МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ КРАСНОДАРСКОГО КРАЯ

«НОВОРОССИЙСКИЙ КОЛЛЕДЖ РАДИОЭЛЕКТРОННОГО ПРИБОРОСТРОЕНИЯ»
ИМЕНИ ГЕНЕРАЛ-МАЙОРА СУХОВЕЦКОГО А.А.
(ГБПОУ КК НКРП)

Комплект оценочных средств

для проведения промежуточной аттестации в форме экзамена

по учебной дисциплине ОП.06 Основы информационной безопасности

в рамках программы подготовки специалистов среднего звена (ППССЗ)

по специальности СПО

10.02.01 Организация и технология защиты информации

2023

СОГЛАСОВАНО
Зам. директора по УМР
_____ Е.В. Кужилева
30 08 2023 г.

УТВЕРЖДАЮ
Зам. директора по УР
_____ Т.В.Трусова
30 08 2023 г.

Одобрен
УМО общепрофессиональных
и специальных дисциплин
специальностей 09.02.03, 10.02.01, 10.02.03
Протокол от 30.08.2023 г. № 1
Председатель УМО
_____О.А.Афиногенова

Комплект оценочных средств для проведения промежуточной аттестации по учебной дисциплине ОП.06. Основы информационной безопасности разработан на основе требований ФГОС среднего общего образования (приказ Министерства образования и науки РФ от 28.07.2014 г. № 805, зарегистрирован в Минюст России от 21.08.2014 г. № 33750), рабочей программы учебной дисциплины ОП.06.Основы информационной безопасности (утв. директором колледжа), Положения о текущем контроле и промежуточной аттестации обучающихся, осваивающих образовательные программы среднего профессионального образования (утв. директором колледжа), Положения о формировании комплекта оценочных средств по учебной дисциплине, междисциплинарному курсу в ГБПОУ КК НКРП (утв. директором колледжа)

Организация-разработчик: ГБПОУ КК «Новороссийский колледж радиоэлектронного приборостроения» (далее ГБПОУ КК НКРП)

Разработчик:
преподаватель ГБПОУ КК НКРП _____ Д.И.Гурская

Рецензенты:
_____ (ФИО, Ревин О.И., главный инженер ООО ВЭН-КО
должность место работы)
_____ (ФИО, Кодорь А.В., директор НПО "Новороссийские системы"
должность место работы)

Рецензия

на комплект оценочных средств учебной дисциплины ОП.06 Основы информационной безопасности

специальности 10.02.01 Организация и технология защиты информации

Подготовлен Гурской Д.И. преподавателем ГБПОУ КК НКРП

Комплект оценочных средств для проведения промежуточной аттестации в форме экзамена по учебной дисциплине ОП.06 Основы информационной безопасности разработан на основе ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации.

Методическая разработка содержит:

- Паспорт комплекта оценочных средств, где указана область применения комплекта оценочных средств

- Комплект оценочных средств, где представлены задания для проведения экзамена в виде теста и условия выполнения задания

- Пакет экзаменатора

- Методические материалы, определяющие процедуры оценивания знаний, умений и практического опыта, характеризующие этапы формирования компетенций.

В соответствии с ФГОС СПО контрольно-оценочные средства являются составной частью нормативно-методического обеспечения системы оценки качества освоения студентами ППССЗ СПО.

Паспорт комплекта оценочных средств имеет содержательные связи общих и профессиональных компетенций с их компонентами (знаниями, умениями, элементами практического опыта) в контексте требований к результатам подготовки по программе учебной дисциплине ОП.06 Основы информационной безопасности.

Объем комплекта оценочных средств соответствует учебному плану подготовки. По качеству комплект оценочных средств в целом обеспечивает объективность и достоверность результатов при проведении оценивания с различными целями, дает возможность определить соответствие студентов конкретной квалификационной характеристики.

Структура комплекта соответствует современным требованиям. Содержание каждого его элемента разработано с достаточной степенью полноты и законченности.

Таким образом, рецензируемый комплект оценочных средств содержит все необходимые элементы рекомендуемой структуры, обладает достаточной полнотой и законченностью, является ценным практическим документом данной дисциплины.

Рецензент:

подпись Федоров А.В., инженер НПО "НовоТест Системы"

Рецензия

на комплект оценочных средств учебной дисциплины ОП.06 Основы информационной безопасности

специальности 10.02.01 Организация и технология защиты информации

составил преподаватель Гурская Д.И.

