырыңыз.
51. Тәуекел (risk) ұғымын анықтаңыз және «қауіптің сәтті іске асуындағы ықтимал зиян» ретінде түсіндіріңіз.
52. Сапалық және сандық тәуекел бағалаудың айырмашылығын айтыңыз: қай кезде қайсысы тиімді және неге?
53. Тәуекелдерді категориялау (критикалық/жоғары/орта/төмен) қалай жасалады және әр категория үшін қандай басқару тактикасы қолданылады?
54. Тәуекел картасын құру кезінде жүйелік тәсілді қалай қолданасыз: факторларды толық анықтау, көпдеңгейлі талдау, әдістерді интеграциялау.
55. Тәуекелді өңдеудің 4 стратегиясын (avoid/reduce/transfer/accept) нақты мысалдармен түсіндіріңіз және таңдауға әсер ететін факторларды атаңыз.
56. ҚР «Ақпараттандыру туралы» Заңы ақпараттық жүйелерді құру/пайдалану/қорғау тұрғысынан нені реттейді? Ұйым үшін қандай міндеттер туындайды?
57. ҚР «Дербес деректер және оларды қорғау туралы» Заңы бойынша деректерді жинау/сақтау/өңдеу/қорғауда операторға қандай талаптар қойылады?
58. ҚР «Байланыс туралы» Заңының қауіпсіздік пен мемлекеттік органдар байланысы тұрғысындағы маңызын түсіндіріңіз (инфрақұрылым, қауіпсіздік, қорғаныс, құқық қорғау аспектілері).
59. Ақпараттық қауіпсіздік аудитін жүргізудің кезеңдерін (жоспарлау → ақпарат жинау → талдау → есеп) сипаттап, әр кезеңде қандай әдістер/құралдар қолданылатынын түсіндіріңіз.
60. NAC (Network Access Control) енгізу: BYOD/IoT/қонақ құрылғыларын желіге жіберу саясатын жасаңыз (802.1X, posture check, quarantine VLAN, guest portal).
61. Желіні басқару арнасының қауіпсіздігі: SSH, HTTPS, SNMPv3, AAA,

management VLAN, out-of-band management ұйымдастырудың толық схемасын ұсыныңыз.

62. SNMP және желілік мониторинг қауіпсіздігі: SNMPv2c тәуекелдері, SNMPv3 артықшылығы, қауіпті конфигурациялар және hardening шаралары.
63. Логтау және корреляция: firewall/IDS/AD/DNS/VPN/Proxy логтарын жинау архитектурасын жасаңыз (retention, time sync/NTP, нормализация, корреляция мысалы).
64. Network segmentation vs microsegmentation: классикалық VLAN/ACL және microsegmentation (policy-based) тәсілдерін салыстырып, қай инфрақұрылымда қайсысы тиімді екенін негіздеңіз.
65. DMZ жобалау: веб-сервер/почта/DNS сияқты сыртқы сервистер үшін DMZ схемасы
66. Backup/DR (RPO/RTO): корпоративтік желі үшін қалпына келтіру жоспарын құрыңыз (критикалық сервистерді ранжирлеу, резерв арналар, failover, тестілеу).
67. DLP және деректердің сыртқа шығуы (exfiltration): e-mail/web/USB/VPN арналарында бақылау қоюдың тәсілдерін салыстырыңыз (DLP, CASB, proxy, firewall, UEBA).
68. SSL/TLS қауіпсіз баптау: әлсіз шифрлар/протоколдарды өшіру, сертификат айналымы, HSTS/OCSP stapling сияқты параметрлердің қауіпсіздікке әсерін түсіндіріңіз.
69. Secure email және фишингке қарсы қорғаныс: SPF/DKIM/DMARC рөлі, пошта шлюзі, sandbox, пайдаланушыны оқыту — интеграцияланған қорғаныс моделін жасаңыз.
70. Қауіпсіздік инциденті кезіндегі дәлелдеме (evidence) жинау: журнал тұтастығын сақтау, chain of custody, уақыт синхронизациясы, оқшаулау әрекеттерінің реті.
71. Қосымшалардың желілік қауіпсіздігі: reverse proxy/WAF, rate limiting, API gateway, mTLS қолданудың артықшылықтары және шектеулері (нақты веб/API сценариймен).
72. Идентификация, аутентификация, авторизация, аудит ұғымдарын анықтаңыз. Әр кезеңнің мақсаты қандай және олар бір-бірімен қалай байланысады?
73. DAC, MAC, RBAC, ABAC модельдерін салыстырыңыз: бақылау принципі, икемділік, әкімшілендіру күрделілігі, қорғаныс деңгейі, қолданылатын орта. Ұйым үшін модель таңдаудың негіздемесін келтіріңіз.
74. Логин/пароль арқылы идентификация неге осал (фишинг, brute-force, әлеуметтік инженерия)? Пароль саясатын және қосымша қорғаныс бақылауларын ұсыныңыз.
75. MFA, 2FA және бірфакторлы аутентификацияның айырмашылығын түсіндіріңіз. Қайсысы қандай жүйелер үшін міндетті болуы керек және неге?
76. Биометриялық аутентификация мен токен/смарт-карта негізіндегі

аутентификацияны салыстырыңыз: қауіпсіздік, ыңғайлылық, инфрақұрылым талабы, құпиялылық тәуекелі.

