**Общие требования,**

**предъявляемые к лицу, поступающему в магистратуру по образовательной программе «7M12303 – Противодействие киберпреступности»**

**(научно-педагогическое направление)**

В области **Основы информационных систем и технологий** кандидату предлагается знать цели и задачи информационных систем, функции информационных систем, аппаратные средства и виртуализацию, безопасность сетей, средства защиты информации, облачные технологии и Big Data, перспективы развития технологий больших данных, применение ИС в логистике и транспорте, методы оценки эффективности информационных систем.

В области **Технологии киберпреступности** кандидат должен знать виды киберпреступлений, инновации и технологии для борьбы с киберпреступностью, развитие технологий и новые угрозы, атаки на определённые платформы, виды социальной инженерии, искусственный интеллект в киберпреступности, искусственный интеллект в анализе вредоносного программ, инструменты и ресурсы для хакеров, психологические типы киберпреступников, клевета и распространение ложной информации.

В области **Цифровая криминалистика** от кандидата требуется знать понятие, сущность и ключевые характеристики цифровой криминалистики как самостоятельной отрасли криминалистического знания, анализируются международные соглашения и стандарты в сфере обращения с цифровыми доказательствами (Будапештская конвенция и др.), допустимые формы доказательств: аудио- и видеозаписи, материалы фото- и киносъемки, другие материалы на электронных, цифровых и иных материальных носителях, процесс извлечения, анализа и интерпретации доказательств с компьютерной техники для использования в уголовном процессе, значение создания судебно-допустимой документации и верификации полученных результатов.