Содержание комплекта оценочных средств для проведения промежуточной аттестации в форме экзамена по учебной дисциплине ОП.06 Основы информационной безопасности соответствует уровню знаний выпускников среднего специального учебного заведения.

Структура комплекта соответствует современным требованиям, необходимый объем знаний, умений и навыков студентов соответствует обязательному минимуму содержания среднего специального учебного заведения.

Паспорт комплекта оценочных средств содержательные связи общих и профессиональных компетенций с их компонентами (знаниями, умениями, элементами практического опыта) в контексте требований к результатам подготовки по программе учебной дисциплине ОП.06 Основы информационной безопасности.

Контрольно-оценочные материалы для экзамена, представленные в КОС предназначены для контроля и оценки результатов освоения учебной дисциплине ОП.06 Основы информационной безопасности.

При помощи комплекта оценочных средств осуществляется контроль и управление процессом приобретения студентами необходимых знаний, умений, практического опыта и компетенций, определенных ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации.

Объем комплекта оценочных средств соответствует учебному плану подготовки. По качеству комплект оценочных средств в целом обеспечивает объективность и достоверность результатов при проведении оценивания с различными целями, дает возможность определить соответствие студентов конкретной квалификационной характеристики.

Направленность КОС соответствует целям по специальности 10.02.01 Организация и технология защиты информации, будущей профессиональной деятельности студента.

Таким образом, рецензируемый комплект оценочных средств содержит все необходимые элементы рекомендуемой структуры, обладает достаточной плотностью и законченностью.

Рецензент: 

О.А.Афиногенова, преподаватель высшей квалификационной категории ГБПОУ КК НКРП

1 Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

Комплект оценочных средств (КОС) предназначен для оценки результатов освоения учебной дисциплины ОП.06 Основы информационной безопасности

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

Результаты освоения (объекты оценивания)	**Основные показатели оценки результата и их критерии**	**Тип задания № задания**	**Форма аттестации (в соответствии с учебным планом)**
Умение			
классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	определять степень конфиденциальности, уметь определять вид тайн для защищенной информации	Текущий контроль. Экзамен.	Выполнение практических занятий №1,5,6,8. Аудиторная и внеаудиторная самостоятельная работа, анализ выполнения практических заданий.
применять основные правила и документы системы сертификации Российской Федерации	уметь защищать информацию и поддерживающую инфраструктуру от случайных или преднамеренных воздействий	Текущий контроль. Экзамен.	Выполнение практических занятий №10,11,12. Аудиторная и внеаудиторная самостоятельная работа, анализ выполнения практических заданий.
классифицировать основные угрозы безопасности информации	определять основные угрозы безопасности информации	Текущий контроль. Экзамен.	Выполнение практических занятий №2,3,4,7,9. Аудиторная и внеаудиторная самостоятельная работа, анализ выполнения практических заданий.
сущность и понятие информационной безопасности, характеристику ее составляющих	правильность понимания сущности и значимости информационной безопасности	Контрольная работа. Тестирование. Экзамен.	Аудиторная и внеаудиторная самостоятельная работа, проверка знаний по лекциям.

место информационной безопасности в системе национальной безопасности страны	понять какое место информационной безопасности в системе национальной безопасности страны	Контрольная работа. Тестирование. Экзамен.	Аудиторная и внеаудиторная самостоятельная работа, проверка знаний по лекциям.
источники угроз информационной безопасности и меры по их предотвращению	изучить основные источники угроз и меры по их предотвращению	Контрольная работа. Тестирование. Экзамен.	Аудиторная и внеаудиторная самостоятельная работа, проверка знаний по лекциям.
жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	изучить конфиденциальную информацию	Контрольная работа. Тестирование. Экзамен.	Аудиторная и внеаудиторная самостоятельная работа, проверка знаний по лекциям.
современные средства и способы обеспечения информационной безопасности	изучить информационную безопасность	Контрольная работа. Тестирование. Экзамен.	Аудиторная и внеаудиторная самостоятельная работа, проверка знаний по лекциям.

2 Комплект оценочных средств

2.1 Объект оценивания «Знание»: сущность и понятие информационной безопасности, характеристику ее составляющих, место информационной безопасности в системе национальной безопасности страны, источники угроз информационной безопасности и меры по их предотвращению, жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи, современные средства и способы обеспечения информационной безопасности.

Тест

Задание # 1

Вопрос:

Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:

Выберите несколько из 6 вариантов ответа:

1) конфиденциальность
2) целостность
3) доступность
4) учет
5) неотрекаемость
6) мобильность

Задание # 2

Вопрос:

Сопоставьте понятия и их определения.