77. Авторизация механизмдері: қолжетімділік матрицасы, ACL, capability-тізімдер. Масштабталуы, басқарылуы, құқықты қайтарып алу қиындығы бойынша салыстырыңыз.
78. Бұлтты ортада қолжетімділікті басқару: IAM, федеративті қолжетімділік, үздіксіз верификация/Zero Trust қағидалары. Бұлтта дәстүрлі периметрлік тәсіл неге жеткіліксіз?
79. Қолжетімділік аудиті және мониторингі: журналдарда қандай міндетті өрістер болуы керек және не үшін журналдардың тұтастығын/орталықтандырылған сақталуын қамтамасыз ету маңызды?
80. PAM (Privileged Access Management) деген не? "Ең аз привилегия" қағидасын, привилегияны уақытша көтеру (JIT), привилегияланған сессияларды мониторинг/жазу қалай іске асады?
81. OSI моделі және байланыс хаттамаларының стандартты стектері
82. Корпоративтік желілерді қорғаудың заманауи технологиялары
83. Network segmentation vs microsegmentation: классикалық VLAN/ACL және microsegmentation (policy-based) тәсілдерін салыстырып, қай инфрақұрылымда қайсысы тиімді екенін негіздеңіз.
84. DMZ жобалау: веб-сервер/почта/DNS сияқты сыртқы сервистер үшін DMZ схемасын жасап, inbound/outbound ережелерін және журналдау саясатын көрсетіңіз.
85. Ransomware-ға қарсы желілік қорғаныс: lateral movement-ті тоқтату (SMB/WinRM/RDP), сегментация, least privilege, backup (immutable/offline) стратегиясын жүйелі түрде сипаттаңыз.
86. Backup/DR (RPO/RTO): корпоративтік желі үшін қалпына келтіру жоспарын құрыңыз (критикалық сервистерді ранжирлеу, резерв арналар, failover, тестілеу).
87. Wireless корпоративтік дизайн: бірнеше SSID (corp/guest/iot), VLAN-дарға бөлу, WPA2-Enterprise/WPA3, WIDS/WIPS, rogue AP анықтау және инцидент сценарийі.
88. Vulnerability management lifecycle: сканерлеу → тәуекелге байлау → remediation → қайта тексеру. CVSS ғана жеткілікті ме? Эксплуатация ықтималдығын қалай ескересіз?
89. Penetration testing нәтижесін енгізу: табылған осалдықтарды risk map-қа кірістіріп, приоритеттеу және түзету жол картасын (roadmap) құрыңыз.
90. Қауіпсіздік инциденті кезіндегі дәлелдеме (evidence) жинау: журнал тұтастығын сақтау, chain of custody, уақыт синхронизациясы, оқшаулау

Ұсынылатын әдебиеттер тізімі

Негізгі әдебиеттер

1. Чернега В.С. Методы и средства защиты периметра локальных компьютерных сетей: учебно-методическое пособие по выполнению лабораторных работ по дисциплине «Безопасность компьютерных сетей». –

Севастополь: СевГУ, 2024. – 38 с. (электронный вариант: э-библиотека Esil University - https://cloud.esil.edu.kz).
2. Белоусова Е.С. Основы построения локальных сетей. Лабораторный практикум: учебно-методическое пособие. – Минск: БГУИР, 2020. – 103 с.: ил. – ISBN 978-985-543-562-5. (электронный вариант: э-библиотека Esil University - https://cloud.esil.edu.kz).
3. Макаренко С.И. Защита компьютерных сетей и телекоммуникаций: учебное пособие. – СПб.: Наукоёмкие технологии, 2024. – 311 с. – ISBN 978-5-907618-79-4. (электронный вариант: э-библиотека Esil University - https://cloud.esil.edu.kz).
4. Мартынов А.П., Мартынова И.А., Русаков А.А. Информационная безопасность и защита информации: учебное пособие. - 2-е изд. - Москва: Ай Пи Ар Медиа, 2024. - 130 с. - ISBN 978-5-4497-2349-9. (электронный вариант: э-библиотека Esil University - https://cloud.esil.edu.kz).
5. Платунова С.М., Елисеев И.В., Авксентьева Е. Ю. Реализация комплексной безопасности в корпоративных сетях: шлюз безопасности как универсальное средство для обеспечения защиты данных и предотвращения вторжений. - СПб.: Университет ИТМО, 2020. - 64 с. (электронный вариант: э-библиотека Esil University - https://cloud.esil.edu.kz).

