

ГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ
«НИЖЕГОРОДСКИЙ ПРОМЫШЛЕННО- ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

КОНТРОЛЬНО ОЦЕНОЧНЫЕ СРЕДСТВА

учебной дисциплины

ОП.04 Технические средства информатизации

специальность

10.02.01 «Организация и технология защиты информации»

Нижний Новгород
2022 г.

Контрольно-оценочные средства профессионального модуля учебной дисциплины ОП.04 Технические средства информатизации разработаны на основе ФГОС СПО по специальности: 10.02.01 Организация и технология защиты информации и рабочей программы учебной дисциплины ОП.04 Технические средства информатизации

Организация-разработчик:

ГБПОУ «Нижегородский промышленно-технологический техникум»

1. ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений студентов, освоивших программу учебной дисциплины ОП.06 Основы информационной безопасности.

КОС включают контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме экзамена.

КОС разработаны на основании следующих положений:

ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации;
основной профессиональной образовательной программы по специальности СПО 10.02.01 Основы информационной безопасности;
программы учебной дисциплины ОП.06 Основы информационной безопасности.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В процессе освоения дисциплины у обучающегося должны формироваться общие и профессиональные компетенции.

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

Умения:

У1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

У2 применять основные правила и документы системы сертификации Российской Федерации;

У3 классифицировать основные угрозы безопасности информации;

Знания:

З1 сущность и понятие информационной безопасности, характеристику ее составляющих;

З2 место информационной безопасности в системе национальной безопасности страны;

З3 источники угроз информационной безопасности и меры по их предотвращению;

З4 жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;

З5 современные средства и способы обеспечения информационной безопасности;

3 ОЦЕНКА ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Формы и методы контроля

Контроль и оценка освоения учебной дисциплины по темам

Формой аттестации по учебной дисциплине является **-Экзамен**

№	Контролируемые умения, знания	Контролируемые разделы (темы) учебной дисциплины	Наименование оценочного средства
1	У1	Тема 1 Политика и концепции информационной безопасности	Т, УО, А
2	У3	Тема 2 Уязвимость информации в информационных системах	Т, УО, А
3	У2 У3	Тема 3 Защита информации	ПЗ 1,- ПЗ16
4		Экзамен	Т, УО

Условные обозначения: ПЗ – практическое занятие, работа, УО – устный ответ, Т – тестирование, А - Анализ наблюдений за усвоением умений и знаний

Критерии оценивания устных и письменных ответов

Отметкой "ОТЛИЧНО" оценивается ответ, который показывает прочные знания основных процессов изучаемого вопроса, отличается глубиной и полнотой раскрытия темы, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа.

Отметкой "ХОРОШО" оценивается ответ, который показывает прочные знания основных процессов изучаемого вопроса, отличается глубиной и полнотой раскрытия темы, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако, допускается одна - две неточности в ответе.

Отметкой "УДОВЛЕТВОРИТЕЛЬНО" оценивается ответ, свидетельствующий в основном о знании процессов изучаемого вопроса, отличающийся недостаточной глубиной и полнотой раскрытия темы; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры;

недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа.

Отметкой "НЕУДОВЛЕТВОРИТЕЛЬНО" оценивается ответ, обнаруживающий незнание процессов изучаемого вопроса, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

Критерии оценивания тестирования

Процент результативности (правильных ответов)	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
60 ÷ 79	3	удовлетворительно
менее 60	2	неудовлетворительно

3.1. ЗАДАНИЯ ДЛЯ ОЦЕНКИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

ВХОДНОЙ КОНТРОЛЬ: ТЕСТИРОВАНИЕ

Оцениваемые знания: *остаточные знания по дисциплине*

Задание # 1

Вопрос:

Сопоставьте названия программ и изображений

Укажите соответствие для всех 6 вариантов ответа:



- Antivir
- DrWeb
- Nod 32
- Antivirus Kaspersky
- Avast
- Antivirus Panda

Задание # 2

Вопрос:

RAID-массив это

Выберите один из 5 вариантов ответа:

- 1) Набор жестких дисков, подключенных особым образом
- 2) Антивирусная программа

- 3) Вид хакерской утилиты
- 4) База защищенных данных
- 5) Брандмауэр

Задание # 3

Вопрос:

