**«7M120303 – Киберқылмысқа қарсы іс-қимыл» білім беру бағдарламалары бойынша ғылыми-педагогикалық магистратураға қабылданатын кандидатқа қойылатын жалпы талаптар**

**Ақпараттық жүйелер мен технологиялардың негіздері -** саласында үміткерден ақпараттық жүйелердің мақсаты мен міндеттерін, ақпараттық жүйелердің функцияларын, аппараттық құралдар және виртуалдандыруды, деректер базасының өнімділігін оңтайландыру және реттеуді, желінің қауіпсіздігін, ақпаратты қорғау құралдарын, бұлтты технологиялар және Big Data, ақпараттық жүйелердегі перспективалар мен сын-қатерлерін, логистика мен көлікте АЖ қолданудын, ақпараттық жүйелердің тиімділігін бағалау әдістері туралы білімі болуы тиіс.

**Киберқылмыс технологиялары -** саласында үміткерден киберқылмыс түрлерін, киберқылмыспен күресудің инновациялары мен технологияларын, технологияның дамуы және жаңа қауіптерін, белгілі бір платформаларға шабуылдарды, әлеуметтік инженерия түрлері, киберқылмыстағы жасанды интеллект, зиянды бағдарламаны талдаудағы жасанды интеллект, хакерлерге арналған құралдар мен ресурстарды, киберқылмыскерлердің психологиялық түрлерін, жала жабу және жалған ақпарат таратуды түсіну талап етіледі.

**Сандық криминалистика** – саласындаүміткерден криминалистиканың дербес саласы ретінде цифрлық криминалистиканың түсінігі, мәні және негізгі сипаттамаларын, цифрлық дәлелдемелерді өңдеу саласындағы халықаралық келісімдер мен стандарттар (Будапешт конвенциясы және т.б.) талдауды, дәлелдемелердің рұқсат етілген нысандары: аудио-бейне жазбалар, фото және киноматериалдар, электрондық, цифрлық және басқа да материалдық тасымалдаушылардағы басқа материалдарды, қылмыстық процесте пайдалану үшін компьютерлік техникадан дәлелдемелерді алу, талдау және түсіндіру процесін, криминалистикалық рұқсат етілген құжаттаманы құрудың және алынған нәтижелерді тексерудің маңыздылығы туралы білімі болуы тиіс.