Қосымша әдебиеттер

1. Joseph Migga Kizza. Computer Communications and Networks. Springer London Heidelberg New York Dordrecht 2015 – 545 p. ISBN 978-1-4471-6653-5 ISBN 978-1-4471-6654-2 (eBook), DOI 10.1007/978-1-4471-6654-2
2. Н.А. Руденков [и др.].. Технологии защиты информации в компьютерных сетях: учебное пособие - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. - 368 с. - ISBN 978-5-4497-0931-8. - Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. - URL: http://www.iprbookshop.ru/102069.html
3. Фороузан Б.А. Криптография и безопасность сетей: учебное пособие / Фороузан Б.А.. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. - 776 с. - ISBN 978-5-4497-0946-2.
4. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии) Издательство «Горячая линия-Телеком» 2018
5. Олифер Виктор, Олифер Наталья О-54 Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. - СПб.: Питер, 2021. - 1008 с.: ил. - (Серия «Учебник для вузов»). ISBN 978-5-4461-1426-9

«Қорғалған бағдарламалық қамтамасыз етуді жобалау» пәні бойынша бағдарлама

Тақырып 1. Қауіпсіз Ақпараттық жүйелерді жобалаудың жалпы ережелері

Қауіпсіз ақпараттық жүйелердің түсінігі мен мақсаты. Қорғалған бағдарламалық жасақтаманы жобалау принциптері мен кезеңдері. Ақпараттық жүйенің өмірлік циклі кезеңдеріндегі қауіпсіздіктің рөлі. Ақпараттық жүйелерді жобалау әдістемесінің негіздері.

Тақырып 2. Ақпараттық жүйелерді жобалау әдіснамасының негіздері

Ақпараттық жүйелерді жобалау әдістемесінің түсінігі. Құрылымдық және объектіге бағытталған тәсілдер. Ақпараттық жүйелердің өмірлік циклінің модельдері: каскадты, итеративті, спиральды, икемді әдістемелер. Өмірлік циклде ақпараттық қауіпсіздік талаптарын есепке алу.

Тақырып 3. Дизайн негіздері

Ақпараттық жүйелерді жобалау түсінігі. Жобалау кезеңдері мен нәтижелері. Функционалды модельдеу. Ақпараттық жүйенің idef0 функционалды моделінің мақсаты мен ерекшеліктері.

Тақырып 4. Ақпараттық жүйенің жіктелуі

Ақпараттық жүйелерді мақсаты, ауқымы, деректерді өңдеу режимі және қауіпсіздік деңгейі бойынша жіктеу. Ақпарат қауіпсіздігінің өзекті қатерлері туралы түсінік. Қауіптерді анықтау әдістемесі. Ақпараттық жүйенің қауіп-қатер моделін жасау.

Тақырып 5. Ақпараттық жүйенің idef0 функционалды моделі (AS-IS)

AS-IS моделінің мақсаты. Ақпараттық жүйенің ағымдағы күйінің функционалды моделін құру. Ақпаратты өңдеу процестерін талдау және қауіпсіздік тұрғысынан осалдықтарды анықтау.

Тақырып 6. Ақпараттық жүйеде қолданылатын ақпаратты қорғау шаралары мен құралдарына қойылатын талаптар

Ақпаратты қорғаудың ұйымдастырушылық, бағдарламалық және техникалық шараларына қойылатын талаптар. Ақпаратты қорғау құралдарына қойылатын талаптар. Қорғау шараларының анықталған қатерлерге және нормативтік талаптарға сәйкестігі.

Тақырып 7. Ақпараттық жүйенің idef0 функционалды моделі (to-BE)

To-BE моделінің мақсаты. Ақпараттық жүйенің мақсатты күйін жобалау. Функционалды модельде ақпаратты қорғау шараларының көрінісі. AS-IS және TO-BE модельдерін салыстырмалы талдау.

Тақырып 8. Қауіпсіз ақпараттық жүйенің idef0 функционалды моделі (to-BE)

Қауіпсіз ақпараттық жүйенің функционалды моделін құру. Ақпаратты қорғау механизмдерін деректерді өңдеу процестеріне біріктіру. Қорғау құралдары мен шараларын таңдаудың негіздемесі.

Тақырып 9. Қауіпсіз ақпараттық жүйенің Use Case мінез-құлық диаграммалары

Use Case диаграммаларының мақсаты. Диаграммалардың негізгі

элементтері. Пайдаланушы және әкімші функцияларының сипаттамасы. Қауіптер мен қауіпсіздік талаптарын талдау үшін Use Case диаграммаларын пайдалану.

Тақырып 10. Ақпараттық жүйеде ақпаратты қорғау құралдарын орнату және баптау

Ақпаратты қорғау құралдарын енгізу процестері. Бағдарламалық және аппараттық құралдарды орнату және конфигурациялау. Пайдалану құжаттамасын әзірлеу. Пайдалану барысында ақпаратты қорғауды қамтамасыз ету жөніндегі іс-шараларды айқындайтын құжаттар.

