МИНИСТЕРСТВО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
"НЕФТЕКУМСКИЙ РЕГИОНАЛЬНЫЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ"

Комплект
Контрольно - оценочных средств по учебной дисциплине
ОП. 16 Информационная безопасность

основной профессиональной образовательной программы (ОПОП)
по специальности СПО
09.02.07 «Информационные системы и программирование»

2022 г.

ОДОБРЕНО:
НА ЗАСЕДАНИИ ПМО специальностей 09.02.03«Программирование в компьютерных системах», 09.02.02«Компьютерные сети» и профессии 09.01.03 «Мастер по обработке цифровой информации»
ПРОТОКОЛ №_3_
«03» ноября 2022 г.
Руководитель ПМО

 / И.А.Мазяр /

Комплект контрольно- оценочных средств составлен в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности **09.02.07 Информационные системы и программирование**

УТВЕРЖДАЮ:
Заместитель директора по УПР

 /З.К.Брилева /
(ФИО)

Составитель: Усенко Анна Геннадьевна, преподаватель ГБПОУ НРПК

Рецензент: Мазяр Ирина Анатольевна, преподаватель ГБПОУ НРПК

Содержание

1. Паспорт комплекта оценочных материалов

В результате освоения учебной дисциплины «Информационная безопасность» обучающийся должен обладать предусмотренными ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование» следующими умениями, знаниями, которые формируются общими компетенциями:

а) общие (ОК):

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

б*) профессиональные (ПК):*

ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.

В результате освоения дисциплины «Информационная безопасность» обучающийся должен обладать предусмотренными ФГОС и ПОП следующими умениями и знаниями:

Уметь:

У1. Обрабатывать текстовую и числовую информацию.

У2. Применять мультимедийные технологии обработки и представления информации.

У3.Обрабатывать экономическую и статистическую информацию, используя средства пакета прикладных программ.

знать:

З1.Назначение и виды информационных технологий, технологии сбора, накопления, обработки, передачи и распространения информации.

З2.Состав, структуру, принципы реализации и функционирования информационных технологий.

З3.Базовые и прикладные информационные технологии

З4.Инструментальные средства информационных технологий.

Практический опыт ФГОС СПО не предусмотрен.

Формой аттестации по дисциплине «Информационная безопасность» является дифференцированный зачет.

2. Результаты освоения дисциплины, подлежащие проверке

В результате аттестации по дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих компетенций:

Результаты обучения	Критерии обучения	Формы и методы обучения
Знания: **З1.** Назначение и виды информационных технологий, технологии сбора, накопления, обработки, передачи и распространения информации. **З2**. Состав, структуру, принципы реализации и функционирования информационных технологий. **З3.**Базовые и прикладные информационные технологии **З4**.Инструментальные средства информационных технологий. **Умения:** **У1.**Обрабатывать текстовую и числовую информацию. **У2.**Применять мультимедийные технологии обработки и представления информации. **У3.**Обрабатывать экономическую и статистическую информацию, используя средства пакета прикладных программ.	**«Отлично»** - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. **«Хорошо»** содержание полностью, некоторые теоретическое курса освоено без пробелов, умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. **«Удовлетворительно»** - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. **«Неудовлетворительно»** - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	•Компьютерное тестирование на знание терминологии по теме; Тестирование. Защита реферата.. Семинар Наблюдение за выполнением практического задания. (деятельностью студента) •Оценка выполнения практического задания(работы)

3. Оценка освоения дисциплины

3.1. Формы и методы оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС по дисциплине «Информационная безопасность», направленные на формирование общих компетенций

Проверяемые умения и знания	Форма контроля
Текущий контроль	
У1-У3	Практические занятия, Самостоятельная работа, Реферат
З1-З4	Устный опрос, Самостоятельная работа, Реферат, Тестирование
ОК1-2, ОК 4-5, ОК9	Устный опрос, Практические занятия, Самостоятельная работа, Тестирование
Промежуточная аттестация	
У1–У3; З 1 – З4; ОК1-2, ОК 4-5, ОК9; ПК4.4, ПК 11.6	Дифференцированный зачет.