Укажите соответствие для всех 5 вариантов ответа:

1) возможность ознакомиться с информацией имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями.
2) возможность внести изменение в информацию должны иметь только те лица, кто на это уполномочен.
3) возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.
4) все значимые действия лица, выполняемые им в рамках, контролируемых системой безопасности, должны быть зафиксированы и проанализированы.
5) лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения.

__ конфиденциальность
__ целостность
__ доступность
__ учет
__ неотрекаемость

Задание # 3

Вопрос:

... - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.

Выберите один из 5 вариантов ответа:

1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание # 4

Вопрос:

... - распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности.

Выберите один из 5 вариантов ответа:

1) Политика

2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание # 5

Вопрос:

... - обеспечение уверенности в том, что участник процесса обмена информацией определен верно, т.е. действительно является тем, чей идентификатор он предъявил.

Выберите один из 5 вариантов ответа:

1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание # 6

Вопрос:

... - создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа.

Выберите один из 5 вариантов ответа:

1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание # 7

Вопрос:

... - формирование профиля прав для конкретного участника процесса информационного обмена из набора правил контроля доступа.

Выберите один из 5 вариантов ответа:

1) Политика
2) Идентификация
3) Аутентификация
4) Контроль доступа
5) Авторизация

Задание # 8

Вопрос:

... - обеспечение соответствия возможных потерь от нарушения информационной безопасности затратам на их построение.

Выберите один из 5 вариантов ответа:

1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

Задание # 9

Вопрос:

... - поддержание среды информационного обмена в минимально допустимом работоспособном состоянии и соответствии требованиям информационной безопасности в условиях деструктивны внешних или внутренних воздействий.

Выберите один из 5 вариантов ответа:

1) Реагирование на инциденты
2) Управление конфигурацией
3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

Задание # 10

Вопрос:

... - совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности.

Выберите один из 5 вариантов ответа:

1) Реагирование на инциденты
2) Управление конфигурацией

3) Управление пользователями
4) Управление рисками
5) Обеспечение устойчивости

Задание # 11

Вопрос:

Перечислите основные направления информационной безопасности.

Выберите несколько из 4 вариантов ответа:

1) Физическая безопасность
2) Компьютерная безопасность
3) Визуальная безопасность
4) Сензитивная безопасность

Задание # 12

Вопрос:

Перечислите состав службы информационной безопасности.

Выберите несколько из 6 вариантов ответа:

1) Руководитель службы
2) Операционный отдел
3) Исследовательский отдел
4) Методический отдел
5) Отдел общения с прессой
6) Отдел бухгалтерии

Задание # 13

Вопрос:

Составление списка объектов, которые будут подлежать защите, и субъектов, которые задействованы в данном информационном пространстве, и будут влиять на информационную защиту системы, - это ...

Запишите ответ:

_____

Задание # 14

Вопрос:

Критериями определения уровня безопасности систем являются:

Выберите несколько из 5 вариантов ответа:

1) Оранжевая книга
2) Красная книга
3) Зеленая книга
4) Серо-буромалиновая книга
5) Белая книга

Задание # 15

Вопрос:

... - выпущенные Министерством обороны США критерии оценки уровня безопасности компьютерных систем.

Выберите один из 5 вариантов ответа:

1) Оранжевая книга
2) Красная книга
3) Белая книга
4) Зеленая книга
5) Открытая книга

Задание # 16

Вопрос:

... - выпущенные Министерством обороны США расширение критериев оценки уровня безопасности компьютерных систем для случаев использования компьютерных систем в информационной сети.

Выберите один из 5 вариантов ответа:

1) Оранжевая книга
2) Красная книга
3) Белая книга
4) Зеленая книга
5) Открытая книга

Задание # 17

Вопрос:

Перечислите модели классификации информационных объектов.

Выберите несколько из 5 вариантов ответа:

1) По наличию
2) По несанкционированной модификации (целостность)

3) По разглашению
4) По принадлежности
5) По аппелируемости

Задание # 18

Вопрос:

Какой считается информация, по классификации информационных объектов, если без нее можно работать, но очень короткое время.

Выберите один из 6 вариантов ответа:

1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

Задание # 19

Вопрос:

Какой считается информация, по классификации информационных объектов, если без нее можно работать, но ее использование экономит ресурсы.

Выберите один из 6 вариантов ответа:

1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

Задание # 20

Вопрос:

Какой считается по классификации информационных объектов устаревшая или неиспользуемая информация, не влияющая на работу субъекта.