Тақырып 11. Statechart қауіпсіз ақпараттық жүйесінің мінез-құлық диаграммалары

Statechart диаграммаларының мақсаты. Қауіпсіз ақпараттық жүйедегі күйлер мен ауысулардың сипаттамасы. Қорғаныс механизмдерін іске асыруда жүйенің мінез-құлқын модельдеу үшін диаграммаларды қолдану.

Тақырып 12. Қауіпсіз ақпараттық жүйенің белсенділік мінез-құлық диаграммалары

Белсенділік диаграммаларының мақсаты. Ақпаратты өңдеу процестерін және қауіпсіздікті қамтамасыз ету процестерін модельдеу. Activity және Statechart диаграммаларын салыстыру.

Тақырып 13. Аттестаттау сынақтарының бағдарламасы мен әдістемесі

Ақпараттық жүйелерді аттестаттау сынақтарының мақсаты. Аттестаттау бағдарламасы мен әдістемесінің құрылымы. Сынақтарды өткізу және нәтижелерді ресімдеу тәртібі.

Тақырып 14. Ақпараттық жүйені пайдалану ортасының қауіпсіздігін қамтамасыз ету

Ақпараттық жүйені пайдалану ортасы туралы түсінік. Пайдалану ортасының қауіпсіздігін қамтамасыз ету шаралары. Ақпаратты қорғау жүйесін басқару. Қауіпсіздік әкімшісінің міндеттері.

Тақырып 15. Құрылымдық диаграммалар

Сынып диаграммалары және олардың мақсаты. Орналастыру диаграммалары. Қауіпсіз бағдарламалық жасақтаманы жобалау кезінде құрылымдық диаграммаларды қолдану. Құпия сипаттағы ақпаратты мұрағаттау. Машиналық тасымалдағыштардан деректерді және қалдық ақпаратты жою.

«Қорғалған бағдарламалық қамтамасыз етуді жобалау» пәні бойынша сұрақтар

1. 1. Қауіпсіз ақпараттық жүйе ұғымы және оның мақсаты.
2. Қорғалған бағдарламалық жасақтаманы жобалаудың мақсаттары мен міндеттері.
3. Қауіпсіз Ақпараттық жүйелерді жобалаудың негізгі принциптері.
4. АЖ жобалау кезеңдеріндегі ақпараттық қауіпсіздіктің рөлі.
5. Ақпараттық жүйелерді жобалау әдістемесінің түсінігі.
6. Ақпараттық жүйелерді жобалаудың негізгі тәсілдері.
7. АЖ жобалау әдіснамасындағы қауіпсіздік орны.

8. Ақпараттық жүйенің өмірлік циклі туралы түсінік.
9. Ақпараттық жүйелердің өмірлік циклінің негізгі модельдері.
10. АЖ өмірлік циклінің әртүрлі кезеңдеріндегі қауіпсіздік талаптарын есепке алу.
11. Ақпараттық жүйелерді жобалау түсінігі.
12. Ақпараттық жүйені жобалаудың негізгі кезеңдері.
13. АЖ жобалау кезінде функционалды модельдеудің мақсаты.
14. Ақпараттық жүйенің функционалды моделі туралы түсінік.
15. IDEF0 белгісі және оның мақсаты.
16. Idef0 функционалды моделінің негізгі элементтері.
17. IDEF0 диаграмма ережелері.
18. Қорғалған бағдарламалық жасақтаманы жобалаудағы idef0 рөлі.
19. Ақпараттық жүйелерді мақсаты бойынша жіктеу.
20. Ақпараттық жүйелердің масштабы мен архитектурасы бойынша жіктелуі.
21. Ақпараттық жүйелерді қорғау деңгейі бойынша жіктеу.
22. Ақпарат қауіпсіздігіне төнетін қатерлер ұғымы.
23. Ақпарат қауіпсіздігіне төнетін қауіптердің жіктелуі.
24. Ақпарат қауіпсіздігінің өзекті қатерлері туралы түсінік.
25. Ақпарат қауіпсіздігінің өзекті қатерлерін анықтау әдістемесі.
26. Ақпараттық жүйенің қауіп-қатер моделі туралы түсінік.
27. Қауіп моделін әзірлеу кезеңдері.
28. Қорғалған бағдарламалық жасақтаманы жобалау кезінде қауіп-қатер моделін қолдану.
29. Ақпараттық жүйенің as-is моделінің мақсаты.
30. Idef0 as-is функционалды моделін құру.
31. AS-IS моделіне негізделген осалдықтарды талдау.
32. АЖ жобалау кезінде as-is моделінің шектеулері.
33. Ақпараттық жүйенің TO-BE мақсатты моделінің мақсаты.
34. AS-IS және TO-BE модельдерінің айырмашылығы.
35. To-BE моделіндегі ақпаратты қорғау шараларының көрінісі.
36. Қорғалған бағдарламалық жасақтаманы жобалау кезінде to-BE қолданудың артықшылықтары.
37. Қауіпсіз ақпараттық жүйе ұғымы.
38. Idef0 қауіпсіз IC функционалды моделінің ерекшеліктері.
39. Ақпаратты қорғау механизмдерін функционалды модельдерге біріктіру.
40. TO-BE қауіпсіз АЖ моделінде қорғау шараларын таңдаудың негіздемесі.
41. Ақпараттық жүйеде ақпаратты қорғау шараларына қойылатын талаптар.
42. Ақпаратты қорғау құралдарына қойылатын талаптар.
43. Қорғау шараларының анықталған қатерлерге сәйкестігі.
44. Қорғау құралдарын таңдау кезінде нормативтік талаптарды есепке алу.