3.2. Типовые задания для оценки освоения учебной дисциплины

Типовые вопросы для устного опроса

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности.
4. Надёжность и уязвимость информации в информационных системах.
5. Технические меры обеспечения ИБ.
6. Программно-математические меры обеспечения ИБ.
7. Разграничение доступа к защищаемой информации.
8. Административные меры обеспечения ИБ.
9. Законодательные и морально-этические меры обеспечения ИБ.
10. Криптографические методы обеспечения ИБ.
11. Контроль доступа к аппаратуре.
12. Использование простого и динамически изменяющегося пароля.
13. Особенности защиты информации в персональных компьютерах (ПК).
14. Идентификация и аутентификация пользователей в информационных системах.
15. Защита ПК от несанкционированного доступа.
16. Регистрация всех обращений к защищаемой информации.
17. Компьютерный вирус. Понятия и пути распространения вирусов.
18. Основные способы заражения программ.
19. Основные классы вирусов.
20. Программные и аппаратные закладки.
21. Классификация закладок и их общие характеристики.
22. Саморазмножающиеся и другие разновидности закладок.
23. Троянский конь.
24. Структура и способы распространения.
25. Временная и логическая бомба. Структура и способы распространения.
26. Винлокер. Структура и способы распространения.
27. Червь. Структура и способы распространения.
28. Признаки проявления вредоносных программ.
29. Классификация угроз для мобильных устройств.
30. Характеристика вредоносных программы для мобильных устройств.
31. Программы-вымогатели для мобильных устройств.
32. Вредоносные приложения.
33. Методики оценки рисков в сфере информационной безопасности.
34. Своевременная компьютерная профилактика.
35. Обязательное использование антивирусной защиты.
36. Физическое отключение внутренней сети организации от Интернета и использование для выхода в Интернет выделенных компьютеров.
37. Классификация антивирусных программ.
38. Программы-детекторы, программы-ревизоры и фильтры.
39. Программы-полифаги (доктора).
40. Профилактика заражения вирусом.
41. Антивирус Касперского.
42. Основы безопасности мобильных устройств.
43. Методы защиты мобильных устройств от киберугроз.
44. Специальная программа – «сканер».
45. Проверка в режиме «налету».
46. Проверка соответствия уровня защищенности ИС требованиям стандартов в области ИБ.

47. Программное обеспечение для оценки рисков информационной безопасности.
48. Оценка рисков по графику соотношения – «затраты на защиту — ожидаемые потери». Идентификация риска.
49. Модель безопасности с полным перекрытием.
50. Содержание и структура правового обеспечения.
51. Законодательство об информации, информационных технологиях и о защите информации.
52. Правовой режим информации.
53. Правовой статус обладателя информации.
54. Правовой режим информационных технологий.
55. Государственное регулирование отношений в сфере защиты информации.
56. Основные нормативно-правовые акты и методические документы в области защиты информации.
57. Основные общие нормативные правовые акты.
58. Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных.
59. Руководящие документы и методические указания в сфере защиты информации.
60. Персональные данных, их классификация.
61. Правовые основы использования персональных данных.
62. Принципы обработки персональных данных.
63. Создание и оценка соответствия информационной системы персональных данных.
64. Права субъектов персональных данных.
65. Обязанности оператора при обработке персональных данных.
66. Электронная цифровая подпись.

Критерии и шкала оценивания устного опроса

отлично	1) студент полно излагает материал, дает правильное определение основных понятий; 2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; 3) излагает материал последовательно и правильно с точки зрения норм литературного языка.
хорошо	студент дает ответ, удовлетворяющий тем же требованиям, что и для отметки, но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
удовлетворительно	студент обнаруживает знание и понимание основных положений данной темы, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
неудовлетворительно	студент обнаруживает незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «неудовлетворительно» отмечает такие недостатки в подготовке, которые являются серьезным препятствием к успешному овладению последующим материалом.