**Ақпараттық жүйелер мен технологиялардың негіздері**

**ЕМТИХАН СҰРАҚТАРЫ**

1. Ақпараттық жүйе дегеніміз не және оның ұйым қызметіндегі негізгі функциялары қандай?
2. Ақпараттық технологиялардың негізгі құрамдас бөліктері қандай және олар өзара қалай әрекеттеседі?
3. Ақпараттық жүйелерде дерекқорлардың рөлі қандай және дерекқорлардың негізгі түрлері қандай?
4. Операциялық, басқарушылық және стратегиялық ақпараттық жүйелер арасындағы айырмашылық неде?
5. Ақпараттық технологиялар ұйымның бизнес-процестерінің тиімділігін арттыруға қалай ықпал етеді?
6. Ақпараттық жүйелерді жіктеудің негізгі критерийлері қандай және олар қандай жүйелерді қамтиды?
7. Транзакциялық ақпараттық жүйелер (ТАЖ) мен басқарушылық ақпараттық жүйелер (БАЖ) арасындағы айырмашылық неде?
8. Ақпараттық жүйенің архитектурасын қандай компоненттер құрайды және олардың жүйе жұмысындағы рөлі қандай?
9. Операциялық ақпараттық жүйелердің (ОАЖ) функциялары қандай және олар ұйым ішінде қандай міндеттерді шешеді?
10. Стратегиялық ақпараттық жүйелер (САЖ) дегеніміз не және олар ұйымның ұзақ мерзімді мақсаттарына жетуге қалай ықпал етеді?
11. Ақпараттық жүйелердің аппараттық құралдары дегеніміз не және олар қандай негізгі жабдық санаттарына бөлінеді?
12. Ақпараттық жүйенің аппараттық архитектурасында орталық процессордың (ОП) рөлі қандай?
13. Жедел жад (RAM) қандай функциялар атқарады және ол ақпараттық жүйенің өнімділігіне қалай әсер етеді?
14. Ақпараттық жүйелерде қатты дискілер мен твердотельді жинақтауыштардың (SSD) арасындағы негізгі айырмашылықтар қандай?
15. Аппараттық құралдар мен бағдарламалық жасақтама қалай өзара әрекеттеседі және бұл өзара әрекеттесу жүйе жұмысы үшін неліктен маңызды?
16. Бағдарламалық жасақтама (БЖ) дегеніміз не және ол қандай негізгі санаттарға бөлінеді?
17. Операциялық жүйелер қандай функциялар атқарады және олар аппараттық құралдар мен қосымшаларды басқаруда қандай рөл атқарады?
18. Жүйелік бағдарламалық жасақтама мен қолданбалы бағдарламалық жасақтаманың айырмашылығы неде?
19. Бағдарламалық жасақтама ақпараттық жүйелердің қауіпсіздігіне қалай әсер етеді және бұл қауіпсіздікті қамтамасыз ету үшін қандай шаралар қабылдануы мүмкін?
20. Бағдарламалық жасақтама өмірлік циклының (БЖӨЦ) негізгі кезеңдері қандай және олардың әрқайсысы әзірлеу мен қолдауда қандай мәнге ие?
21. Дерекқор дегеніміз не және оны басқа деректер сақтау форматтарынан ерекшелейтін негізгі сипаттамалар қандай?
22. Реляциялық және нереляциялық дерекқорлардың айырмашылығы неде?
23. Дерекқорларды басқару жүйесінің (ДББЖ) рөлі қандай және ол қандай негізгі функцияларды орындайды?
24. Деректер моделі дегеніміз не және қандай модельдер (мысалы, реляциялық, объектілік) ДББЖ-де жиі қолданылады?
25. ДББЖ-дегі транзакциялар қалай жұмыс істейді және олар деректер тұтастығын қамтамасыз ету үшін қандай ACID қасиеттеріне ие болуы тиіс?
26. Ақпараттық жүйені жобалаудың негізгі кезеңдері қандай және әрбір кезеңде қандай міндеттер шешіледі?
27. Ақпараттық жүйеге қойылатын функционалдық және функционалдық емес талаптар дегеніміз не және оларды жобалау сатысында неліктен ескеру маңызды?
28. Деректерді модельдеу мен процестерді модельдеу арасындағы айырмашылық неде?
29. Ақпараттық жүйелерді жобалаудың негізгі әдістері қандай және олардың басты ерекшеліктері неде?
30. Ақпараттық жүйелерді жобалаудағы құжаттама дегеніміз не және жобалаудың әртүрлі кезеңдерінде қандай құжаттар жасалуы қажет?
31. Ақпараттық жүйенің қауіпсіздігі оны жобалау кезінде қалай қамтамасыз етіледі?
32. Компьютерлік желілер дегеніміз не және олардың қандай негізгі түрлері бар (LAN, WAN, MAN)
33. Компьютерлік желілердің негізгі компоненттері қандай және олар ақпараттық жүйелердің жұмысында қандай рөл атқарады?
34. Желілік хаттамалар дегеніміз не және олар желідегі құрылғылар арасында өзара әрекеттесуді қалай қамтамасыз етеді?
35. Сымсыз технологиялардың жұмыс істеу принциптері қандай және олар сымды желілермен салыстырғанда қандай артықшылықтарға ие?
36. Ақпараттық жүйелердегі желілік технологияларды киберқауіптерден қорғау үшін қандай қауіпсіздік шаралары қолданылуы тиіс?
37. Бұлттық технологиялар дегеніміз не және бұлттық қызметтердің қандай негізгі модельдері бар (IaaS, PaaS, SaaS)?
38. Бизнесте және ұйымдарда бұлттық технологияларды пайдаланудың негізгі артықшылықтары қандай?
39. Виртуализация дегеніміз не және ол бұлттық технологиялармен қалай байланысты?
40. Бұлттық архитектураның негізгі компоненттері қандай және олар бұлттық шешімдерді орналастыруда қандай рөл атқарады?
41. Бұлттық технологияларды пайдалануда қандай тәуекелдер мен мәселелер туындауы мүмкін және оларды қалай азайтуға болады?
42. Ақпараттық қауіпсіздік дегеніміз не және ол ақпараттық жүйелерді қорғау контексінде қандай мақсаттарды көздейді?
43. Ақпараттық жүйелерге төнетін қауіптердің қандай негізгі түрлері бар және әрқайсысына мысалдар келтіріңіз.
44. Ақпараттық жүйелердің қауіпсіздігін қамтамасыз ету үшін қолданылатын негізгі ақпаратты қорғау құралдары қандай?
45. Ақпараттық қауіпсіздік саясаты дегеніміз не және ол қандай негізгі элементтерді қамтуы тиіс?
46. Ақпараттық жүйелерді қорғау контексінде желілер мен коммуникация қауіпсіздігінің негізгі аспектілері қандай?
47. Big Data (Үлкен деректер) дегеніміз не және оны сипаттайтын негізгі ерекшеліктер қандай?
48. Үлкен деректер жүйелерінің архитектурасының негізгі компоненттері қандай?
49. Үлкен деректерді өңдеу және талдау үшін қандай құралдар мен технологиялар қолданылады?
50. Үлкен деректер технологияларын бизнесте және басқа салаларда пайдаланудың қандай артықшылықтары бар?
51. Big Data аясында қандай деректерді талдау әдістері мен алгоритмдері қолданылады?
52. Жасанды интеллект (ЖИ) дегеніміз не және оның негізгі санаттары мен технологиялары қандай?
53. Жасанды интеллект ақпараттық жүйелерде процестерді автоматтандыру үшін қалай қолданылады?
54. Ақпараттық жүйелерде деректерді өңдеу мен талдауға қандай машиналық оқыту әдістері қолданылады?
55. Жасанды интеллект ақпараттық жүйелердің қауіпсіздігін жақсартуға қалай ықпал етеді?
56. Ақпараттық жүйелерге ЖИ енгізудің негізгі артықшылықтары мен кемшіліктері қандай?
57. Ақпараттық жүйелерді бизнес-процестерге енгізудің негізгі кезеңдері қандай?
58. Ұйымдарда ақпараттық жүйелерді енгізуге байланысты қандай негізгі мәселелер мен тәуекелдер туындайды?
59. Ақпараттық жүйелерді бизнес-процестерге біріктіру арқылы компаниялар қандай артықшылықтарға қол жеткізе алады?
60. Ақпараттық жүйелерді енгізудің бизнестегі тиімділігін қалай бағалауға болады?
61. Жаңа ақпараттық жүйені компаниядағы қолданыстағы IT-шешімдермен үйлестіру қалай қамтамасыз етіледі?
62. Ақпараттық жүйелердің тиімділігін бағалау әдістері қандай?
63. Ақпараттық жүйені енгізу немесе жаңғырту туралы шешім қабылдауға қаржылық бағалау қалай әсер етеді?
64. Ақпараттық жүйелердің тиімділігін бағалауда ескерілуі тиіс негізгі қаржылық емес аспектілер қандай?
65. Ақпараттық жүйелердің тиімділігін бағалау кезінде қандай проблемалар мен тәуекелдер туындауы мүмкін?
66. Ұйымдағы ақпараттық жүйенің тиімділігін бағалау процесінің кезеңдері қандай?
67. Алдағы 5–10 жылда ақпараттық технологиялардың дамуындағы негізгі үрдістер қандай?
68. Үлкен деректер мен аналитика технологиялары бизнес-процестердің тиімділігін арттыру контексінде қалай дамуы мүмкін?
69. Ақпараттық жүйелер денсаулық сақтау саласында клиенттерге қызмет көрсету сапасын қалай жақсартады?
70. Қаржы секторында қауіпсіздік пен операциялар тиімділігін арттыру үшін қандай ақпараттық технологиялар қолданылады?

