|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Аннотация** | | |  |  |  |
|  |  |  |  |  |  |
| **Рабочей программы дисциплины** | | |  |  |  |
|  |  |  |  |  |  |
| Кафедра шахматного искусства и компьютерной математики | | | |  |  |
| Дисциплина | | Информационная безопасность телекоммуникационных систем | |  |  |
| Направление подготовки | | 02.03.03 Математическое обеспечение и администрирование информационных систем | |  |  |
| Профиль | | Разработка и администрирование информационных систем | |  |  |
| Объем дисциплины | | 8 з.е | |  |  |
| Формы промежуточной аттестации | | Зачет | |  |  |
|  |  | Экзамен, Курсовая работа | |  |  |
| **Краткое** **содержание** **дисциплины** | | | | | |
|  |  | | | |  |
|  |
| Тема | Наименование темы | | | |  |
| Тема 1. | Основные понятия и анализ угроз информационной безопасности. Разработка политики информационной безопасности на уровне БД (УК-8, ПК-7) | | | |  |
| Тема 2. | Разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным. (ПК-1, ПК-2) | | | |  |
| Тема 3. | Классическая криптография (ПК-1, ПК-2) | | | |  |
| Тема 4. | Симметричные алгоритмы шифрования (ПК-1, ПК-2) | | | |  |
| Тема 5. | Хэш-функции (ПК-1, ПК-2) | | | |  |
| Тема 6. | Электронно-цифровая подпись (ПК-1, ПК-2) | | | |  |
| Тема 7. | Асимметричные алгоритмы шифрования (ПК-1, ПК-2) | | | |  |
| Тема 8. | Стеганография и стеганоанализ (ПК-1, ПК-2) | | | |  |
| Тема 9. | Уязвимости программного обеспечения (ПК-1, ПК-2) | | | |  |
| Тема 10. | Компьютерные вирусы и методы их обнаружения (ПК-1, ПК-2) | | | |  |
| Тема 11. | Разделение прав в операционных системах (ПК-1, ПК-2) | | | |  |
| Тема 12. | Методы авторизации и аутентификации пользователей (ПК-1, ПК-2) | | | |  |
| Тема 13. | Безопасность сетей ЭВМ (ПК-1, ПК-2) | | | |  |
| Тема 14. | Ассиметричные алгоритмы шифрования (продолжение) (ПК-1, ПК-2) | | | |  |
| Тема 15. | Стеганография и стеганоанализ (продолжение) (ПК-1, ПК-2) | | | |  |
| Тема 16. | Уязвимости программного обеспечения (продолжение) (ПК-1, ПК-2) | | | |  |
| Тема 17. | Компьютерные вирусы и методы их обнаружения (продолжение) (ПК-1, ПК-2) | | | |  |
| Тема 18. | Разделение прав в операционных системах (продолжение) (ПК-1, ПК-2) | | | |  |
| Тема 19. | Методы авторизации и аутентификации пользователей (продолжение) (ПК-1, ПК-2) | | | |  |
| Тема 20. | Безопасность сетей ЭВМ (продолжение) (ПК-1, ПК-2) | | | |  |
|  |  |  |  |  |  |
| **Список** **литературы** | | | | | |
|  |  |  |  |  |  |
| **Основная литература:** | | | | | |
| 1. Крамаров С.О., Тищенко Е.Н. Криптографическая защита информации. [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2018. - 324 с. – Режим доступа: https://znanium.com/catalog/product/901659 | | | | | |
|

|  |
| --- |
| 2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2019. - 592 с. – Режим доступа: https://znanium.com/catalog/product/996789 |
| 3. Крамаров С.О., Тищенко Е.Н. Криптографическая защита информации. [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2019. - 324 с. – Режим доступа: https://znanium.com/catalog/product/1018903 |
| 4. Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 118 с. – Режим доступа: https://znanium.com/catalog/product/1178153 |
| 5. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно- издательский центр ИНФРА-М", 2022. - 223 с. – Режим доступа: https://znanium.com/catalog/product/1178148 |
| 6. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2022. - 592 с. – Режим доступа: https://znanium.com/catalog/product/1843022 |
| 7. Ищейнов В. Я., Мецатунян М. В. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 256 с. – Режим доступа: https://znanium.com/catalog/product/1861659 |
| 8. Моргунов А.В. Информационная безопасность [Электронный ресурс]:Учебно- методическая литература. - Новосибирск: Новосибирский государственный технический университет (НГТУ), 2019. - 83 с. – Режим доступа: https://znanium.com/catalog/product/1866895 |
| 9. Гришина Н. В. Основы моделирования процессов и систем защиты информации [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 107 с. – Режим доступа: https://znanium.com/catalog/product/1891122 |
|  |
| **Дополнительная литература:** |
| 1. Бабаш А.В., Баранова Е.К. Моделирование системы защиты информации: Практикум [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО�, 2021. - 320 с. – Режим доступа: https://znanium.com/catalog/product/1232287 |
|
| 2. Баранова Е.К., Бабаш А.В., Ларин Д.А. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО�, 2022. - 236 с. – Режим доступа: https://znanium.com/catalog/product/1843171 |
| 3. Гришина Н. В. Основы управления информационной безопасностью [Электронный ресурс]:Учебно-методическая литература. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 99 с. – Режим доступа: https://znanium.com/catalog/product/1859951 |
|  |
| **Перечень** **информационных** **технологий,** **включая** **перечень** **лицензионного** **программного** **обеспечения** **и** **информационных** **справочных** **систем,** **онлайн** **курсов,** **используемых** **при** **осуществлении** **образовательного** **процесса** **по** **дисциплине** |
|  |
| **Перечень лицензионного программного обеспечения:** |
|  |
| Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии 30.09.2023. |
| Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии 30.09.2023. |
| Adobe Reader. Лицензия freeeware. Срок действия лицензии - без ограничения срока. |
| Secret Net 7. Клиент (автономный режим работы). Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017. |
| hMailServer. Лицензия AGPL. Срок действия лицензии - без ограничения срока. |
| Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока. |