Типовые задания для рефератов

Примерные темы рефератов

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности.
4. Надёжность и уязвимость информации в информационных системах.
5. Административные меры обеспечения ИБ.
6. Законодательные и морально-этические меры обеспечения ИБ.
7. Криптографические методы обеспечения ИБ.
8. Использование простого и динамически изменяющегося пароля.
9. Идентификация и аутентификация пользователей в информационных системах.
10. Защита ПК от несанкционированного доступа.
11. Компьютерный вирус. Понятия и пути распространения вирусов.
12. Основные способы заражения программ.
13. Признаки проявления вредоносных программ.
14. Классификация угроз для мобильных устройств.
15. Характеристика вредоносных программы для мобильных устройств.
16. Программы-вымогатели для мобильных устройств.
17. Вредоносные приложения.
18. Методики оценки рисков в сфере информационной безопасности.
19. Программы-детекторы, программы-ревизоры и фильтры.
20. Программы-полифаги (доктора).
21. Профилактика заражения вирусом.
22. Антивирус Касперского.
23. Основы безопасности мобильных устройств.
24. Методы защиты мобильных устройств от киберугроз.
25. Проверка соответствия уровня защищенности ИС требованиям стандартов в области ИБ.
26. Программное обеспечение для оценки рисков информационной безопасности.
27. Законодательство об информации, информационных технологиях и о защите информации.
28. Государственное регулирование отношений в сфере защиты информации.
29. Основные нормативно-правовые акты и методические документы в области защиты информации.
30. Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных.
31. Руководящие документы и методические указания в сфере защиты информации.
32. Правовые основы использования персональных данных.
33. Принципы обработки персональных данных.
34. Создание и оценка соответствия информационной системы персональных данных.
35. Права субъектов персональных данных.
36. Обязанности оператора при обработке персональных данных.
37. Электронная цифровая подпись.

Критерии и шкала оценки реферата

Оценка	Характеристики ответа и реферата студента
отлично	выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
хорошо	основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
удовлетворительно	имеются существенные отступления от требований к реферированию. В частности: тема освещена частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
неудовлетворительно	тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Типовые практические работы

Семинарское занятие. Актуальность проблемы обеспечения безопасности информации

Цель занятия: Освоить студентам актуальность современной проблемы обеспечения безопасности информации.

Задание 1

Подготовка рефератов-докладов по вопросам темы занятия:

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности.
4. Надёжность и уязвимость информации в информационных системах.

Задание 2.

Подготовиться к обсуждению на семинарском занятии учебных вопросов:

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности.
4. Надёжность и уязвимость информации в информационных системах.

Методические рекомендации по выполнению заданий

Для выполнении задания 1 необходимо:

1) выбрать из предлагаемого перечня тему реферата-доклада или подобрать тему самостоятельно, при этом тема реферата должна соответствовать тематике учебных вопросов рассматриваемых в Задании 2 на семинарское занятие.

2) подобрать материал для написания реферата из рекомендуемых источников информации, а также из источников определенных в результате самостоятельного поиска в сети Интернет, печатных и электронных изданий специальной технической литературы и в населенных пунктах по месту проживания студента (для студентов заочной формы обучения);

3) оформить реферат согласно Приложения 1 к настоящим методическим указаниям.

Для выполнения задания 2 необходимо:

1) Изучить материал конспекта лекции по вопросам выносимым на семинарское занятие;

2) Изучить рекомендуемые информационные источники по вопросам, выносимым на семинарское занятие с использованием методических рекомендаций по работе с литературой, указанных в Приложении 2 к настоящим методическим указаниям.

Практическое занятие. Средства защиты от вредоносных программ.

Задание 1

Изобразить схему «Классификация антивирусных программ» с указанием программ-детекторов, программы-ревизоров и программ-фильтров.

Задание 2

Описать действия оператора ПК по профилактике заражения ПК вирусом.

Задание 3

Установить пробную версию антивируса от лаборатории Касперского на ПК.

Критерии и шкала оценки практического задания/работы

отлично	студент самостоятельно и правильно решил учебно-профессиональную задачу, уверенно, логично, последовательно и аргументировано излагал свое решение, используя понятия дисциплины.
хорошо	студент самостоятельно и в основном правильно решил учебно-профессиональную задачу, уверенно, логично, последовательно и аргументировано излагал свое решение, используя понятия дисциплины.
удовлетворительно	студент в основном решил учебно-профессиональную задачу, допустил несущественные ошибки, слабо аргументировал свое решение, используя в основном понятия дисциплины.
неудовлетворительно	ставится, если: студент не решил учебно-профессиональную задачу.