**ҰСЫНЫЛАТЫН ӘДЕБИЕТТЕР ТІЗІМІ**

**Негізгі әдебиеттер:**

1. Pierre Kosovich. Basic concepts of information and communication technologies. Lecture notes. ITdesk.info. Open society for the exchange of ideas «Reflections», Zagreb, 2020. - 17 p.
2. Гохберг Г.С. Информационные технологии: учебник для студ. учреждений сред. проф. образования / Г.С.Гохберг, А.В.Зафиевский, А. А. Короткин. — 9-е изд., перераб. и доп. — М.: Издательский центр «Академия», 2021 — 240 с.
3. Kuznetsov, S.D. Fundamentals of Modern Databases. Information and Analytical Materials of the Information Technologies Center. Viewed 28 January 2015. [electronic resource]. – Access mode, http; // Citforum.ru/ index.html, free. – Sagle. From the screen [circulation date December 2020].
4. Cambridge IGCSE ICT. Book. – Cambridge, 2016. – 439 p.
5. Egiedi T.M., Muto S., Guseva Т.V. Standardization in the Field of ICT: «Green» Strategy. Competence 6/10/2013. [electronic resource]. – Access mode www.diros.n1, free. – Ver. from the screen [circulation date December 2020].
6. Orlov S.A. Software Engineering. Textbook for high schools. – 5th edition updated and updated. The standard of the third generation. – St. Petersburg: Peter, 2020. – 640 p.
7. Шыныбеков Д.А., Ускенбаева Р.К., Сербин В.В., Дузбаев Н.Т., Молдагулова А.Н., Дуйсебекова К.С., Сатыбалдиева Р.Ж., Хасенова Г.И., Б. Урмашев. Информационно-коммуникационные технологии. 1-е изд. Учебник. – Алматы, 2020. – 559 стр.
8. D. Shvnvbekov, R. Uskenbayeva. V. Serbin,N. Duzbayev,A. Moldagulova, K. Duysebekova. R. Satybaldiyeva, G. Khasenova, B. Urmashev. Information and Communication Technologies. Textbook. In 2 parts. Part 2. 1st edition - Almaty: IITU, 2017.
9. Абрамкина О.А. Информационно-коммуникационные технологии. Конспекты лекций для студентов специальности 5В100200 – Системы информационной безопасности.–Алматы: АУЭС, 2017 - 67 с.
10. Nurpeisova T.B., Kaidash I.N. N 98 Information and Communication Technologies: Textbook. / T.B. Nurpeisova, I.N. Kaidash – Almaty: «Bastau», 2020. – 480 p.