Выразите свое согласие или несогласие

Укажите истинность или ложность вариантов ответа:

- Почтовый червь активируется в тот момент, когда к вам поступает электронная почта
- Если компьютер не подключен к сети Интернет, в него не проникнут вирусы
- Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls
- Чтобы защитить компьютер недостаточно только установить антивирусную программу
- На Web-страницах могут находиться сетевые черви

Задание # 4

Вопрос:

Отметьте составные части современного антивируса

Выберите несколько из 5 вариантов ответа:

- 1) Модем
- 2) Принтер
- 3) Сканер
- 4) Межсетевой экран
- 5) Монитор

Задание # 5

Вопрос:

Вредоносные программы - это
(выберите один из вариантов ответа)

Выберите один из 5 вариантов ответа:

- 1) шпионские программы
- 2) программы, наносящие вред данным и программам, находящимся на компьютере
- 3) антивирусные программы
- 4) программы, наносящие вред пользователю, работающему на зараженном компьютере
- 5) троянские утилиты и сетевые черви

Задание # 6

Вопрос:

К вредоносным программам относятся:
(выберите несколько вариантов ответа)

Выберите несколько из 5 вариантов ответа:

- 1) Потенциально опасные программы
- 2) Вирусы, черви, трояны
- 3) Шпионские и рекламные программы
- 4) Вирусы, программы-шутки, антивирусное программное обеспечение
- 5) Межсетевой экран, брандмауэр

Задание # 7

Вопрос:

Сетевые черви это

Выберите один из 5 вариантов ответа:

- 1) Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты
- 2) Вирусы, которые проникнув на компьютер, блокируют работу сети

- 3) Вирусы, которые внедряются в документы под видом макросов
- 4) Хакерские утилиты управляющие удаленным доступом компьютера
- 5) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

Задание # 8

Вопрос:

К биометрической системе защиты относятся:
(выберите несколько вариантов ответа)

Выберите несколько из 5 вариантов ответа:

- 1) Защита паролем
- 2) Физическая защита данных
- 3) Антивирусная защита
- 4) Идентификация по радужной оболочке глаз
- 5) Идентификация по отпечаткам пальцев

Задание # 9

Вопрос:

Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...

Выберите один из 5 вариантов ответа:

- 1) Загрузочный вирус
- 2) Макровирус
- 3) Троян
- 4) Сетевой червь
- 5) Файловый вирус

Задание # 10

Вопрос:

Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию.

Запишите ответ:

Задание # 11

Вопрос:

Руткит - это...

Выберите один из 5 вариантов ответа:

- 1) вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю
- 2) разновидность межсетевое экрана
- 3) программа использующая для распространения Рунет (Российскую часть Интернета)
- 4) вредоносная программа, маскирующаяся под макрокоманду
- 5) программа для скрытого взятия под контроль взломанной системы

Задание # 12

Вопрос:

Компьютерные вирусы это

Выберите несколько из 5 вариантов ответа:

- 1) Вредоносные программы, наносящие вред данным.
- 2) Программы, уничтожающие данные на жестком диске
- 3) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.
- 4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера

5) Это скрипты, помещенные на зараженных интернет-страничках

Задание # 13

Вопрос:

Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

Выберите один из 5 вариантов ответа:

- 1) Загрузочный вирус
- 2) Макровирус
- 3) Файловый вирус
- 4) Сетевой червь
- 5) Троян

Задание # 14

Вопрос:

Укажите порядок действий при наличии признаков заражения компьютера

Укажите порядок следования всех 3 вариантов ответа:

- Сохранить результаты работы на внешнем носителе
- Запустить антивирусную программу
- Отключиться от глобальной или локальной сети

Задание # 15

Вопрос:

Вирус поражающий документы называется

Выберите один из 5 вариантов ответа:

- 1) Троян
- 2) Файловый вирус
- 3) Макровирус
- 4) Загрузочный вирус
- 5) Сетевой червь

Пакет преподавателя

Показатели оценки результатов освоения программы учебной дисциплины:

Номер задания	Показатели оценки результата (требования к выполнению задания)
1	3; 4; 1; 6; 2; 5;
2	1
3	Нет; Нет; Нет; Да; Да;
4	3; 4; 5;
5	2
6	1; 2; 3;
7	5

Номер задания	Показатели оценки результата (требования к выполнению задания)
8	4; 5;
9	1
10	троян
11	5
12	3
13	3
14	2; 3; 1;
15	3

Тестовые задания для экзаменуемого

Задание #1

Какие существуют основные уровни обеспечения защиты информации?