3.2.4. Типовые тестовые задания

1. Под информационной безопасностью понимается…

А) 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.

Б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия

В) нет правильного ответа

2.Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

7. Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

8. Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

9. Целостность можно подразделить:

А) статическую

Б) динамичную

В) структурную

10. Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные

12. Угроза – это…
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..
А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

15. Окно опасности – это…
А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?
А) должно стать известно о средствах использования пробелов в защите.
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:
А) по спектру И.Б.
Б) по способу осуществления
В) по компонентам И.С.

17. По каким компонентам классифицируется угрозы доступности:
А) отказ пользователей

Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

18. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные

19. Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

20. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

21. Какие существуют грани вредоносного П.О.?
А) вредоносная функция
Б) внешнее представление
В) способ распространения

22. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) все ответы правильные

23. Вирус – это…
А) код обладающий способностью к распространению путем внедрения в другие программы
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

24. Черви – это…
А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

25. Конфиденциальную информацию можно разделить:
А) предметную
Б) служебную
В) глобальную

26. Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

27. Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

28. К какому виду угроз относится присвоение чужого права?
А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

29. Отказ, ошибки, сбой – это:
А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

30. Отказ - это…
А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

31. Ошибка – это…
А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

32. Сбой – это…
А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

33. Побочное влияние – это…
А) негативное воздействие на систему в целом или отдельные элементы
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

34. СЗИ (система защиты информации) делится:
А) ресурсы автоматизированных систем
Б) организационно-правовое обеспечение
В) человеческий компонент

35. Что относится к человеческому компоненту СЗИ?
А) системные порты
Б) администрация

В) программное обеспечение

36. По уровню обеспеченной защиты все системы делят:
А) сильной защиты
Б) особой защиты
В) слабой защиты

37. По активности реагирования СЗИ системы делят:
А) пассивные
Б) активные
В) полупассивные

38. Правовое обеспечение безопасности информации – это…
А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

39. Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные
40. Информацию с ограниченным доступом делят:
А) государственную тайну
Б) конфиденциальную информацию
В) достоверную информацию

41. Что относится к государственной тайне?
А) сведения, защищаемые государством в области военной, экономической … деятельности
Б) документированная информация
В) нет правильного ответа

42. Вредоносная программа - это…
А) программа, специально разработанная для нарушения нормального функционирования систем
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

43. Основополагающие документы для обеспечения безопасности внутри организации:
А) трудовой договор сотрудников
Б) должностные обязанности руководителей
В) коллективный договор

44. К организационно - административному обеспечению информации относится:
А) взаимоотношения исполнителей
Б) подбор персонала
В) регламентация производственной деятельности

45. Что относится к организационным мероприятиям:

А) хранение документов

Б) проведение тестирования средств защиты информации

В) пропускной режим

46. Какие средства используется на инженерных и технических мероприятиях в защите информации:

А) аппаратные

Б) криптографические

В) физические

47. Программные средства – это…

А) специальные программы и системы защиты информации в информационных системах различного назначения

Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла

В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

48.. Криптографические средства – это…

А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

Критерии и шкала оценки тестовых заданий

Количество правильных ответов	**Оценка**
86 – 100%	отлично
71 – 85%	хорошо
53 – 70%	удовлетворительно
52%	неудовлетворительно

3.2.5. Типовые задания для самостоятельной работы

Подготовиться к семинарскому занятию на тему «Актуальность проблемы обеспечения безопасности информации».

Вопросы семинара:

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности.
4. Надёжность и уязвимость информации в информационных системах.

Методические рекомендации по написанию доклада – реферата или доклада с использованием разработанной презентации.

Доклад – это вид самостоятельной работы студентов, заключающийся в разработке студентами темы на основе изучения литературы и развернутом публичном сообщении по данной проблеме.

Цель доклада - сформировать научно-исследовательские навыки и умения у студентов, способствовать овладению методами научного познания, освоить навыки публичного выступления, научиться критически мыслить. При этом главная составляющая - это публичное выступление.