**Қосымша әдебиеттер:**

1. A.V. Kuzin, S.V. Levonesov, Databases. Textbook for high school. (5 th ed.) – Publishing Academy: 2019. – 317 p.
2. Дырдина Е.В. Информационно-коммуникационные технологии в компетентностно-ориентированном образовании: учебно-методическое пособие / Е.В. Дырдина, В.В. Запорожко, А.В. Кирьякова. – Оренбург: ООО ИПК «Университет», 2018 – 227 с.
3. Rechinsky A.V., Sergeev S.F. Development of User Interfaces. Usability testing of information system interfaces. – SPb.: Publishing house of Polytechnic. University, 2019. – 145 p. – (Tutorial).
4. Kretschmer, T. (2018), “Information and Communication Technologies and Productivity Growth: A Survey of the Literature”, OECD Digital Economy Papers, No. 195, OECD Publishing.
5. Пьер Косович. Основные понятия информационных коммуникационных технологий. Конспект лекций. ITdesk.info. Открытое общество для обмена идеями «Отражения», Загреб, 2020–17 с.
6. June J. Parsons and Dan O.ja, New Perspectives on Computer Concepts 16th Edition - Comprehensive, Thomson Coarse Technology, a division of Thomson Learning, Inc Cambridge, MA. COPYRIGHT € 2014.
7. Hans J. Schnoll E-Govemment: Information, Technology, and Transformation: Information, Technology, and Transformation (Routledge, Mar 12, 2015 - Political Science - 343 pages).
8. Vijav K. Vaishnavi, Vjjav K. Vaishnavi, William Kuechlcr Design Science Research Methods and Patterns: Innovating Information and Communication Technology, 2nd Edition 2015 by CRC Press.
9. Tanenbaum E., Bos H. T18 Modern operating systems. 4 th ed. – St. Petersburg: Peter, 2015. – 1120 p.: ill. – (Series «Classic Computer Science»).
10. Go For IT English Reading: учебное пособие по английскому языку для бакалавров 1–2 курса факультета информационных систем и технологий очной формы обучения / сост. Л. В. Корухова, Н.Н. Новосельцева. – Ульяновск: УлГТУ, 2016. – 168 с.