Выберите несколько из 7 вариантов ответа:

- 1) административный
- 2) физический
- 3) законодательный
- 4) программно-технический
- 5) процедурный
- 6) вероятностный
- 7) распределительный

Задание #2

В чем состоит задача криптографа?

Выберите один из 2 вариантов ответа:

- 1) обеспечить конфиденциальность и аутентификацию передаваемых сообщений
- 2) взломать систему защиты

Задание #3

Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

Запишите ответ:

- 1) Ответ:

Задание #4

Как подразделяются вирусы в зависимости от деструктивных возможностей?

Выберите один из 4 вариантов ответа:

- 1) Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы
- 2) Резидентные, нерезидентные
- 3) Безвредные, неопасные, опасные, очень опасные
- 4) Сетевые, файловые, загрузочные, комбинированные

Задание #5

Какие законы существуют в России в области компьютерного права?

Выберите несколько из 6 вариантов ответа:

- 1) о правовой ответственности
- 2) об информации, информатизации, защищенности информации
- 3) о гражданском долге
- 4) о государственной тайне
- 5) об авторском праве и смежных правах
- 6) о правовой охране программ для ЭВМ и БД

Задание #6

В чем заключается основная причина потерь информации, связанной с ПК?

Выберите один из 3 вариантов ответа:

- 1) с глобальным хищением информации
- 2) с появлением интернета
- 3) с недостаточной образованностью в области безопасности

Задание #7

Линейное шифрование -

Выберите один из 3 вариантов ответа:

- 1) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
- 2) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами
- 3) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу

Задание #8

К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

- 1) актуальность
- 2) конфиденциальность
- 3) целостность
- 4) доступность
- 5) дискретность

Задание #9

Разновидности угроз безопасности

Выберите несколько из 6 вариантов ответа:

- 1) программные
- 2) физические
- 3) программно-математические
- 4) организационные
- 5) техническая разведка
- 6) технические

Задание #10

Что такое криптология?

Выберите один из 3 вариантов ответа:

- 1) защищенная информация
- 2) область доступной информации
- 3) тайная область связи

Задание #11

Что такое компьютерный вирус?

Выберите один из 4 вариантов ответа:

- 1) Разновидность программ, которые способны к размножению
- 2) Разновидность программ, которые плохо работают
- 3) Разновидность программ, которые самоуничтожаются
- 4) Разновидность программ, которые не работают

Задание #12

Что является основой для формирования государственной политики в сфере информации? (Ответьте 1 словом)

Запишите ответ:

- 1) Ответ:

Задание #13			
Установите соответствие			
Укажите соответствие для всех 4 вариантов ответа:			
1)		Защита информации от утечки по материально-вещественному каналу	1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
2)		защита информации от утечки по акустическому каналу	2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
3)		Защита информации от утечки по электромагнитным каналам	3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей
4)		Защита информации от утечки по визуально-оптическому каналу	4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

Задание #14

К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

Запишите ответ:

1) Ответ:

Задание #15

Кто является знаковой фигурой в сфере информационной безопасности

Выберите один из 4 вариантов ответа:

- 1) Митник
- 2) Паскаль
- 3) Шеннон
- 4) Беббидж

Задание #16

К методам защиты от НСД относятся

Выберите несколько из 5 вариантов ответа:

- 1) увеличение доступа;
- 2) аутентификация и идентификация
- 3) разграничение доступа;
- 4) разделение доступа;
- 5) ограничение доступа.