Этапы подготовки доклада:

выбор темы доклада;

подбор и изучение наиболее важных учебных, научных работ по данной теме, нормативных правовых актов;

анализ изученного материала, выделение наиболее значимых для раскрытия темы доклада фактов, мнений ученых;

составление плана доклада;

написание текста доклада с соблюдением требований научного стиля.

Структура доклада:

1. Вступление, в котором указываются:

тема доклада;

цель доклада;

связь данной темы с другими темами;

актуальность, проблематика темы;

краткий обзор изученной литературы по данной теме и т.п.

2. Основная часть, которая содержит логичное, последовательное изложение материала.

3. Заключение, в котором:

подводятся итоги, формулируются выводы;

подчеркивается значение рассмотренной проблемы;

выделяются основные проблемы, пути и способы их решения и т.п.;

4. Приложения (схемы, таблицы для более наглядного освещения темы).

Требования к оформлению доклада-реферата: согласно Приложения 1.

Методические рекомендации по подготовке презентации к докладу

Компьютерную презентацию, сопровождающую выступление докладчика, удобнее всего подготовить в программе MS Power Point. Презентация как документ представляет собой последовательность сменяющих друг друга слайдов - то есть электронных страничек, занимающих весь экран монитора (без присутствия панелей программы). Чаще всего демонстрация презентации проецируется на большом экране, реже - раздается собравшимся как печатный материал. Количество слайдов адекватно содержанию и продолжительности выступления (например, для 5-минутного выступления рекомендуется использовать не более 10 слайдов).

На первом слайде обязательно представляется тема выступления и сведения об

авторах. Следующие слайды можно подготовить, используя две различные стратегии их подготовки:

1 стратегия: на слайды выносится опорный конспект выступления и ключевые слова с тем, чтобы пользоваться ими как планом для

выступления. В этом случае к слайдам предъявляются следующие требования:

- объем текста на слайде - не больше 7 строк;

маркированный/нумерованный список содержит не более 7 элементов;

- отсутствуют знаки пунктуации в конце строк в маркированных и нумерованных списках;
- значимая информация выделяется с помощью цвета, кегля, эффектов анимации.

Особо внимательно необходимо проверить текст на отсутствие ошибок и опечаток. Основная ошибка при выборе данной стратегии состоит в том, что выступающие заменяют свою речь чтением текста со слайдов.

2 стратегия: на слайды помещается фактический материал (таблицы, графики, фотографии и пр.), который является уместным и достаточным средством наглядности, помогает в раскрытии стержневой идеи выступления. В этом случае к слайдам предъявляются следующие требования:

- выбранные средства визуализации информации (таблицы, схемы, графики и т. д.) соответствуют содержанию;
- использованы иллюстрации хорошего качества (высокого разрешения), с четким изображением (как правило, никто из присутствующих не заинтересован вчитываться в текст на ваших слайдах и всматриваться в мелкие иллюстрации);

Максимальное количество графической информации на одном слайде - 2 рисунка (фотографии, схемы и т.д.) с текстовыми комментариями (не более 2 строк к каждому). Наиболее важная информация должна располагаться в центре экрана.

Основная ошибка при выборе данной стратегии - «соревнование» со своим иллюстративным материалов (аудитории не предоставляется достаточно времени, чтобы воспринять материал на слайдах). Обычный слайд, без эффектов анимации должен демонстрироваться на экране не менее 10 - 15 секунд. За меньшее время присутствующие не успеет осознать содержание слайда. Если какая-то картинка появилась на 5 секунд, а потом тут же сменилась другой, то аудитория будет считать, что докладчик ее подгоняет. Обратного (позитивного) эффекта можно достигнуть, если докладчик пролистывает множество слайдов со сложными таблицами и диаграммами, говоря при этом «Вот тут приведен разного рода *вспомогательный* материал, но я его хочу пропустить, чтобы не перегружать выступление подробностями». Правда, такой прием делать в *начале* и в *конце* презентации - рискованно, оптимальный вариант -в середине выступления.

Если на слайде приводится сложная диаграмма, ее необходимо предварить вводными словами (например, «На этой диаграмме приводится то-то и то-то, зеленым отмечены показатели А, синим - показатели Б»), с тем, чтобы дать время аудитории на ее рассмотрение, а только затем приступать к ее обсуждению. Каждый слайд, в среднем должен находиться на экране не меньше 40 - 60 секунд (без учета времени на случайно возникшее обсуждение). В связи с этим лучше настроить презентацию не на автоматический показ, а на смену слайдов самим докладчиком.

