МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

ИНСТИТУТ ЦИФРОВЫХ ТЕХНОЛОГИЙ

**Кафедра «Общая информатика»**

**ВОПРОСЫ К ЗАЧЕТУ И ЗАДАНИЯ ПО ДИСЦИПЛИНЕ**

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ»

**ДЛЯ ОБУЧАЮЩИХСЯ 3 КУРСА ЗАОЧНОЙ ФОРМЫ ОБУЧЕНИЯ ПО СПЕЦИАЛЬНОСТИ 40.05.02 ПРАВООХРАНИТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ**

**СПЕЦИАЛИЗАЦИЯ «ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ»**

***Рекомендации по подготовке реферата***

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ**

**Общие требования к оформлению реферата**

Реферат выполняется обучающимися попоследней цифре зачетной книжки, в машинописном виде параметры шрифта: гарнитура шрифта - Times New Roman, начертание - обычный, кегль шрифта - 14 пунктов, цвет текста – авто (черный); контрольные работы оформляют на листах формата А4 (210х297), текст печатается на одной стороне листа через полтора интервала; поля страницы: верхнее и нижнее поля – 20 мм; правое и левое поля – 15 мм. Текст по ширине. Нумерация страниц -внизу справа.

Структура реферата:

Реферат должен содержать:

1. Титульный лист;
2. Содержание;
3. Введение;
4. Основную часть;
5. Заключение;
6. Список использованной литературы.

Оптимальный объем 12-16 страниц печатного текста(на бумажных носителях, в электронном виде), разметка страниц- нижний правый угол.

Требования к содержанию:

1. Во введении формулируется актуальность темы, историографический обзор, цель и задачи исследования, практическая значимость (примерный объем введения 2-3 страницы).

2. Основная часть содержит анализ научной литературы по изучаемой теме. Материал основной части должен быть разбит на разделы, каждый раздел – озаглавлен, заголовок – отражать содержание раздела основной части (объем основной части - 12 - 16 страниц).

3. Заключение должно характеризовать в сжатом виде результаты исследования, четкие выводы.

При подготовке реферата необходимо использовать достаточное для раскрытия темы и анализа литературы количество источников, непосредственно относящихся к изучаемой теме.

4. Список литературы оформляется по следующим критериям:

-в алфавитном порядке

-тематически-хронологический

-по видам источников

В приложение включается вспомогательный материал, на базе которого проводилось исследование: репродукции, иллюстрации, копии документов, фотографии, рисунки, схемы, таблицы, статистические данные.

ИЗ КОМПЛЕКТА ТЕСТОВЫХ ВОПРОСОВ ВЫБРАТЬ 5 И РЕШИТЬ.

ОБЯЗАТЕЛЬНО!

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Институт цифровых технологий

**Кафедра «Общая информатика»**

**РЕФЕРАТ**

по дисциплине:

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ»

ТЕМА: «……………………………………………………….»

Выполнил(а):

Обучающийся \_\_курса

ФИО

Проверила:

старший преподаватель Борлакова М.А.

г.Черкесск, 2025

**Вопросы к зачету**

по дисциплине

«Основы информационной безопасности в правоохранительных органах»