Задание #17

К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

- 1) доступность
- 2) целостность
- 3) конфиденциальность
- 4) дискретность
- 5) актуальность

Задание #18

Под ИБ понимают

Выберите один из 3 вариантов ответа:

- 1) защиту информации от компьютерных вирусов
- 2) защиту от несанкционированного доступа
- 3) защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера

Задание #19

Надежным средством отвода наведенных сигналов на землю служит

Запишите ответ:

1) Ответ:

Задание #20

К видам защиты информации относятся:

Выберите несколько из 4 вариантов ответа:

- 1) юридические;
- 2) морально-этические;
- 3) административно-организационные;
- 4) правовые и законодательные;

Задание #21

Техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации- все это есть

Запишите ответ:

1) Ответ:

Задание #22

Какие атаки предпринимают хакеры на программном уровне?

Выберите несколько из 4 вариантов ответа:

- 1) атаки на уровне сетевого ПО
- 2) атаки на уровне пакетов прикладных программ
- 3) атаки на уровне СУБД
- 4) атаки на уровне ОС

Задание #23

"Маскарад"- это

Выберите один из 2 вариантов ответа:

- 1) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями
- 2) осуществление специально разработанными программами перехвата имени и пароля

Задание #24

Кодирование информации -

Выберите один из 2 вариантов ответа:

- 1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
- 2) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.

Задание #25

Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

Выберите один из 4 вариантов ответа:

- 1) системой уничтожения.
- 2) системой безопасности;
- 3) системой защиты;
- 4) системой угроз;

Задание #26

Под изоляцией и разделением (требование к обеспечению ИБ) понимают

Выберите один из 2 вариантов ответа:

- 1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)
- 2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

Задание #27

Физические средства защиты информации

Выберите один из 4 вариантов ответа:

- 1) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- 2) это программы, предназначенные для выполнения функций, связанных с защитой информации
- 3) средства, которые реализуются в виде автономных устройств и систем
- 4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Задание #28

Прочность защиты в АС

Выберите один из 3 вариантов ответа:

- 1) группа показателей защиты, соответствующая определенному классу защиты
- 2) способность системы защиты информации обеспечить достаточный уровень своей безопасности
- 3) вероятность не преодоления защиты нарушителем за установленный промежуток времени

Задание #29

Под ИБ понимают

Выберите один из 3 вариантов ответа:

- 1) защиту информации от компьютерных вирусов
- 2) защиту от несанкционированного доступа
- 3) защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера

Задание #30				
Установите соответствие				
Укажите соответствие для всех 2 вариантов ответа:				
1)		стеганография	1)	наука о скрытой передаче информации путем сохранения в тайне самого факта передачи
2)		криптография	2)	наука скрывающая содержимое секретного сообщения

Задание #31

Что такое несанкционированный доступ (НСД)?

Выберите один из 5 вариантов ответа:

- 1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
- 2) Удаление не нужной информации
- 3) Создание резервных копий в организации
- 4) Правила и положения, выработанные в организации для обхода парольной защиты
- 5) Вход в систему без согласования с руководителем организации

Задание #32

Угроза - это

Выберите один из 2 вариантов ответа:

- 1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов
- 2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

Задание #33

Утечка информации

Выберите один из 3 вариантов ответа:

- 1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
- 2) потеря, хищение, разрушение или неполучение переданных данных
- 3) ознакомление постороннего лица с содержанием секретной информации

Задание #34

Что такое криптография?

Выберите один из 3 вариантов ответа:

- 1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
- 2) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом
- 3) область доступной информации

Задание #35

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется

Выберите один из 4 вариантов ответа:

- 1) кодируемой
- 2) недостоверной
- 3) защищаемой
- 4) шифруемой

Задание #36

Что такое аутентификация?

Выберите один из 5 вариантов ответа:

- 1) Определение файлов, из которых удалена служебная информация
- 2) Нахождение файлов, которые изменены в информационной системе несанкционированно
- 3) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
- 4) Определение файлов, из которых удалена служебная информация
- 5) Проверка количества переданной и принятой информации

Задание #37

Продолжите фразу: " Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой - это..."