45. Use Case мінез-құлық диаграммаларының түсінігі.
46. Қауіпсіз АЖ-да Use Case диаграммаларын тағайындау.
47. Use Case диаграммаларының негізгі элементтері.
48. Қауіпсіздік талаптарын талдау үшін Use Case пайдалану.
49. Use Case диаграммаларындағы пайдаланушылар мен әкімшілердің рөлі.
50. АЖ-да ақпаратты қорғау құралдарын орнату процестері.
51. Бағдарламалық және техникалық қорғаныс құралдарын орнату.
52. Ақпаратты қорғау жүйесін енгізу кезеңдері.
53. Ақпаратты қорғау жөніндегі пайдалану құжаттамасы.
54. Ақпаратты қорғауды қамтамасыз ету жөніндегі оператордың құжаттары.
55. Statechart диаграммаларының мақсаты.
56. Ақпараттық жүйенің қауіпсіздік күйлерін көрсету.
57. Жүйенің реакцияларын модельдеу үшін Statechart пайдалану.
58. Белсенділік диаграммаларының мақсаты.
59. Activity көмегімен қауіпсіздік процестерін модельдеу.
60. Activity және Statechart диаграммаларын салыстыру.
61. Аттестаттау сынақтарының бағдарламасы мен әдістемесі туралы түсінік.
62. Ақпараттық жүйенің аттестациялық сынақтарын жүргізу мақсаттары.
63. Аттестациялық сынақтар бағдарламасының құрылымы.
64. Аттестаттау сынақтарын өткізу тәртібі.
65. Аттестаттау сынақтарының нәтижелерін ресімдеу.
66. Ақпараттық жүйені пайдалану ортасы туралы түсінік.
67. АЖ пайдалану ортасының қауіпсіздігінің негізгі қауіптері.
68. Пайдалану ортасының қауіпсіздігін қамтамасыз ету шаралары.
69. Ақпаратты қорғау жүйесін басқару.
70. Қауіпсіздік әкімшісінің функциялары.
71. Ақпараттық жүйенің құрылымдық диаграммалары туралы түсінік.
72. Сынып диаграммаларының мақсаты.
73. Қорғалған бағдарламалық жасақтаманы жобалау кезінде сынып диаграммаларын қолдану.
74. Орналастыру диаграммаларының мақсаты.
75. Орналастыру диаграммаларында АЖ архитектурасының көрінісі.
76. Құпия сипаттағы ақпаратты мұрағаттау ұғымы.
77. Құпия ақпаратты мұрағаттауға қойылатын талаптар.
78. АЖ - да мұрағаттық ақпаратты сақтау процестері.
79. Ақпаратты жою ұғымы.
80. Машиналық ақпарат құралдарынан деректерді өшіру әдістері.
81. Қалдық ақпаратты жою.
82. Машиналық ақпарат тасығыштарды жоюға қойылатын талаптар.
83. Ақпаратты жою процестерін құжаттау.
84. Ақпаратты қорғау жүйесіндегі деректерді мұрағаттау мен жоюдың

рөлі.

85. Қорғалған бағдарламалық жасақтаманы жобалаудың кешенді тәсілі.

86. Функционалды, мінез-құлық және құрылымдық модельдердің байланысы.

87. Қорғалған Ақпараттық жүйелерді жобалау кезіндегі қателер.

88. Қорғалған бағдарламалық жасақтаманы жобалау сапасын бағалау критерийлері.

89. Қорғалған АЖ жобалауды дамытудың өзекті бағыттары.

90. Ұйымның ақпараттық қауіпсіздігін қамтамасыз етудегі жобалаудың рөлі.

Ұсынылатын әдебиеттер тізімі

Негізгі әдебиеттер

1 Duisebekova R.S. and etc. Database in IS: textbook / L.S. Kopbossyn.- Almaty, 2016.-329 p.

2 Гвоздева Т.В. Проектирование информационных систем. Стандартизация: Учебное пособие / Т.В. Гвоздева Б.А. Баллод. - СПб.: Лань, 2019. - 252.

3 Дыбская В.В. Проектирование системы распределения в логистике: Монография / В.В. Дыбская. - М.: Инфра-М, 2019. - 277.

4 Конюх В.Л. Проектирование автоматизированных систем производства: Учебное пособие / В.Л. Конюх. - М.: Курс, 2018. - 64.