* 1. Понятие информации, информационной сферы, безопасности информации и информационной безопасности субъекта.
  2. Основные составляющие национальных интересов в информационной сфере.
  3. Виды и источники угроз информационной безопасности страны (на примере России).
  4. Принципы государственной политики обеспечения информационной безопасности страны (на примере Российской Федерации).
  5. Информационная сфера и информационная безопасность правоохранительных органов.
  6. Обеспечение информационной безопасности в процессе деятельности оперативных подразделений органов внутренних дел.
  7. Важнейшие составляющие интересов в информационной сфере и основные угрозы информационной безопасности правоохранительных органов.
  8. Защита информации. Комплексный подход к защите информации.
  9. Классификация методов защиты информации.
  10. Понятие и виды каналов утечки информации ограниченного доступа. «Типовые» каналы утечки информации объектов информатизации ПО.
  11. «Типовые» каналы утечки информации объектов информатизации ПО. Условия и факторы, способствующие утечке информации ограниченного доступа.
  12. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.
  13. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки.
  14. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты.
  15. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки.
  16. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.
  17. Уязвимость компьютерных систем. Понятие несанкционированного доступа. Классы и виды несанкционированного доступа.
  18. Уязвимость компьютерных систем. Модель злоумышленника.
  19. Понятие «идентификации пользователя». Задача идентификации пользователя. Использование идентификации в защите информационных процессов.
  20. Методы и средства защиты данных от несанкционированного доступа.
  21. Основные методы НСД при физическом контакте с компьютером.
  22. Классический алгоритм поведения злоумышленника при удаленном несанкционированном доступе в компьютерную систему.
  23. Основные причины утечки информации с охраняемых объектов.
  24. Разграничение доступа к информации. Идентификация и аутентификация.
  25. Криптографические методы защиты данных. Электронно-цифровая подпись.
  26. Основные угрозы безопасности информации в компьютерных системах.
  27. Вредоносные программы и методы борьбы с ними.
  28. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.
  29. Методы и средства воздействия на безопасность сетей.
  30. Особенности построения защиты информации в телекоммуникационных сетях. Современные технические и программные средства сетевой защиты компьютерной информации.
  31. Применение электронно-цифровой подписи для защиты документов.
  32. Идентификация электронных и бумажных документов. Реквизиты и свойства документов.
  33. Свойства файла и свойства электронного документа.
  34. Свойства электронного документа – фиксация в электронном документе и в бумажной форме.
  35. Свойства электронного документа – поиск документов по заданному фрагменту текста.
  36. Свойства электронного документа – поиск документов по заданным свойствам.
  37. Понятие и назначение шаблона процессуальных документов.
  38. Создание нового шаблона на основе одного из стандартных шаблонов MS Word.
  39. Создание нового шаблона на основе готового электронного документа.
  40. Извлечение и использование готовых шаблонов процессуальных документов изстандартных шаблонов MS Word.
  41. Сохранение шаблонов и создание на их основе новых документов.
  42. Автоматизация заполнения электронных документов. Создание защищенного шаблона
  43. Виды и параметры полей форм. Текстовое поле, флажок, список.
  44. Понятие и места установки паролей.
  45. Современные требования к надежным паролям.
  46. Виды атак на пароли и классификация паролей.
  47. Правила составления и запоминания надежных (сложных) паролей.
  48. Парольная защита документов MS Word. Установка и различные виды парольной защиты.
  49. Возможности преодоления и обхода парольной защиты документов MS Word.
  50. Приемы скрытия текста и графических объектов в документе.
  51. Приемы обнаружения скрытых текстовых и графических объектов в документе.
  52. Защита различных объектов в MS Excel: книги, листа, ячейки, выделенного диапазона.
  53. Создание защищенной таблицы с редактируемыми областями.
  54. Скрытие объектов в Excel: окна Excel, окна книги, листов, ячеек, выделенных диапазонов, формул.
  55. Приемы скрытия текста и графических объектов в документе MS Excel.
  56. Приемы обнаружения скрытых текстовых и графических объектов в документе MS Excel.
  57. Шифрование любых файлов с документами.
  58. Добавление текстовой информации в конец графического файла.
  59. Запаковка текста внутри графического файла с искажением последнего.
  60. Сокрытие текста внутри графического файла без искажения последнего.
  61. Понятие и квалификация преступлений в сфере компьютерной информаций

Темы рефератов

**по дисциплине «Основы информационной безопасности в правоохранительных органах»**

1. Классификация вредоносных программ и защита от их воздействия.
2. Темы и шаблоны в Microsoft Office Word как средства профессионального оформления документов.
3. Применение полей Microsoft Office Word в электронном делопроизводстве.
4. Поля Microsoft Office Word как средство быстрого извлечения информации.
5. Возможности Microsof tOffice Word по защите и разграничению доступа при работе в корпоративной сети.
6. Растущие угрозы компьютерной безопасности как следствие коммерциализации Интернета..
7. Средства электронной подготовки и обработки документов бланкового типа.
8. Обеспечение безопасности и защита документов Microsoft Office Word.
9. Форматы файлов и преобразование документов в Microsoft Office Word.
10. Система защиты информации в России
11. Правовые способы защиты информации в России
12. Угроза информационной безопасности от вредоносных программ
13. Защита информации от вредоносных программ
14. Угрозы неприкосновенности личного пространства человека с развитие информационных технологий и Интернета.
15. Информационное неравенство, цифровое разделение общества, информационная бедность. Проблемы, последствия, пути решения.
16. Политика безопасности и информационной безопасности России
17. Информационные риски (опасность возникновения убытков или ущерба в результате применения информационных технологий, ИТ-риски).
18. Информационная война и агрессивная политика в Интернете (определение, в отношении своей страны, другой страны, цели, формы, примеры, терроризм, национализм, религиозный фанатизм).
19. Последствия развития Интернета в современных государствах. Основные угрозы со стороны Интернета для современного государства (в частности, политические и экономические).
20. Подходы к государственному регулированию Интернета в России и других государствах. Мероприятия и законодательные инициативы.

Комплект тестовых вопросов

по дисциплине «Основы информационной безопасности в правоохранительных органах»

Компетенции, формируемые в процессе изучения дисциплины

1. «Разъяснение, представление, понятие о чём-либо» сведения (сообщения, данные) неза- висимо от формы их представления -это………………………………………………….
2. Интерпретация информации – это
   * переход к семантическому смыслу.
   * переход к синтаксическому смыслу.
   * расшифровка информации
   * искажение информации
3. Какого типа бывает информации по отношению к источнику или приемнику
   * входная, выходная и внутренняя
   * исходная, промежуточная и результирующая
   * постоянная, переменная и смешанная
   * первичная и вторичная
4. Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуре

–это…………………………………………………………………………………..