**КИБЕРҚЫЛМЫС ТЕХНОЛОГИЯЛАРЫ**

**ЕМТИХАН СҰРАҚТАРЫ**

1. Киберқылмыс дегеніміз не және оның негізгі санаттары қандай?
2. Компьютерлік жүйелерді бұзу және деректерді ұрлау үшін киберқылмыскерлер жиі қолданатын технологиялар мен әдістер қандай?
3. Киберқылмыс контексіндегі әлеуметтік инженерия дегеніміз не және ол шабуылдарды жүзеге асыруда қалай қолданылады?
4. Зиянды бағдарламалар қалай жұмыс істейді және олардың негізгі түрлері қандай?
5. Киберқылмыстардан қорғану үшін қандай шаралар қолдануға болады?
6. Киберқылмыс ұғымын анықтаңыз және олар қандай негізгі санаттарға бөлінеді?
7. Кибералаяқтық дегеніміз не?
8. Киберкеңістікте зияткерлік меншікке қарсы жасалатын қылмыстарға қандай әрекеттер жатады?
9. Жеке тұлғаға қарсы жасалатын киберқылмыстар қалай жіктеледі?
10. Кибертерроризм дегеніміз не және ол кибервандализмнен несімен ерекшеленеді?
11. Киберқылмыс аясындағы әлеуметтік инженерия дегеніміз не?
12. Психологиялық факторлар әлеуметтік инженерия тиімділігіне қалай әсер етеді?
13. Әлеуметтік инженерия шабуылдарында эмоцияны манипуляциялау қандай рөл атқарады?
14. Претекстинг дегеніміз не және ол киберқылмыста қалай қолданылады?
15. Киберқылмыскерлер шабуыл кезінде жиі қолданатын психологиялық осалдықтар қандай?
16. Жасанды интеллект (AI) кибершабуылдарды автоматтандыру үшін қалай қолданылуы мүмкін?
17. Deepfake дегеніміз не және бұл технология киберқылмыста қалай қолданылуы мүмкін?
18. AI-дың киберқылмыста қолданылуынан қорғану үшін қандай шаралар қабылдануы мүмкін?
19. Кибершабуылдардан қорғаныс тиімділігін арттыруда AI қандай рөл атқарады?
20. Киберқылмыста AI қолданылуы тергеу мен қылмыскерді анықтауды қалай күрделендіруі мүмкін?
21. DDoS-шабуылы дегеніміз не және ол веб-сайт немесе желі жұмысына қалай әсер етуі мүмкін?
22. SQL-инъекция дегеніміз не және ол желілік шабуылдарда қалай қолданылуы мүмкін?
23. Фишинг дегеніміз не және фишингтік шабуылдардың қандай түрлері бар?
24. MITM (Man-in-the-Middle) шабуылы дегеніміз не және ол желі қауіпсіздігіне қандай қатер төндіреді?
25. Сниффинг дегеніміз не және ол желілік шабуылдарда қалай қолданылады?
26. Хакерлік мәдениеттегі «ақ шляпалар» мен «қара шляпалар» дегеніміз не?
27. Руткит дегеніміз не және ол хакерлік шабуылдарда қалай қолданылады? Оларды анықтау және жою әдістері қандай?
28. Әлеуметтік инженерия дегеніміз не және ол жүйені бұзуда қалай қолданылады?
29. Brute force шабуылы дегеніміз не және ол парольдерді бұзуда қалай қолданылады? Мұндай шабуылдардан қорғану шаралары қандай?
30. Фишинг дегеніміз не және хакерлер оны аккаунттарды бұзу үшін қалай қолданады?
31. Адамдарды киберқылмысқа итермелейтін негізгі психологиялық факторлар қандай?
32. Киберқылмыскерлер мотивациясында идеологиялық және саяси көзқарастар қандай рөл атқарады?
33. Киберқылмыскерлерге тән тұлғалық ерекшеліктер қандай?
34. Әлеуметтік оқшаулану мен әлеуметтік қолдаудың болмауы киберқылмысқа тартылуға қалай әсер етеді?
35. Қаржылық мотивтер киберқылмыскерлердің мотивациясында қандай рөл атқарады?
36. Фишинг криптовалютаны ұрлау үшін қалай қолданылуы мүмкін?
37. Смарт-келісімшартқа шабуыл дегеніміз не және ол криптовалюта ұрлығына қалай әкелуі мүмкін?
38. Криптоджекинг дегеніміз не және қаскөйлер бұл әдісті криптовалюта табу үшін қалай пайдаланады?
39. MITM-шабуылдары криптовалюта ұрлау үшін қалай қолданылуы мүмкін?
40. SIM-сваппинг дегеніміз не және ол криптовалюта ұрлау үшін қалай пайдаланылады?
41. Зияткерлік меншік ұғымы нені білдіреді?
42. Авторлық құқық дегеніміз не және ол цифрлық ортада қалай бұзылуы мүмкін?
43. Патент дегеніміз не және патенттік құқықты бұзудың салдары қандай?
44. Тауар белгісі дегеніміз не және ол қалай бұзылуы мүмкін?
45. Коммерциялық құпия зияткерлік меншікте қандай рөл атқарады және оны бұзу не болып саналады?
46. Кибербуллинг дегеніміз не және ол цифрлық ортада қандай түрлерде кездеседі?
47. Киберсталкинг дегеніміз не және ол кибербуллингтен несімен ерекшеленеді?
48. Киберкеңістікте жеке тұлғаны ұрлау (identity theft) нені білдіреді?
49. «Ревендж порн» дегеніміз не және ол қандай құқықтық және этикалық мәселелерді қозғайды?
50. Вишинг дегеніміз не және ол жеке тұлғаға қарсы киберқылмыс ретінде қалай қолданылады?
51. Ұйымдасқан киберқылмыс дегеніміз не және ол жеке тұлғалар жасаған қылмыстардан несімен ерекшеленеді?
52. Ұйымдасқан киберқылмыстық топтар өз операцияларын жүзеге асыру үшін жиі қолданатын әдістер мен технологиялар қандай?
53. Ұйымдасқан киберқылмыстық топтар даркнет пен көлеңкелі нарықты өз қызметтерінде қалай пайдаланады?
54. Ұйымдасқан киберқылмыстық топтар жиі жасайтын қылмыстардың қандай түрлері бар?
55. Ұйымдасқан киберқылмысқа қарсы қандай күрес шаралары қолданылуы мүмкін?
56. «Сындарлы инфрақұрылым» деген ұғым нені білдіреді және оған қандай нысандар жатады?
57. Сындарлы инфрақұрылымға бағытталуы мүмкін кибершабуылдардың қандай түрлері бар?
58. SCADA-жүйелері дегеніміз не және олар неге кибершабуылдардың нысанасына айналады?
59. Сумен жабдықтау жүйелеріне жасалған сәтті кибершабуылдың ықтимал салдары қандай?
60. Сындарлы инфрақұрылымды кибершабуылдардан қорғау үшін қандай қауіпсіздік шаралары қолданылуы мүмкін?
61. Киберсоғыс дегеніміз не және ол кибертерроризмнен несімен ерекшеленеді?
62. «Киберқару» дегеніміз не және ол киберсоғыста қалай қолданылады?
63. Кибертерроризм аясында қандай кибершабуылдар қолданылуы мүмкін?
64. Киберсоғыс пен кибертерроризмде жалған ақпарат пен дезинформация қандай рөл атқарады?
65. «Олқылықтарды жауапты түрде жариялау» ұғымы нені білдіреді және ол киберқауіпсіздік саласындағы маңызды этикалық қағидат ретінде несімен ерекшеленеді?
66. Киберқылмыс пен киберқауіпсіздік аясында жасанды интеллект қолданылуына байланысты қандай этикалық дилеммалар туындауы мүмкін?
67. Желі трафигін бақылау және талдау құралдарын қолдануда қандай этикалық мәселелер пайда болуы мүмкін?
68. Соңғы жылдары киберқылмыскерлер шабуылдарды жүзеге асыру үшін қандай жаңа технологиялар мен әдістерді қолдана бастады?
69. Криптовалюта мен блокчейн технологияларының дамуы киберқылмысқа қалай әсер етті?
70. Ransomware-as-a-Service (RaaS) дегеніміз не және бұл модель бопсалаушы бағдарламалардың таралуына қалай ықпал етті?