**ОСНОВЫ ИНФОРМАЦИОННЫХ СИСТЕМ и технологий**

**ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ:**

1. Что такое информационная система и какие ее основные функции в организации?
2. Каковы ключевые компоненты информационных технологий, и как они взаимодействуют между собой?
3. Какую роль играют базы данных в информационных системах, и какие основные типы баз данных существуют?
4. В чем разница между операционными, управленческими и стратегическими информационными системами?
5. Как информационные технологии способствуют повышению эффективности бизнес-процессов в организации?
6. Каковы основные критерии классификации информационных систем и какие виды систем они охватывают?
7. В чем заключается различие между транзакционными информационными системами (TIS) и управленческими информационными системами (УИС)?
8. Какие компоненты составляют архитектуру информационной системы, и какова их роль в функционировании системы?
9. Каковы функции операционных информационных систем (ОИС) и какие задачи они решают в организации?
10. Что такое стратегические информационные системы (СИС), и как они способствуют достижению долгосрочных целей организации?
11. Что такое аппаратные средства информационных систем и какие основные категории оборудования они включают?
12. Какова роль центрального процессора (ЦП) в аппаратной архитектуре информационной системы?
13. Какие функции выполняет оперативная память (ОП) и как она влияет на производительность информационной системы?
14. Каковы основные отличия между жесткими дисками и твердотельными накопителями (SSD) в контексте использования в информационных системах?
15. Как аппаратные средства взаимодействуют с программным обеспечением, и какое значение имеет это взаимодействие для функционирования информационных систем?
16. Что такое программное обеспечение (ПО) и какие основные категории ПО существуют в информационных системах?
17. Каковы функции операционных систем и какую роль они играют в управлении аппаратными средствами и приложениями?
18. Что такое системное ПО и как оно отличается от прикладного ПО?
19. Как программное обеспечение влияет на безопасность информационных систем и какие меры можно предпринять для ее обеспечения?
20. Каковы основные этапы жизненного цикла программного обеспечения (ЖЦПО), и какое значение имеет каждый из этих этапов для разработки и поддержки ПО?
21. Что такое база данных и какие основные характеристики отличают её от других форматов хранения данных?
22. Объясните разницу между реляционными и нереляционными базами данных.
23. Какова роль системы управления базами данных (СУБД) и какие основные функции она выполняет?
24. Что такое модель данных и какие модели (например, реляционная, объектная) наиболее распространены в СУБД?
25. Как работают транзакции в СУБД и какие свойства (ACID) они должны обеспечивать для обеспечения целостности данных?
26. Каковы основные этапы проектирования информационной системы и какие задачи решаются на каждом из них?
27. Что такое функциональные и нефункциональные требования к информационной системе, и почему их важно учитывать на этапе проектирования?
28. Объясните разницу между моделированием данных и моделированием процессов.
29. Какие основные методы проектирования информационных систем существуют, и в чем их ключевые отличия?
30. Что такое документация в проектировании информационных систем и какие виды документов должны быть созданы на различных этапах проектирования?
31. Как обеспечивается безопасность информационной системы в процессе ее проектирования?
32. Что такое компьютерные сети и какие основные типы сетей (LAN, WAN, MAN) существуют?
33. Каковы основные компоненты компьютерных сетей и какую роль они играют в функционировании информационных систем?
34. Что такое сетевые протоколы, и как они обеспечивают взаимодействие между устройствами в сети?
35. Каковы основные принципы работы беспроводных технологий и их преимущества по сравнению с проводными сетями?
36. Какие меры безопасности необходимо применять для защиты сетевых технологий в информационных системах от киберугроз?
37. Что такое облачные технологии и какие основные модели облачных услуг (IaaS, PaaS, SaaS) существуют?
38. Каковы основные преимущества использования облачных технологий для бизнеса и организаций?
39. Что такое виртуализация и как она соотносится с облачными технологиями?
40. Каковы основные компоненты облачной архитектуры, и какую роль они играют в развертывании облачных решений?
41. Какие риски и проблемы могут возникнуть при использовании облачных технологий, и как их можно минимизировать?
42. Что такое информационная безопасность и какие основные цели она преследует в контексте защиты информационных систем?
43. Какие основные виды угроз существуют для информационных систем, и какие примеры можно привести для каждой категории?
44. Каковы основные средства защиты информации, используемые для обеспечения безопасности информационных систем?
45. Что такое политика информационной безопасности и какие ключевые элементы она должна включать?
46. Каковы основные аспекты безопасности сетей и коммуникаций в контексте защиты информационных систем?
47. Что такое Big Data и какие основные характеристики определяют большие данные?
48. Каковы основные компоненты архитектуры систем Big Data?
49. Какие инструменты и технологии используются для обработки и анализа больших данных?
50. Каковы преимущества использования технологий больших данных в бизнесе и других отраслях?
51. Какие методы и алгоритмы анализа данных применяются в Big Data?
52. Что такое искусственный интеллект (ИИ) и каковы его основные категории и технологии?
53. Как искусственный интеллект применяется в информационных системах для автоматизации процессов?
54. Какие методы машинного обучения используются для обработки и анализа данных в информационных системах?
55. Как искусственный интеллект способствует улучшению безопасности информационных систем?
56. В чем заключаются основные преимущества и недостатки внедрения ИИ в информационные системы?
57. Какие основные этапы внедрения информационных систем в бизнес-процессы можно выделить?
58. Каковы основные проблемы и риски, связанные с внедрением информационных систем в организации?
59. Какие преимущества могут получить компании при интеграции информационных систем в свои бизнес-процессы?
60. Как можно оценить эффективность внедрения информационных систем в рамках бизнеса?
61. Как обеспечить совместимость новой информационной системы с существующими IT-решениями в компании?
62. Какие методы оценки эффективности информационных систем вы знаете?
63. Как финансовая оценка может повлиять на принятие решений по внедрению или модернизации информационной системы?
64. Каковы основные нефинансовые аспекты, которые следует учитывать при оценке эффективности информационных систем?
65. Какие проблемы и риски могут возникнуть при оценке эффективности информационных систем?
66. Каковы этапы процесса оценки эффективности информационной системы в организации?
67. Каковы основные тенденции в развитии информационных технологий, которые ожидаются в ближайшие 5–10 лет?
68. Как могут развиваться технологии больших данных и аналитики в контексте повышения эффективности бизнес-процессов?
69. Как информационные системы улучшают качество обслуживания клиентов в сфере здравоохранения?
70. Какие информационные технологии используются в финансовом секторе для повышения безопасности и эффективности операций?

**СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ**

**Основная литература:**

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., Урмашев Б. Информационно-коммуникационные технологии. 1-е изд. Учебник. – Алматы, 2020. – 559 стр.
8. Shvnvbekov D., Uskenbayeva R., Serbin V., Duzbayev N., Moldagulova A., Duysebekova K., Satybaldiyeva R., Khasenova G., Urmashev B. 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.

**Дополнительная литература:**

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).
	* 1. 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.
		2. Tanenbaum E., Bos H. T18 Modern operating systems. 4 th ed. – St. Petersburg: Peter, 2015. – 1120 p.: ill. – (Series «Classic Computer Science»).
		3. 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.

**ТЕХНОЛОГИИ КИБЕРПРЕСТУПНОСТИ**

**ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ:**

1. Что такое киберпреступность и какие основные категории киберпреступлений вы знаете?
2. Какие технологии и методы чаще всего используются киберпреступниками для взлома компьютерных систем и кражи данных?
3. Что такое социальная инженерия в контексте киберпреступности и как она используется для проведения атак?
4. Объясните, как работает вредоносное ПО и какие существуют его основные виды.
5. Какие меры могут быть предприняты для защиты от киберпреступлений?
6. Определите понятие киберпреступления и объясните, на какие основные категории они делятся.
7. Что такое кибермошенничество?
8. Какие преступления относятся к категории преступлений против интеллектуальной собственности в киберпространстве?
9. Как классифицируются киберпреступления против личности?
10. Что такое кибертерроризм и как он отличается от кибервандализма?
11. Что такое социальная инженерия в контексте киберпреступности?
12. Как психологические аспекты влияют на эффективность социальной инженерии?
13. Какую роль играет манипуляция эмоциями в атаках социальной инженерии?
14. Что такое претекстинг и как он используется в киберпреступности?
15. Какие психологические уязвимости чаще всего используются киберпреступниками при проведении атак?
16. Как искусственный интеллект (AI) может быть использован для автоматизации кибератак?
17. Что такое deepfake и как эта технология может быть использована в киберпреступности?
18. Какие меры можно предпринять для защиты от использования AI в киберпреступности?
19. Как AI может использоваться для повышения эффективности защиты от кибератак?
20. Как использование AI в киберпреступности может усложнить расследование и обнаружение преступников?
21. Что такое DDoS-атака и как она может повлиять на работу веб-сайта или сети?
22. Опишите, что такое SQL-инъекция и как она может быть использована злоумышленниками для проведения сетевых атак.
23. Что такое фишинг и какие виды фишинговых атак существуют?
24. Объясните, что такое MITM-атака (Man-in-the-Middle) и какие угрозы она представляет для безопасности сети?
25. Что такое сниффинг и как он может быть использован в сетевых атаках?
26. Что такое "белые шляпы" и "черные шляпы" в хакерской культуре?
27. Опишите, что такое руткиты и как они используются в хакерских атаках. Какие методы можно использовать для обнаружения и удаления руткитов?
28. Что такое социальная инженерия и как она может быть использована в процессе взлома системы?
29. Объясните, что такое атака типа "brute force" и как она используется для взлома паролей. Какие меры могут быть приняты для защиты от таких атак?
30. Что такое фишинг и как он используется хакерами для взлома учетных записей?