5 Трусов А.В. технология проектирования информационных систем: учебное пособие.-М.: Инфра-Инженерия, 2023.-244 с.

Қосымша әдебиеттер

1 Белов В.В. Проектирование информационных систем: Учебник / В.В. Белов. - М.: Академия, 2018. - 144.

2 Жук А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, 2А.И. Тимошкин. - М.: Риор, 2017. - 480 с.

3 Хетагуров Я.А. Проектирование автоматизированных систем обработки информации и управления (АСОИУ) / Я.А. Хетагуров. - М.: БИНОМ. Лаборатория знаний, 2015. - 240.

4 Хорольский В.Я. Проектирование и эксплуатация энергоустановок телекоммуникационных систем: Учебное пособие / В.Я. Хорольский, А.Б. Ершов. - М.: Форум, 2019. - 285.

5 Хорев П. Б. Программно-аппаратная защита информации. Учебное пособие. М.: Инфра-М. 2022. 327.

«Ақпаратты қорғаудың криптографиялық әдістері» пәні бойынша бағдарлама

Тақырып 1. Компьютерлік жүйеде ақпаратты қорғау мәселелері.

Қазіргі компьютерлік жүйелердегі ақпаратты қорғаудың негізгі мәселелері. Компьютерлік жүйелердегі осалдықтардың себептері. Адам факторының ақпаратты қорғау деңгейіне әсері. Компьютерлік жүйелердегі Ақпарат қауіпсіздігінің бұзылуының салдары.

Тақырып 2. Ақпаратты қорғаудың құқықтық негізі.

Ақпаратты қорғаудың құқықтық негізінің түсінігі мен маңызы. Ақпараттық қауіпсіздік саласындағы құқықтық реттеудің негізгі бағыттары. Ақпаратты қорғау саласындағы заңнаманы бұзғаны үшін жауапкершілік. Ақпараттық қауіпсіздікті қамтамасыз етудегі нормативтік-құқықтық актілердің рөлі.

Тақырып 3. Ақпаратты өңдеудің автоматтандырылған жүйелерінің қауіпсіздігінің негізгі мәселелері.

Криптографиялық принциптер. Ақпаратты өңдеудің автоматтандырылған жүйелерінің қауіпсіздігінің негізгі қауіптері. Ақпаратты өңдеудің автоматтандырылған жүйелерінің қауіпсіздігін қамтамасыз ету ерекшеліктері. Ақпараттық қоғамның криптографиялық принциптері. Ақпаратты өңдеудің автоматтандырылған жүйелеріндегі ақпаратты қорғау үшін криптографияның маңызы.

Тақырып 4. Криптографияның негіздері мен түсініктері.

Криптография ұғымы және оның негізгі міндеттері. Криптографияның негізгі терминдері мен түсініктері. Криптографияның дамуының қысқаша тарихы. Ақпаратты қорғау жүйелеріндегі криптографияның қазіргі маңызы.

Тақырып 5. Кілтті Криптография. Симметриялық криптожүйелер.

Құпия кілтпен криптография ұғымы. Классикалық симметриялы криптожүйелердің жұмыс принциптері. Симметриялық шифрлаудың артықшылықтары мен кемшіліктері. Симметриялық криптожүйелерді қолдану салалары.

Тақырып 6. Симметриялық Алгоритмдер.

Симметриялық шифрлау алгоритмдерінің негізгі сипаттамалары. Қазіргі симметриялы криптожүйелер. Симметриялық алгоритмдердің криптографиялық төзімділік критерийлері. Симметриялық шифрлау алгоритмдерінің жұмыс режимдері.

Тақырып 7. Ашық кілттерді тарату жүйесі.

Ашық кілттерді тарату жүйесінің мақсаты. Ашық кілттерді тарату жүйелерінің жұмыс істеу принциптері. Криптографиялық кілттерді тарату кезіндегі қауіпсіздік қатерлері. Қауіпсіздікті қамтамасыз етудегі ашық кілт инфрақұрылымының рөлі.

Тақырып 8. Диффи-Хеллман Жүйесі.

Диффи–Хеллман алгоритмінің мақсаты мен принциптері. Диффи–Хеллман жүйесінде дискретті көрсеткіштерді қолдану. Диффи–Хеллман алгоритмінің артықшылықтары мен шектеулері. Диффи–Хеллманды қолданудағы қауіптер мен қорғаныс шаралары.

Тақырып 9. Ақпараттың дәлдігі.

Ақпараттың дәлдігі және оның мәні туралы түсінік. Ақпараттың дәлдігіне әсер ететін факторлар. Ақпараттың дәлдігін қамтамасыз ету және бақылау әдістері. Ақпараттық жүйелердегі ақпараттың бұрмалануының салдары.

Тақырып 10. Аппараттық шифрлау.

Аппараттық шифрлаудың түсінігі мен мақсаты. Аппараттық шифрлаудың артықшылықтары мен кемшіліктері. Аппараттық шифрлауды қолдану салалары. Ақпаратты қорғау жүйесіндегі аппараттық шифрлаудың рөлі.