1. Информация по ее изменчивости бывает:
   * входная, выходная и внутренняя
   * исходная, промежуточная и результирующая
   * постоянная, переменная и смешанная
   * первичная и вторичная
2. Информация по ее полноте бывает:
   * избыточная, достаточная и недостаточная
   * открытая (общедоступная) и закрытая (конфиденциальная)
   * входная, выходная и внутренняя
   * исходная, промежуточная и результирующая
3. Информация по доступу к ней бывает:
   * открытая (общедоступная) и закрытая (конфиденциальная)
   * избыточная, достаточная и недостаточная
   * исходная, промежуточная и результирующая
   * постоянная, переменная и смешанная
4. Комплекс мероприятий, направленных на обеспечение информационной безопасности это…………………………………………………………………………………………..
5. Информация, которая не зависит от личного мнения или суждения, называется:
   * достоверной
   * актуальной
   * объективной
   * полезной
   * понятной
6. Информационное право составляет:
   * нормативную базу информационного общества
   * государственную политику
   * нормативную базу аграрного общества
   * нормативную базу до индустриального общества
7. Регистрация доменных имён, содержащих торговую марку, принадлежащую другому лицу, с целью их дальнейшей перепродажи или недобросовестного использования -это

……………………………………………………………………..

1. Обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей –это…………………………………………………….
   * контрольный чек
   * ярлык
   * обозначение, служащее для индивидуализации товаров
   * договор купли-продажи
2. Информационные ресурсы по виду информации:
   * политическая
   * конфиденциальная
   * передвижная
   * на бумажном носителе
3. Основными техническими средствами являются:
   * средства связи и телекоммуникаций
   * прикладный программы
   * операционные системы
   * словари
4. Программа просмотра гипертекстовых страниц WWW:
   * браузер
   * протокол
   * сервер
   * HTML
5. Вспомогательное приспособление, позволяющее точнее провести какое-либо действие – это……………………………………………………………………………………….
6. Передача имущественных прав может осуществляться
   * на основе судебного иска
   * на основе авторского договора
   * без авторского договора
7. Кто является основным ответственным за определение уровня классификации информации
   * Руководитель среднего звена
   * Высшее руководство
   * Владелец
   * Пользователь
8. Укажите субъектов доступа к информации:
   * Носитель
   * Потребитель
   * Накопитель
   * Собственник
   * Владелец
9. Выбери правильный ответ
   * На чем основан принцип работы антивирусных мониторов:
   * На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю
   * На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
   * На подсчете контрольных сумм для присутствующих на диске файлов или

системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.

* + На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные

1. Выбери правильный ответ

На чем основан принцип работы антивирусных иммунизаторов:

* + На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные
  + На проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски
  + На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т.д.
  + На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю 22.Выбери правильный ответ

Что необходимо сделать при обнаружении файлового вируса?

* + Компьютер необходимо отключить от сети и проинформировать системного администратора
  + Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются
  + Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

1. Выбери правильный ответ

Что необходимо сделать при обнаружении загрузочного вируса:

* + Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются
  + Компьютер необходимо отключить от сети и проинформировать системного администратора
  + Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен

1. Выбери правильный ответ

В чем заключается метод защиты - ограничение доступа:

* + В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
  + В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
  + В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
  + В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. приведении её к неявному виду.

1. Несанкционированное копирование информации -это……………………………..
2. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название
   * Токен
   * Password
   * Login

Перечень основной и дополнительной учебной литературы

1. Молдованова, О. В. Информационные системы и базы данных : учебное пособие / О. В. Молдованова. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2017. — 178 c. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/45470.html>
2. Информационные технологии в юридической деятельности : учебное пособие для студентов вузов, обучающихся по специальностям «Юриспруденция» и

«Правоохранительная деятельность» / С. Я. Казанцев, Н. М. Дубинина, А. И. Уринцов [и др.] ; под редакцией А. И. Уринцова. — 2-е изд. — Москва : ЮНИТИ-ДАНА, 2020. — 352 c. — ISBN 978-5-238-03242-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/109189.html>

1. Шевко, Н. Р. Информационные технологии в юридической деятельности : учебное пособие

/ Н. Р. Шевко, С. Я. Казанцев, О. Э. Згадзай ; под редакцией С. Я. Казанцева. — Казань : Казанский юридический институт МВД России, 2018. — 230 c. — ISBN 978-5-901593-69-1.

— Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/86477.html>

1. Мистров, Л. Е. Информационные технологии в юридической деятельности. Microsoft Office 2010 : учебное пособие / Л. Е. Мистров, А. В. Мишин. — Москва : Российский государственный университет правосудия, 2018. — 232 c. — ISBN 978-5-93916-503-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/65857.htm>

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Российская газета <http://www.rg.ru/>
2. Журналы: Административное право, Горячая линия бухгалтера, Делопроизводство, Жилищное право, Мастер продаж, Секретарское дело, Трудовое право [http://www.top-](http://www.top-personal.ru/) [personal.ru/](http://www.top-personal.ru/)
3. Газета «Учет, налоги, право» <http://www.gazeta-unp.ru/>
4. Журнал «Домашний адвокат» <http://www.bestlawyers.ru/jr/jr.html>
5. Российский юридический журнал [http://www.ruzh.org](http://www.ruzh.org/)/