Особо тщательно необходимо отнестись к ***оформлению презентации.*** Для всех слайдов презентации по возможности необходимо использовать один и тот же шаблон оформления кегль - для заголовков - не меньше 24 пунктов, для информации - не менее 18. В презентациях не принято ставить переносы в словах.

Подумайте, не отвлекайте ли вы слушателей своей же презентацией? Яркие краски, сложные цветные построения, излишняя анимация, выпрыгивающий текст или иллюстрация — не самое лучшее дополнение к научному докладу. Также нежелательны звуковые эффекты в ходе демонстрации презентации. Наилучшими являются контрастные цвета фона и текста (белый фон - черный текст; темно-синий фон - светло-желтый текст и

т. д.). Лучше не смешивать разные типы шрифтов в одной презентации. Рекомендуется не злоупотреблять прописными буквами (они читаются хуже).

Неконтрастные слайды будут смотреться тусклыми и невыразительными, особенно в светлых аудиториях. Для лучшей ориентации в презентации по ходу выступления лучше пронумеровать слайды. Желательно, чтобы на слайдах оставались поля, не менее 1 см с каждой стороны. Вспомогательная информация (управляющие кнопки) не должны преобладать над основной информацией (текстом,

иллюстрациями). Использовать встроенные эффекты анимации можно только, когда без этого не обойтись (например, последовательное появление элементов диаграммы). Для акцентирования внимания на какой-то конкретной информации слайда можно воспользоваться лазерной указкой.

Диаграммы готовятся с использованием мастера диаграмм табличного процессора MS Excel. Для ввода числовых данных используется числовой формат с разделителем групп разрядов. Если данные (подписи данных) являются дробными числами, то число отображаемых десятичных знаков должно быть одинаково для всей группы этих данных (всего ряда подписей данных). Данные и подписи не должны накладываться друг на друга и сливаться с графическими элементами диаграммы. Структурные диаграммы готовятся при помощи стандартных средств рисования пакета MS Office. Если при форматировании слайда есть необходимость пропорционально уменьшить размер диаграммы, то размер шрифтов реквизитов должен быть увеличен с таким расчетом, чтобы реальное отображение объектов диаграммы соответствовало значениям, указанным в таблице. В таблицах не должно быть более 4 строк и 4 столбцов — в противном случае данные в таблице будет просто невозможно увидеть. Ячейки с названиями строк и столбцов и наиболее значимые данные рекомендуется выделять цветом.

Табличная информация вставляется в материалы как таблица текстового процессора MS Word или табличного процессора MS Excel. При вставке таблицы как объекта и пропорциональном изменении ее размера реальный отображаемый размер шрифта должен быть не менее 18 pt. Таблицы и диаграммы размещаются на светлом или белом фоне.

Если Вы предпочитаете воспользоваться помощью оператора (что тоже возможно), а не листать слайды самостоятельно, очень полезно предусмотреть ссылки на слайды в тексте доклада ("Следующий слайд, пожалуйста...").

Заключительный слайд презентации, содержащий текст «Спасибо за внимание» или «Конец», вряд ли приемлем для презентации, сопровождающей публичное выступление, поскольку завершение показа слайдов еще не является завершением выступления. Кроме того, такие слайды, так же как и слайд «Вопросы?», дублируют устное сообщение. Оптимальным вариантом представляется повторение первого слайда в конце презентации, поскольку это дает возможность еще раз напомнить слушателям тему выступления и имя докладчика и либо перейти к вопросам, либо завершить выступление.

Для показа файл презентации необходимо сохранить в формате «Демонстрация PowerPoint» (Файл — Сохранить как — Тип файла — Демонстрация PowerPoint). В этом случае презентация автоматически открывается в режиме полноэкранного показа (slideshow) и слушатели избавлены как от вида рабочего окна программы PowerPoint, так и от потерь времени в начале показа презентации.