**ҰСЫНЫЛАТЫН ӘДЕБИЕТТЕР ТІЗІМІ**

**Негізгі әдебиеттер:**

1. Овчинский В.С. "Основы борьбы с киберпреступностью и кибертерроризмом". — М.: Юр. НОРМА, 2024. — 528 с. [Электронный ресурс]. – Режим доступа: https://infra-m.ru/catalog/pravo\_yuridicheskie\_nauki/osnovy\_borby\_s\_kiberprestupnostyu\_i\_kiberterrorizmom\_1/

2.Масалков А.С. "Особенности киберпреступлений в России. Инструменты нападения и защита информации". — М.: ДМК-Пресс, 2018. — 226 с. [Электронный ресурс]. – Режим доступа: https://www.labirint.ru/books/626293/

3.Побегайло А.Э. "Борьба с киберпреступностью: учебное пособие". — М.: Университет прокуратуры Российской Федерации, 2018. — 184 с. [Электронный ресурс]. – Режим доступа: https://www.agprf.org/konkurs-na-luchshee-izdanie/informatsiya-o-konkurse-na-luchshee-izdanie-akadem343/luchshee-uchebnoe-izdanie/

4.Сборник статей "Преступность в сфере компьютерных технологий". — Центр исследований преступности, 2003. [Электронный ресурс]. – Режим доступа: https://www.crime-research.org/books.html

5.Учебно-методическое пособие "Обзор модулей по киберпреступности". — Управление ООН по наркотикам и преступности, 2020. [Электронный ресурс]. – Режим доступа: https://www.unodc.org/e4j/ru/cybercrime/teaching-guide/overview-of-cybercrime-modules.html

6.Сен Дж. и др. "Компьютерная и сетевая безопасность". — arXiv, 2020. [Электронный ресурс]. – Режим доступа:https://arxiv.org/abs/2007.16147

7.Книга "Киберпреступления – топ лучшей литературы по теме". — MyBook. [Электронный ресурс]. – Режим доступа: https://mybook.ru/tags/kiberprestupleniya/

**Қосымша әдебиеттер:**

1. Шнайер Б. "Взломать всё: Как сильные мира сего используют уязвимости систем в своих интересах". — М.: Альпина Паблишер, 2019. — 368 с. [Электронный ресурс]. – Режим доступа: https://www.litres.ru/brus-shnayyer/vzlomat-vse-kak-silnye-mira-sego-ispolzuyut-uyazvimosti-sistem-v-svoih-interesah/

2.Тегмарк М. "Жизнь 3.0. Быть человеком в эпоху искусственного интеллекта". — М.: Альпина Паблишер, 2018. — 460 с. [Электронный ресурс]. – Режим доступа: https://www.litres.ru/maks-tegmark/zhizn-3-0-byt-chelovekom-v-epohu-iskusstvennogo-intellekta/

3.Мола К. "Пурпурная сеть". — М.: Эксмо, 2020. — 320 с. [Электронный ресурс]. – Режим доступа: https://www.litres.ru/karmen-mola/purpurnaya-set/

4.Сен Дж. и др. "Компьютерная и сетевая безопасность". — arXiv, 2020. [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2007.16147

5.Нурс Дж. Р. С. "Киберпреступность и вы: как преступники атакуют и какие человеческие факторы они стремятся использовать". — arXiv, 2018. [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/1811.06624