31. Какие основные психологические факторы могут мотивировать людей становиться киберпреступниками?
32. Какую роль играют идеологические и политические убеждения в мотивации киберпреступников?
33. Какие личностные черты могут быть характерны для киберпреступников?
34. Как социальная изоляция и отсутствие социальной поддержки могут способствовать вовлечению в киберпреступность?
35. Какую роль играют финансовые мотивы в мотивации киберпреступников?
36. Что такое фишинг и как он может быть использован для хищения криптовалют?
37. Объясните, что такое атака на смарт-контракт и как она может привести к хищению криптовалют.
38. Что такое "криптоджекинг" и как злоумышленники используют этот метод для незаконного получения криптовалют?
39. Как злоумышленники могут использовать атаки "человек посередине" (MITM) для хищения криптовалют?
40. Что такое "SIM-сваппинг" и как он используется для кражи криптовалют?
41. Что понимается под понятием "интеллектуальная собственность"?
42. Что такое авторские права и как они могут быть нарушены в цифровой среде?
43. Что такое патент и каковы последствия нарушения патентных прав?
44. Что такое товарный знак и как может произойти его нарушение?
45. Какова роль коммерческой тайны в интеллектуальной собственности и что считается ее нарушением?
46. Что такое кибербуллинг и какие формы он может принимать в цифровом пространстве?
47. Что такое киберсталкинг и как он отличается от кибербуллинга?
48. Что понимается под понятием "кража личности" в киберпространстве?
49. Объясните, что такое "ревендж порн" и какие правовые и этические вопросы оно поднимает.
50. Что такое вишинг и как он используется для проведения киберпреступлений против личности?
51. Что такое организованная киберпреступность и чем она отличается от одиночных киберпреступлений?
52. Какие методы и технологии чаще всего используются организованными киберпреступными группами для осуществления своих операций?
53. Как организованные киберпреступные группы используют даркнет и теневые рынки для своей деятельности?
54. Какие виды преступлений наиболее часто совершаются организованными киберпреступными группами?
55. Какие меры могут быть предприняты для борьбы с организованной киберпреступностью?
56. Что понимается под термином "критическая инфраструктура" и какие объекты к ней относятся?
57. Какие виды кибератак могут быть направлены на критическую инфраструктуру?
58. Что такое SCADA-системы и почему они являются мишенью для кибератак?
59. Каковы потенциальные последствия успешной кибератаки на системы водоснабжения?
60. Какие меры безопасности могут быть предприняты для защиты критической инфраструктуры от кибератак?
61. Что такое кибервойна и чем она отличается от кибертерроризма?
62. Что такое "кибероружие" и как оно используется в кибервойнах?
63. Какие виды кибератак могут быть использованы в рамках кибертерроризма?
64. Какую роль играют фальшивые новости и дезинформация в кибервойнах и кибертерроризме?
65. Что такое "ответственное раскрытие уязвимостей" и почему оно является важным этическим принципом в кибербезопасности?
66. Объясните этические дилеммы, связанные с использованием искусственного интеллекта в киберпреступности и кибербезопасности.
67. Какие этические вопросы могут возникнуть при использовании инструментов для мониторинга и анализа сетевого трафика?
68. Какие новые технологии и методы используются киберпреступниками для проведения атак в последние годы?
69. Как развитие криптовалют и блокчейн-технологий влияет на киберпреступность?
70. Что такое Ransomware-as-a-Service (RaaS) и как эта модель повлияла на распространение программ-вымогателей?

**СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ**

**Основная литература:**

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/

**Дополнительная литература:**

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

**ЦИФРОВАЯ КРИМИНАЛИСТИКА**

**Экзаменационные вопросы:**

1. Предмет, объект, система и задачи цифровой криминалистики.
2. Роль и значение цифровых технологий в деятельности правоохранительных органов по борьбе с преступностью.
3. Правовые основы применения цифровых технологий в деятельности органов досудебного расследования.
4. Криминалистическая модель преступлений, совершаемых с использованием цифровых технологий.
5. Задачи цифровой криминалистики.
6. Понятие и сущность цифровой информации как объекта криминалистического исследования.
7. Криминалистическая классификация объективных форм существования цифровой информации.
8. Цифровые следы: понятие, признаки, механизм образования, классификация и особенности фиксации.
9. Криминалистическое исследование вредоносных компьютерных программ и компьютерных атак.
10. Понятие цифровой информации.
11. Свойства цифровой информации.
12. Специфические признаки цифровой информации.
13. Криминалистическое исследование машинных носителей информации.
14. Криминалистическое исследование электронных ключей
15. Криминалистическое исследование пластиковых карт и электронных документов.
16. Криминалистическое исследование компьютерных сетей.
17. Цифровая информация как основа электронных доказательств в расследовании преступлений.
18. Использование цифровых технологий как средств криминалистической техники в проведении следственных действий
19. Понятие аутентификации
20. Тактика представления электронных доказательств в суде по уголовным делам.
21. Криминалистическое обеспечение назначения, производства и оценки результатов судебно компьютерно-технической экспертизы
22. Основные направления использования цифровых технологий в раскрытии и расследовании преступлений.
23. Использование информационных систем и компьютерных сетей для обеспечения межведомственного взаимодействия правоохранительных органов
24. Понятие искусственный интеллект и технологии искусственного интеллекта.
25. Направление мониторинга сети интернет в целях предупреждения уголовных правонарушений.
26. Деятельность лиц осуществляющих досудебное расследование при определении цифровых доказательств.
27. Понятие криминалистической регистрации
28. Роль и значение цифровых технологий в деятельности правоохранительных органов по борьбе с преступностью
29. Криминалистические учеты
30. Правовые основы криминалистической регистрации
31. Информационные технологии в деятельности органов внутренних дел.
32. Использование информационных технологий в правоохранительной деятельности.
33. Виды мониторинга компьютерных сетей в целях пресечения компьютерных преступлений.
34. Оперативно-розыскной мониторинг сети интернет как элемент противодействия преступлениям.
35. Методы расследования киберпреступлений
36. Информационные, теоретические и правовые основы криминалистической регистрации?
37. Система криминалистической регистрации и совершенствование её организации.
38. Научные основы формирования и обеспечения функционирования информационно-поисковых систем регистрации граждан.
39. Генезис современных информационно-поисковых систем регистрации граждан в правоохранительных органах.
40. Создание современных информационно-поисковых систем регистрации граждан
41. Опыт зарубежных стран в создании и использовании правоохранительными органами информационно-поисковых систем регистрации граждан.
42. Современные биометрические технологии и возможности их реализации в информационно-поисковых системах регистрации граждан.
43. Современное состояние информационно-поисковых систем регистрации граждан используемых в практике расследования преступлений и перспективы их развития.
44. Правовые механизмы предупреждения киберпреступлений
45. Методы профилактики и предупреждения преступлений в сфере компьютерных технологий.
46. Основные объекты судебной компьютерно-технической экспертизы.
47. Виды судебной компьютерно-технической экспертизы.
48. Требования, предъявляемые к определению содержания и формулировке вопросов для судебной компьютерно-технической экспертизы.
49. Виды вопросов, выносимых на судебную компьютерно-техническую экспертизу.
50. Алгоритм негласного снятия информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации
51. Способы негласного контроля почтовых и иных отправлений
52. Способы и порядок использования результатов негласных следственных действий в уголовном деле
53. Мероприятия по защите информации полученной негласным путем
54. Признаки преступления в сфере компьютерной информации. Приведите примеры преступлений, способ совершения которых предполагает использование цифровых технологий.
55. Классификация цифровых технологий, используемых правоохранительными органами в процессе раскрытия и расследования преступлений
56. . Следственные действия, используемые для получения цифровой доказательственной информации
57. Оперативно-розыскные мероприятия проводимые для получения цифровой доказательственной информации
58. Различие операций по изъятию носителя цифровой информации и ее копированию
59. Разновидности тактических приемов работы с электронными доказательствами.
60. Общий порядок представления электронных доказательств в судопроизводстве
61. Правовая основа представления результатов оперативно-розыскной деятельности в электронном виде
62. Цифровые технологии, используемые в качестве средств криминалистической техники.
63. Преимущества применения цифровых технологий в качестве средств криминалистической техники.
64. Цифровые технические средства фиксации информации.
65. Космическая, аэросъемка, ЗD-съемка
66. Виды аппаратно-программных комплексов, предназначенных для извлечения цифровой информации.
67. Специализированные криминалистические операционные системы
68. Цифровые технические средства поиска и измерения
69. Специальное программное обеспечение досудебного производства по уголовным делам
70. Алгоритм действий, осуществляемых во время рабочего этапа осмотра сотового радиотелефона

**Список рекомендуемой литературы**

**Основная:**

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.