После подготовки презентации полезно проконтролировать себя вопросами:

- удалось ли достичь конечной цели презентации (что удалось определить, объяснить, предложить или продемонстрировать с помощью нее?);
- к каким особенностям объекта презентации удалось привлечь внимание аудитории?
- не отвлекает ли созданная презентация от устного выступления?

После подготовки презентации необходима репетиция выступления.

Требования к защите доклада на семинарском занятии:

1. Продолжительность выступления обычно не превышает 5-7 минут. Поэтому при подготовке доклада из текста реферата отбирается самое главное. В докладе должно быть

кратко отражено основное содержание всех глав и разделов исследовательской работы.

2. Для успешного выступления с докладом заучите значение всех терминов, которые употребляются в докладе.

3. При соблюдении этих правил у вас должен получиться интересный доклад, который, несомненно, будет высоко оценен преподавателем.

Критерии оценки самостоятельной работы

Максимальное количество баллов **«отлично»** студент получает, если:

– студент свободно применяет знания на практике, не допускает ошибок в воспроизведении изученного материала, выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;

– весь объем материала усвоен полностью;

– обстоятельно с достаточной полнотой излагает соответствующую тему;

– материал (задание) оформлен аккуратно в соответствии с заданием и требованиями к оформлению;

Оценку **«хорошо»** студент получает, если:

– студент знает весь изученный материал, отвечает без особых затруднений на вопросы преподавателя;

– применяет полученные знания на практике;

– в условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя;

– неполно, но правильно изложено задание;

– может обосновать свой ответ, привести необходимые примеры;

– материал оформлен недостаточно аккуратно, в соответствии с заданием и требованиями к оформлению.

Оценку **«удовлетворительно»** студент получает, если:

– студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;

– предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы;

– излагает выполнение задания недостаточно логично и последовательно;

– затрудняется при ответах на вопросы преподавателя;

– материал оформлен не аккуратно или не в соответствии с заданием и требованиями к оформлению.

Оценку **«неудовлетворительно»** студент получает, если:

– у студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена;

– задание изложено неполно, не соответствует заданию;

– при изложении были допущены существенные ошибки, задание не удовлетворяет требованиям к оформлению, установленным к данному виду работы.

4. Контрольно-оценочные материалы для промежуточной аттестации по дисциплине

Задачей промежуточной аттестации по дисциплине является комплексная оценка уровней достижения планируемых результатов обучения.

КОМ предназначен для контроля и оценки результатов освоения учебной дисциплины «Информационная безопасность» по специальности СПО 09.02.07 «Информационные системы и программирование».

Предметом оценки являются умения и знания, приобретенные в период освоения дисциплины.

Уметь:

У1. Обрабатывать текстовую и числовую информацию.

У2. Применять мультимедийные технологии обработки и представления информации.

У3.Обрабатывать экономическую и статистическую информацию, используя средства пакета прикладных программ.

знать:

З1.Назначение и виды информационных технологий, технологии сбора, накопления, обработки, передачи и распространения информации.

З2.Состав, структуру, принципы реализации и функционирования информационных технологий.

З3.Базовые и прикладные информационные технологии

З4.Инструментальные средства информационных технологий.

Промежуточная аттестация по дисциплине проводится в форме дифференцированного зачета по расписанию сессии.

Вопросы к экзамену доводятся до сведения студентов заранее.

Билет к зачету содержит 2 вопроса.

При подготовке к ответу пользование учебниками, учебно-методическими пособиями, средствами связи и электронными ресурсами на любых носителях запрещено.

Время на подготовку ответа – от 30 до 45 минут.

По истечении времени подготовки ответа, студент отвечает на вопросы экзаменационного билета. На ответ студента по каждому вопросу билета отводится, как правило, 3-5 минут.

После ответа студента преподаватель может задать дополнительные (уточняющие) вопросы в пределах предметной области экзаменационного задания.

После окончания ответа преподаватель объявляет обучающемуся оценку по результатам экзамена, а также вносит эту оценку в экзаменационную ведомость, зачетную книжку.

ЗАДАНИЕ ДЛЯ промежуточной аттестации
(дифференцированный зачет)

Вариант 1

Инструкция для обучающихся (экзамен)

Внимательно прочитайте вопросы и задание. Если Вам что-то непонятно, спросите у преподавателя.