**ЦИФРЛЫҚ КРИМИНАЛИСТИКА**

**Емтихан сұрақтары:**

1. Цифрлық криминаслитика пәні, объектісі, жүйесі және міндеттері
2. Құқық қорғау органдарының қылмыспен күресудегі қызметінде цифрлық технологиялардың рөлі мен маңызы.
3. Сотқа дейінгі тергеу органдарының қызметінде цифрлық технологияларды қолданудың құқықтық негіздері.
4. Цифрлық технологияларды қолдану арқылы жасалған қылмыстардың криминалистикалық моделі.
5. Цифрлық криминалистиканың міндеттері
6. Криминалистикалық зерттеу объектісі ретіндегі цифрлық ақпараттың түсінігі мен мәні.
7. Цифрлық ақпараттың болуының объективті нысандарының криминалистикалық классификациясы
8. Цифрлық іздер: түсінігі, сипаттамасы, қалыптасу механизмі, классификациясы және жазу ерекшеліктері.
9. Зиянды компьютерлік бағдарламалар мен компьютерлік шабуылдардың криминалистикалық зерттеу.
10. Цифрлық ақпарат түсінігі.
11. Цифрлық ақпараттың қасиеттері.
12. Цифрлық ақпараттың өзіндік ерекшеліктері.
13. Компьютерді сақтау құралдарына криминалистикалық зерттеу.
14. Электрондық кілттерді криминалистикалық зерттеу
15. Пластикалық карталар мен электрондық құжаттарды криминаслитикалық зерттеу.
16. Компьютерлік желілердің криминалистикалық зерттеу.
17. Цифрлық ақпарат қылмысты тергеудеді электрондық дәлелдемелердің негізі ретінде.
18. Тергеу әрекеттерінде криминалистикалық құрал ретінде цифрлық технологияларды қолдану.
19. Аутентификация түсінігі.
20. Қылмыстық іс бойынша сотта электрондық дәлелдемелерді ұсыну тактикасы.
21. Сот-компьютерлік-техникалық сраптаманы тағайындауды, шығаруды және нәтижелерін бағалауды криминалистикалық қамтамасыз ету.
22. Қылмыстарды ашу мен тергеуде цифрлық технологияларды қолданудың негізгі бағыттары.
23. Құқық қорғау органдарының ведомствоаралық өзара іс-қимылын қамтамасыз ету үшін ақпараттық жүйелер мен компьютерлік желілерді пайдалану.
24. Жасанды интеллект және жасанды интеллект технологиялары туралы түсінік.
25. Қылмыстық құқық бұзушылықтардың алдын алу мақсатында интернет желісін мониторингтеу бағыты.
26. Сотқа дейінгі тергеп-тексеруді жүзеге асыратын тұлғалардың цифрлық дәлелдемелерді анықтаудағы қызметі.
27. Криминалистикалық есепке алу түсінігі.
28. Құқық қорғау органдарының қылмыспен күресудегі қызметіндегі цифрлық технологиялардың рөлі мен маңызы.
29. Криминалистикалық тіркеу.
30. Криминалистикалық есепке алудың құқықтық-аспектілері.
31. Ішкі істер органдарының қызметіндегі ақпараттық технологиялар.
32. Құқық қорғау қызметінде ақпараттық технологияларды қолдану.
33. Компьютерлік қылмыстардың алдын алу мақсатында компьютерлік желі мониторингінің түрлері.
34. Интернет желісін жедел-іздестіру мониторингі қылмыспен күрес элементі ретінде.
35. Киберқылмыстарды тергеу әдістері.
36. Криминалистикалық тіркеудің ақпараттық, теориялық және құқықтық негіздері.
37. Криминалистикалық есепке алу жүйесі және оны ұйымдастыруды жетілдіру.
38. Азаматтарды тіркеудің ақпараттық-іздестіру жүйелерін қалыптастырудың және жұмыс істеуінің ғылыми негіздері.
39. Азаматтарды құқық қорғау органдарында тіркеудің қазіргі заманғы ақпараттық-іздестіру жүйелерінің генезисі.
40. Азаматтарды тіркеудің заманауи ақпараттық-іздестіру жүйелерін құру
41. Құқық қорғау органдарының азаматтарды тіркеуге арналған ақпараттық-іздестіру жүйесін құру және пайдаланудағы шет мемлекеттердің тәжірибесі.
42. Қазіргі заманғы биометриялық технологиялар және оларды азаматтарды тіркеудің ақпараттық-іздестіру жүйелерінде енгізу мүмкіндіктері.
43. Қылмыстарды тергеу тәжірибесінде қолданылатын азаматтарды тіркеудің ақпараттық-іздестіру жүйелерінің қазіргі жағдайы және олардың даму перспективалары.
44. Киберқылмыстардың алдын алудың құқықтық тетіктері.
45. Компьютерлік технологиялар саласындағы қылмыстардың алдын алу және ескерту әдістері.
46. Сот-компьютерлік-техникалық сараптаманың негізгі объектілері.
47. Сот-компьютерлік-техникалық сараптаманың түрлері.
48. Сот-компьютерлік-техникалық сараптама сұрақтарының мазмұны мен құрастырылуын анықтауға қойылатын талаптар.
49. Компьютерлік-техникалық сараптамаға ұсынылатын сұрақтардың түрлері.
50. Ақпаратты жинауға, өңдеуге және сақтауға арналған компьютерлерден, серверлерден және басқа құрылғылардан ақпаратты жасырын жою алгоритмі.
51. Пошта және басқа жөнелтілімдерді жасырын бақылау әдістері.
52. Жасырын тергеу әрекеттерінің нәтижелерін қылмыстық іс бойынша қолданудың әдістері мен тәртібі
53. Жасырын жолмен алынған ақпаратты қорғау шаралары.
54. Компьютерлік ақпарат саласындағы қылмыстың белгілері. Цифрлық технологияларды қолдану арқылы жасалатын қылмыстарға мысал келтіріңіз.
55. Құқық қорғау органдары қылмыстарды ашу және тергеу процесінде қолданатын цифрлық технологиялардың жіктелуі.
56. Цифрлық дәлелдемелерді алу үшін қолданылатын тергеу әрекеттері.
57. Цифрлық дәлелдемелік ақпаратты алу бойынша жүргізілетін жедел-іздестіру іс-шаралары.
58. Цифрлық ақпарат тасымалдаушыны жою және оны көшіру операцияларының айырмашылығы.
59. Электрондық дәлелдемелермен жұмыс істеудің тактикалық әдістерінің түрлері.
60. Сот ісін жүргізуде электрондық дәлелдемелерді ұсынудың жалпы тәртібі.
61. Жедел-іздестіру қызметінің нәтижелерін электронды түрде ұсынудың құқықтық негіздері.
62. Криминалистикалық құрал ретінде қолданылатын цифрлық технологиялар.
63. Криминалистикалық құрал ретінде цифрлық технологияларды қолданудың артықшылықтары.
64. Ақпаратты бекітудің цифрлық техникалық құралдары.
65. Ғарыштық, аэрофототүсірілімдер, 3D фотосуреттері
66. Цифрлық ақпаратты шығаруға арналған аппараттық және бағдарламалық жүйелердің түрлері.
67. Мамандандырылған криминалистикалық операциялық жүйелер
68. Іздеу мен өлшеудің цифрлық техникалық құралдары
69. Қылмыстық істер бойынша сотқа дейінгі өндіріске арналған арнайы бағдарламалық қамтамасыз ету.
70. Ұялы радиотелефонды тексерудің жұмыс кезеңінде орындалатын әрекеттер алгоритмі.