Запишите ответ:

- 1) Ответ:

Задание #38

Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется

Выберите один из 4 вариантов ответа:

- 1) защитой информации
- 2) организацией безопасности
- 3) политикой информации
- 4) политикой безопасности

Задание #39

Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

Выберите один из 4 вариантов ответа:

- 1) сетевого программного обеспечения и системы управления базами данных.
- 2) операционной системы, сетевого программного обеспечения и системы управления базами данных;
- 3) операционной системы, сетевого программного обеспечения
- 4) операционной системы, системы управления базами данных;

Задание #40

Верификация -

Выберите один из 3 вариантов ответа:

- 1) проверка целостности и подлинности инф, программы, документа
- 2) это проверка принадлежности субъекту доступа предъявленного им идентификатора.
- 3) это присвоение имени субъекту или объекту

Задание #41

Выделите группы, на которые делятся средства защиты информации:

Выберите один из 3 вариантов ответа:

- 1) химические, аппаратные, программные, криптографические, комбинированные;
- 2) физические, аппаратные, программные, криптографические, комбинированные;
- 3) физические, аппаратные, программные, этнографические, комбинированные;

Задание #42

Вставьте пропущенное слово:

Информация может быть защищена без аппаратных и программных средств защиты с помощью _____ преобразований.

Запишите ответ:

- 1) Ответ:

Задание #43

Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это

Выберите один из 4 вариантов ответа:

- 1) данные
- 2) текст
- 3) информация
- 4) пароль

Задание #44

Организационные угрозы подразделяются на

Выберите несколько из 4 вариантов ответа:

- 1) физические угрозы
- 2) угрозы воздействия на персонал
- 3) действия персонала
- 4) несанкционированный доступ

Задание #45

Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

Выберите один из 4 вариантов ответа:

- 1) предостережением.
- 2) опасностью;
- 3) намерением;
- 4) угрозой;

Задание #46

Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы

Запишите ответ:

- 1) Ответ:

Задание #47

Основные группы технических средств ведения разведки

Выберите несколько из 5 вариантов ответа:

- 1) дистанционное прослушивание разговоров
- 2) системы определения местоположения контролируемого объекта
- 3) радиомикрофоны
- 4) электронные "уши"
- 5) фотоаппараты

Задание #48

Уровень секретности - это

Выберите один из 2 вариантов ответа:

- 1) ответственность за модификацию и НСД информации
- 2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

Задание #49

Виды технической разведки (по месту размещения аппаратуры)

Выберите несколько из 7 вариантов ответа:

- 1) магнитометрическая
- 2) морская
- 3) воздушная
- 4) фотографическая
- 5) оптическая
- 6) космическая
- 7) наземная

Задание #50

Способ представления информации в вычислительных системах

Запишите ответ:

- 1) Ответ:

Задание #51

Продолжите фразу: "Административная и законодательная мера, соответствующая мере ответственности лица за потерю конкретной секретной информации, регламентирующаяся специальным документом с учетом государственных и военно-стратегических, коммерческих или частных интересов - это..."

Запишите ответ:

- 1) Ответ:

Задание #52

Что такое целостность информации?

Выберите один из 4 вариантов ответа:

- 1) Свойство информации, заключающееся в ее существовании в виде единого набора файлов
- 2) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)
- 3) Свойство информации, заключающееся в возможности изменения только единственным пользователем
- 4) Свойство информации, заключающееся в возможности ее изменения любым субъектом

Задание #53

Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации называется

Запишите ответ:

- 1) Ответ:

Задание #54

Технические средства защиты информации

Выберите один из 4 вариантов ответа:

- 1) средства, которые реализуются в виде электрических, электромеханических и электронных устройств
- 2) это программы, предназначенные для выполнения функций, связанных с защитой информации
- 3) средства, которые реализуются в виде автономных устройств и систем
- 4) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

Задание #55

Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется

Запишите ответ:

- 1) Ответ:

Пакет преподавателя
Показатели оценки результатов освоения программы учебной дисциплины:

Номер задания	Показатели оценки результата (требования к выполнению задания)	Номер задания	Показатели оценки результата (требования к выполнению задания)
1.	1, 3, 4, 5	29.	3
2.	1	30.	1=1, 2=2
3.	Ответ = Техническая	31.	1
4.	3	32.	1
5.	2, 4, 5, 6	33.	3
6.	3	34.	1
7.	1	35.	3
8.	2, 3, 4	36.	3
9.	3, 4, 5	37.	Ответ = пароль
10.	3	38.	4
11.	1	39.	2
12.	Ответ = доктрина	40.	1
13.	1=2, 2=3, 3=1, 4=4	41.	2
14.	Ответ = организационного	42.	Ответ = криптографических
15.	1	43.	3
16.	2, 3, 4, 5	44.	2, 3
17.	1, 2, 3	45.	4
18.	3	46.	Ответ = аутентификации
19.	Ответ = заземление	47.	2, 3, 4
20.	2, 3, 4	48.	2
21.	Ответ = средство защиты информации	49.	2, 3, 6, 7
22.	1, 3, 4	50.	Ответ = двоичный код
23.	1	51.	Ответ = уровень секретности
24.	2	52.	2
25.	3	53.	Ответ = несанкционированным доступом