Тақырып 11. Бағдарламалық жасақтаманы шифрлау.

Ақпаратты бағдарламалық шифрлау ұғымы. Бағдарламалық жасақтаманы шифрлаудың артықшылықтары мен кемшіліктері. Аппараттық және бағдарламалық жасақтаманы шифрлауды салыстыру. АЖ-да бағдарламалық жасақтаманы шифрлауды қолдану.

Тақырып 12. Кілттермен операциялар.

Криптографиялық кілттің өмірлік циклі. Криптографиялық кілттермен негізгі операциялар. Кілттерді сақтау және қорғау талаптары. Криптографиялық кілттерді бұзудың салдары.

Тақырып 13. Гамма-тәсілмен келісім-шарт жасау.

Криптографиядағы гамма-тәсіл ұғымы. Қорғалған шартты белгілеу принциптері. Гамма тәсілінің артықшылықтары мен шектеулері. Ақпаратты қорғау жүйелерінде гамма тәсілін қолдану.

Тақырып 14. Интернет арқылы шекті жабудан қорғау әдістері.

Маргиналды жабылу және оның қаупі туралы түсінік. Интернет желісі арқылы шабуылдардан қорғау әдістері. Ақпаратты қорғаудың желілік құралдары. Интернеттегі ақпаратты қорғаудың кешенді тәсілі.

Тақырып 15. Бағдарламаларды зерттеуден қорғау. Антивирустық қорғаныс.

Бағдарламалық жасақтаманы талдаудан қорғау әдістері. Антивирустық қорғаныс түсінігі мен түрлері. Қазіргі заманғы антивирустық құралдардың жұмыс принциптері. Ақпараттық қауіпсіздік жүйесіндегі антивирустық қорғаудың рөлі.

«Ақпаратты қорғаудың криптографиялық әдістері» пәні бойынша сұрақтар

1. Ақпараттық қауіпсіздік ұғымы және оның негізгі мақсаттары.
2. Ақпараттың негізгі қасиеттері: құпиялылық, тұтастық және қол жетімділік.
3. Компьютерлік жүйелердегі ақпаратты қорғаудың заманауи мәселелері.
4. Ақпарат қауіпсіздігіне төнетін қауіптердің жіктелуі.
5. Ақпараттық қауіпсіздікке ішкі және сыртқы қауіптер.
6. Ақпараттық жүйелердің осалдығы және олардың пайда болу себептері.
7. Ақпаратты қорғауды қамтамасыз етудегі адам факторының рөлі.
8. Ақпараттық қауіпсіздікті бұзудың салдары.
9. Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі бағыттары.
10. Ақпаратты қорғаудың кешенді тәсілі.

11. Қазақстан Республикасында ақпаратты қорғаудың құқықтық негізі.
12. Ақпараттық қауіпсіздік саласындағы негізгі нормативтік-құқықтық актілер.
13. Мемлекеттік, қызметтік және коммерциялық құпия ұғымы.
14. Ақпаратты қорғау саласындағы заңнаманы бұзғаны үшін жауапкершілік.
15. Ақпараттық қауіпсіздікті қамтамасыз етудегі стандарттар мен регламенттердің рөлі.
16. Ақпаратты қорғаудың ұйымдастырушылық шаралары.
17. Ұйымның ақпараттық қауіпсіздік саясаты.
18. Ақпаратты қорғау процестерін Құжаттамалық қамтамасыз ету.
19. Ақпараттық қауіпсіздікті бақылау және аудит.
20. Ақпаратты қорғауды қамтамасыз етудегі персоналдың рөлі.
21. Ақпаратты өңдеудің автоматтандырылған жүйесі туралы түсінік.
22. Ақпаратты өңдеудің автоматтандырылған жүйелерінің қауіпсіздігінің негізгі қауіптері.
23. Ақпаратты өңдеудің автоматтандырылған жүйелеріндегі ақпаратты қорғау ерекшеліктері.
24. Ақпаратты өңдеудің автоматтандырылған жүйелерін қауіпсіздік деңгейі бойынша жіктеу.
25. Ақпаратты өңдеудің автоматтандырылған жүйелерін қорғаудың ұйымдастырушылық және техникалық шаралары.
26. Автоматтандырылған жүйенің қауіп моделі.
27. Ақпараттың құпиялылығын бұзу қаупі.
28. Ақпараттың тұтастығын бұзу қаупі.
29. Ақпараттың қолжетімділігін бұзу қаупі.
30. Ақпараттың қауіпсіздігін қамтамасыз етудегі криптографияның рөлі.
31. Криптография ұғымы және оның негізгі міндеттері.
32. Криптографияның негізгі терминдері мен түсініктері.
33. Криптографияның даму тарихы және негізгі кезеңдері.
34. Ақпараттық қоғамның криптографиялық принциптері.
35. Криптографиялық төзімділік ұғымы.
36. Ақпаратты қорғаудың криптографиялық әдістерінің жіктелуі.
37. Ақпаратты қорғау әдісі ретінде шифрлау.
38. Шифрды шешу және оның мақсаты.
39. Ақпараттық қауіпсіздік жүйесіндегі криптографияның орны.
40. Криптографияны қолданудың шектеулері мен мәселелері.
41. Құпия кілтпен криптография ұғымы.
42. Симметриялық криптожүйелердің жұмыс принципі.
43. Классикалық симметриялық шифрлау алгоритмдері.
44. Қазіргі симметриялы криптожүйелер.
45. Симметриялық шифрлаудың артықшылықтары.
46. Симметриялы криптожүйелердің кемшіліктері.
47. Симметриялық алгоритмдердің криптографиялық төзімділігін бағалау критерийлері.