|  |
| --- |
| **Перечень информационных справочных систем, ресурсов информационно-** **телекоммуникационной сети «Интернет»:** |
|  |
|  |
| Аннотацию подготовил: Часовских В.П. |

.

**Перечень курсовых работ**

|  |  |
| --- | --- |
| ***Дисциплина*** | **Информационная безопасность телекоммуникационных систем** |
| ***Направление подготовки*** | 02.03.03 Математическое обеспечение и администрирование информационных систем |
| ***Направленность (профиль)*** | Разработка и администрирование информационных систем |
| ***Кафедра*** | *Шахматного искусства и компьютерной математики* |
| ***Темы курсовых работ*** | |
| 1. Вопросы информационной безопасности в системах с радиочастотными идентификаторами.  2. Основы информационной безопасности.  3. Основы кибербезопасности.  4. Обеспечение информационной безопасности телефонных переговоров на каналах сотовой связи стандарта GSM.  5. Разработка средств обнаружения несанкционированного доступа к волоконно-оптическим линиям связи.  6. Разработка средства идентификации лиц по антропологическим признакам в видеоряде.  7. Разработка средства сокрытия данных от несанкционированного доступа в видеофильмах.  8. Схемы разделения секретов и их применение для информационной безопасности.  9. Разработка системы информационной безопасности засекречивания нетекстовой информации на каналах Интернет.  10. Решение задач информационной безопасности при обработке и хранении биометрической информации.  11. Исследование вопроса обеспечения информационной безопасности посредством систем детектирования по голосу.  12. Обеспечение информационной безопасности при дистанционном обучении.  13. Применение теории расширяющих графов в задачах информационной безопасности.  14. Разработка и анализ способов обеспечения информационной безопасности удаленного электронного голосования.  15. Исследование современных технологий «электронных денег» (Bitcoin, Darkcoin, etc.) с точки зрения информационной безопасности.  16. Разработка новых алгоритмов электронной подписи и их сравнительный анализ с известными стандартами.  17. Изучение каналов связи с дезинформацией.  18. Управление информационной безопасностью.  19. Управление информационной безопасностью в мобильных устройствах на платформе Google Android.  20. Информационная безопасность облачных хранилищ данных для мобильных устройств на платформе iOS.  21. Противодействие несанкционированному доступу к информации, передаваемой по волоконно-оптическим каналам связи.  22. Разработка системы обеспечения информационной безопасности учета c многофакторной биометрической аутентификацией (отпечаток+голос).  23. Разработка подсистемы безопасности и восстановления работоспособности автономных систем.  24. Обеспечение информационной безопасности в микропроцессорных системах беспроводной связи.  25. Разработка подсистем безопасности и мониторинга банкомата.  26. Разработка подсистемы видеонаблюдения с защищенным контентом.  27. Анализ и управление информационными рисками.  28. Анализ уязвимостей программного обеспечения.  29. Реализация и оценка эффективности новых подходов в обеспечении информационной безопасности.  30. Разработка формализованной модели угроз информационной безопасности на предприятии.  31. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей.  32. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей.  33. Анализ методов и средств анализа защищенности беспроводных сетей.  34. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения.  35. Виброакустические средства современных систем обеспечения информационной безопасности.  36. Средства защиты от ПЭМИН, современное состояние, проблемы и решения.  37. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.  38. Средства обеспечения информационной безопасности банков данных.  39. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).  40. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.  41. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.  42. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.  43. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации.  44. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.  45. Инструментальные средства анализа рисков информационной безопасности.  46. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.  47. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности). | |