Номер задания	Показатели оценки результата (требования к выполнению задания)	Номер задания	Показатели оценки результата (требования к выполнению задания)
26.	2	54.	1
27.	3	55.	Ответ = каналом утечки информации
28.	3		

Критерии оценивания тестирования

Процент результативности (правильных ответов)	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 ÷ 100	5	отлично
80 ÷ 89	4	хорошо
70 ÷ 79	3	удовлетворительно
менее 70	2	неудовлетворительно

Примерные экзаменационные билеты по дисциплине ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 1

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.
2. Архитектура механизмов защиты информации в сетях ЭВМ.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 2

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Основные составляющие и аспекты информационной безопасности
2. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 3

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Классификация угроз информационной безопасности: для личности, для общества, для государства.
2. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 4

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.
2. Проблемы защиты информации в вычислительных сетях.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 5

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Концепция «информационной войны» по оценкам российских спецслужб.

2. В чём заключаются задачи защиты в сетях передачи данных?

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 6

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?

2. Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 7

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Сфера применения информационного оружия.

2. Программы-ревизоры. Программы-фильтры.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 8

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Особенности информационного оружия. Организация защиты.

2. Антивирусы-полифаги. Эвристические анализаторы

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 9

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Основные задачи в сфере обеспечения информационной безопасности.
2. Антивирусные программы. Программы-детекторы. Программы-доктора.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 10

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Отечественные стандарты в области информационной безопасности
2. Методы защиты от вирусов.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 11

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Зарубежные стандарты в области информационной безопасности

2. Как работает вирус?

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 12

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?

2. Способы заражения программ. Стандартные методы заражения.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 13

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Основные критерии оценки надежности: политика безопасности и гарантированность
2. По каким признакам классифицируются вирусы?

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 14

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Понятие государственной тайны. Понятие профессиональной тайны.
2. Компьютерный вирус. Какая программа считается зараженной..

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 15

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Понятие коммерческой тайны. Понятие служебной тайны. Понятие банковской тайны.

2. Методы и средства защиты от закладок..

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 16

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере.

2. Общие характеристики закладок.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 17

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.
2. Программные закладки. Классификация критериев вредоносного воздействия закладок.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 18

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Уязвимость информации в автоматизированных системах обработки данных.
2. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки..

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 19

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Элементы и объекты защиты в автоматизированных системах обработки данных.
2. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации. Дать краткую характеристику.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 20

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Методы защиты информации от преднамеренного доступа.
2. Защита ПК от несанкционированного доступа.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 21

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Защита информации от исследования и копирования.
2. Обеспечение целостности информации в ПК. Физическая защита ПК и носителей информации.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 22

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Ознакомление с использованием простого пароля. Метод обратимого шифрования.
2. Угрозы информации в персональных ЭВМ.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 23

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
2. Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 24

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Использование динамически изменяющегося пароля. Метод «запрос-ответ»
2. Классификация методов криптографического закрытия.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 25

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Использование динамически изменяющегося пароля. Функциональные методы
2. Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.

Составил преподаватель:

Свитнев Д.Н.

«ГБПОУ «Нижегородский промышленно- технологический техникум»

СОГЛАСОВАНО

На заседании ПЦК

Председатель _____ Д.Н. Свитнев

Протокол № __ от «__» _____ г.

УТВЕРЖДАЮ

Зам. директора по УПР

_____ И.А. Пронина

«__» _____ г.

Экзаменационный билет № 26

Дисциплина ОП.06 Основы информационной безопасности

Специальность 10.02.01 организация и технология защиты информации

1. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.
2. Электронная (цифровая) подпись. Цели применения электронной подписи.

Составил преподаватель:

Свитнев Д.Н.