48. Симметриялық шифрлау алгоритмдерінің жұмыс режимдері.
49. Симметриялық алгоритмдерді қолдану салалары.
50. Деректерді қорғаудағы симметриялы криптографияның рөлі.
51. Криптографиялық кілт ұғымы.
52. Криптографиялық кілттің өмірлік циклі.
53. Криптографиялық кілттермен негізгі операциялар.
54. Криптографиялық кілттерді құру.
55. Криптографиялық кілттерді сақтау және қорғау.
56. Кілттерді қорғалған байланыс арналары арқылы беру.
57. Криптографиялық кілттердің бұзылуы және оның салдары.
58. Криптографиялық кілттерді жаңарту және еске түсіру.
59. Криптографиялық кілттерді басқару саясаты.
60. Ақпаратты қорғау жүйесіндегі кілттерді басқарудың рөлі.
61. Криптографиялық кілттерді бөлу мәселесі.
62. Ашық кілттерді тарату жүйесі.
63. Ашық кілт жүйелерінің жұмыс істеу принциптері.
64. Ашық кілт инфрақұрылымы (PKI).
65. PKI мақсаты және негізгі компоненттері.
66. Диффи-Хеллман алгоритмі және оның мақсаты.
67. Диффи–Хеллман алгоритмінде дискретті көрсеткіштерді қолдану.
68. Диффи–Хеллман алгоритмінің артықшылықтары мен шектеулері.
69. Кілттерді бөлу кезіндегі қауіпсіздік қатерлері.
70. Кілттерді тарату арналарын қорғау жолдары.
71. Аппараттық шифрлаудың түсінігі мен мақсаты.
72. Аппараттық шифрлаудың артықшылықтары.
73. Аппараттық шифрлаудың кемшіліктері.
74. Ақпаратты бағдарламалық шифрлау ұғымы.
75. Бағдарламалық жасақтаманы шифрлаудың артықшылықтары.
76. Бағдарламалық жасақтаманы шифрлаудың кемшіліктері.
77. Аппараттық және бағдарламалық жасақтаманы шифрлаудың салыстырмалы сипаттамасы.
78. Ақпараттық жүйелер үшін шифрлау құралдарын таңдау.
79. Шифрлаудың жүйенің жұмысына әсері.
80. Ақпаратты қорғаудың кешенді жүйесіндегі шифрлаудың рөлі.
81. Ақпараттың дәлдігі және оның мәні туралы түсінік.
82. Ақпараттың дәлдігіне әсер ететін факторлар.
83. Ақпараттың тұтастығын қамтамасыз ету әдістері.
84. Деректердің тұтастығы мен дәлдігін бақылау.
85. Бағдарламалық жасақтаманы талдаудан қорғау ұғымы.
86. Бағдарламаларды зерттеуден және кері инженериядан қорғау әдістері.
87. Антивирустық қорғаныс ұғымы.
88. Антивирустық бағдарламалардың түрлері.
89. Қазіргі заманғы антивирустық құралдардың жұмыс принциптері.
90. Ақпараттық қауіпсіздік жүйесіндегі антивирустық қорғаудың рөлі.

Ұсынылатын әдебиеттер тізімі

Негізгі әдебиеттер

1. Peter, H. Gregory Blocking Spam For Business For Dummies® (For Dummies (Computers)) / Peter H. Gregory. - Москва: ИЛ, 2016. - 636 б.
2. Бабаш, А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2016. - 240 б.
3. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 б.
4. Бабенко, Л.К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко. - М.: Гелиос АРВ, 2015. - 921 б.
5. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2016. - 186 б.

Қосымша әдебиеттер

1. Зубов, А.Н. Математика кодов аутентификации / А.Н. Зубов. - М.: Гелиос АРВ, 2014. - 319 б.
2. Криптография: скоростные шифры / А. Молдовян и др. - М.: БХВ-Петербург, 2014. - 496 б.
3. Кузьмин, Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2013. - 192 б.
4. Литвинская, О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. - М.: КноРус, 2015. - 168 б.
5. Осмоловский, С. А. Стохастическая информатика. Инновации в информационных системах / С.А. Осмоловский. - М.: Горячая линия - Телеком, 2012. - 322 б.