**ҰСЫНЫЛАТЫН ӘДЕБИЕТТЕР ТІЗІМІ**

**Негізгі әдебиеттер:**

1. Цифровая криминалистика: Учебник для вузов / Под ред. профессора К.Ж. Капсалямова.– Астана: Университет «Туран-Астана», 2024. – 293с.
2. Балашова А.А. Электронные носители информации: понятие и их использование в системе доказательств, учебное пособие. [Электронный ресурс].Иркутск: Восточно-Сибирский институт МВД России, 2022г., 80 стр.
3. Цифровая криминалистика: учебник для вузов. /В.Б.Вехов. [Электронный ресурс].М.: Издательство Юрайт, 2022 г., 417 стр.
4. Васильева И.Н. Расследование инцидентов информационной безопасности: учебное пособие //И.Н. Васильева, А.В. Климчаков. [Электронный ресурс].Издательство Санкт-Петербургского государственного университета, 2019г., 113 стр.
5. Келдыш Н.В. Информационная безопасность. Защита информации на объектах информатизации. Учебное пособие/ Н.В. Келдыш. Учебное пособие. [Электронные ресурсы].М.: Мир науки, 2017г., 260 стр.
6. Гришина Н. В. Основы информационной безопасности предприятия. Учебное пособие. М.: Инфра-М. 2021. 216 с.
7. Гродзенский Я. С. Информационная безопасность. Учебное пособие. М.: РГ-Пресс. 2024. 144 с.

**Дополнительная литература:**

1. Аубакирова А.А. Методика расследования компьютерных преступлений. Учебно-практическое пособие. Алматы, 2005г.
2. Бердникова О.П. Особенности расследования мошенничества в сфере компьютерной информации: учебное пособие. УрЮИ МВД России, 2022г.
3. Вострецова Е.В. Основы информационной безопасности: учебное пособие. Е.В. Восрецова, А.В. Климчаков. Издательство Уральского университета, 2019г.
4. Ерохин В.В. Безопасность информационных систем. учебное пособие. М.: Флинта, 2015г.
5. Ищейнов В.Я. Информационная безопасность и защита информации. Теория и практика. Учебное пособие. М.: Директ-Медиа, 2020г.