Время на подготовку 30-45 минут.

При подготовке к ответу пользование учебниками, учебно-методическими пособиями, средствами связи и электронными ресурсами на любых носителях запрещено.

Билет 1

Вопрос 1. Административные меры обеспечения ИБ.

Вопрос 2. Основные нормативно-правовые акты и методические документы в области защиты информации.

Зачетная ведомость (или оценочный лист) заполняется в период промежуточной аттестации.

Критерии и шкала оценки экзамена

Оценка	**Характеристики ответа обучающегося**
Отлично	- студент глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой понятий по дисциплине; -правильно решил ситуационную задачу.
Хорошо	- студент твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой понятий по дисциплине; -правильно решил ситуационную задачу.
Удовлетворительно	- студент усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой понятий по дисциплине; - с затруднениями решил ситуационную задачу.
Неудовлетворительно	- студент не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений; - не решил ситуационную задачу

Перечень вопросов к дифференцированному зачету по дисциплине «Информационная безопасность»

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности (ИБ).
4. Надёжность и уязвимость информации в информационных системах.
5. Технические меры обеспечения ИБ.
6. Программно-математические меры обеспечения ИБ.
7. Разграничение доступа к защищаемой информации.
8. Административные меры обеспечения ИБ.
9. Законодательные и морально-этические меры обеспечения ИБ.
10. Криптографические методы обеспечения ИБ.
11. Контроль доступа к аппаратуре.
12. Использование простого и динамически изменяющегося пароля.
13. Особенности защиты информации в персональных компьютерах (ПК).
14. Идентификация и аутентификация пользователей в информационных системах.
15. Защита ПК от несанкционированного доступа.
16. Регистрация всех обращений к защищаемой информации.
17. Компьютерный вирус. Понятия и пути распространения вирусов.
18. Основные способы заражения программ.
19. Основные классы вирусов.
20. Классификация закладок и их общие характеристики.
21. Саморазмножающиеся и другие разновидности закладок.
22. Троянский конь. Структура и способы распространения.
23. Временная и логическая бомба. Структура и способы распространения.
24. Винлокер. Структура и способы распространения.
25. Червь. Структура и способы распространения.
26. Признаки проявления вредоносных программ.
27. Классификация угроз для мобильных устройств.
28. Характеристика вредоносных программы для мобильных устройств.
29. Программы-вымогатели для мобильных устройств.
30. Методики оценки рисков в сфере информационной безопасности.
31. Своевременная компьютерная профилактика от вирусов.
32. Использование антивирусной защиты.
33. Классификация антивирусных программ.
34. Основы безопасности мобильных устройств.
35. Методы защиты мобильных устройств от киберугроз.
36. Программное обеспечение для оценки рисков информационной безопасности.
37. Содержание и структура правового обеспечения информационной безопасности.
38. Государственное регулирование отношений в сфере защиты информации.
39. Основные нормативно-правовые акты и методические документы в области защиты информации.
40. Основные общие нормативные правовые акты по вопросам информационной безопасности.
41. Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных.
42. Персональные данных, их классификация.
43. Принципы обработки персональных данных.
44. Создание и оценка соответствия информационной системы персональных данных.
45. Права субъектов персональных данных.
46. Обязанности оператора при обработке персональных данных.
47. Электронная цифровая подпись.

3.2. Информационное обеспечение обучения
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники литературы:

1. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510
2. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для спо / В. И. Петренко, И. В. Мандрица. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744

Дополнительные источники:

1. Поляков, Е. А. Основы информационной безопасности : учебное пособие / Е. А. Поляков. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2021. — 71 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/282890
2. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. — Краснодар : КубГАУ, 2020. — 332 с. — ISBN 978-5-907346-50-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254168
3. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227

Интернет-ресурсы:

1. https://e.lanbook.com
2. https://t.lanbook.com/tests -сервис самотестирования
3. http://www.intuit.ru
4. Научная электронная библиотека «Киберленинка» – http://cyberleninka.ru/
5. Справочно-правовая система «КонсультантПлюс» - http://www.consultant.ru/
6. https://www.yandex.ru
7. http://www.rambler.ru