Выберите один из 6 вариантов ответа:

1) критической
2) очень важной
3) важной
4) полезной
5) несущественной
6) вредной

Задание # 21

Вопрос:

Какой считается информация, по классификации информационных объектов, разглашение которой может принести моральный ущерб в очень редких случаях.

Выберите один из 6 вариантов ответа:

1) критической
2) очень важной
3) важной
4) значимой
5) малозначимой
6) незначимой

Задание # 22

Вопрос:

Какой считается информация, по классификации информационных объектов, если ее несанкционированное изменение скажется через некоторое время, но не приведет к сбою в работе субъекта, последствия модификации необратимы.

Выберите один из 6 вариантов ответа:

1) критической
2) очень важной
3) важной
4) значимой
5) малозначимой
6) незначимой

Задание # 23

Вопрос:

Жизненный цикл информации состоит из следующих стадий:

Выберите несколько из 4 вариантов ответа:
1) Информация используется в операционном режиме
2) Информация используется в архивном режиме
3) Информация хранится в архивном режиме
4) Информация хранится в операционном режиме

Задание # 24
Вопрос:
Какие существуют основные классы атак?
Выберите несколько из 5 вариантов ответа:
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Атака фрикера
5) Распределенная атака

Задание # 25
Вопрос:
... - это случай, когда злоумышленник оказался непосредственно перед клавиатурой данного компьютера
Выберите один из 5 вариантов ответа:
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Распределенная атака
5) Атака фрикера

Задание # 26
Вопрос:
... - это вариант атаки, когда злоумышленник не видит ту рабочую станцию, с которой он работает.
Выберите один из 5 вариантов ответа:
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Рейдерская атака
5) Социальная инженерия

Задание # 27
Вопрос:
... - это вариант атаки, когда атакуемый компьютер активно отправляет, принимает или обменивается с данными с другими компьютерами сети, локальной или глобальной, а местом приложения атакующего воздействия является сегмент сети или сетевой узел между этими системами.
Выберите один из 5 вариантов ответа:
1) Локальная атака
2) Удаленная атака
3) Атака на поток данных
4) Рейдерская атака
5) Социальная инженерия

Задание # 28
Вопрос:
... - идейный борец за свободу информации, вторгающийся в чужие системы в основном из интереса, без прямой материальной заинтересованности.
Выберите один из 5 вариантов ответа:
1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

Задание # 29
Вопрос:
... - тот, кто взламывает чужие системы, преследуя собственный финансовый интерес.
Выберите один из 5 вариантов ответа:
1) Хакер
2) Кракер
3) Фрикер

4) Джокер
5) Анонимайзер

Задание # 30

Вопрос:

... - злоумышленник, использующий в собственных интересах уязвимости в телефонных системах.

Выберите один из 5 вариантов ответа:

1) Хакер
2) Кракер
3) Фрикер
4) Джокер
5) Анонимайзер

Задание # 31

Вопрос:

... - это набор мероприятий по сбору сведений об информационной системе, напрямую не связанный с техническими подробностями реализации системы, основанный на человеческом факторе.

Запишите ответ:

_____

Задание # 32

Вопрос:

... в аппаратном обеспечении -это устройство, которое выполняет некоторые недокументированные функции, обычно в ущерб пользователю данной информационной системы.

Запишите ответ:

_____

Задание # 33

Вопрос:

... - это устройство, хранящее некий уникальный параметр, на основе которого выдается корректный ответ на запрос системы об аутентификации.

Выберите один из 4 вариантов ответа:

1) Токен
2) Пароль
3) Биометрические параметры
4) Мастер-ключ

Задание # 34

Вопрос:

Выполнение пользователем, получившим доступ в систему, различных несанкционированных действий, называется атакой на ...

Запишите ответ:

_____

Задание # 35

Вопрос:

... - это программа, перехватывающая пакеты, поступающие к данной станции, в том числе и те, которое станция при нормальной работе должна проигнорировать.

Запишите ответ:

_____

Задание # 36

Вопрос:

... позволяют провести анализ и пошаговое выполнение программного обеспечения с тем, чтобы понять его внутреннюю логику и уязвимость или вызвать в его работе сбой с предсказуемым результатом, либо изменить ход работы программы в свою пользу.

Выберите один из 4 вариантов ответа:

1) Дизассемблеры
2) Программы повышения прав
3) Атаки на переполнение буфера
4) Программы подбора паролей

Задание # 37

Вопрос:

... когда поступающие в программу данные вызывают сбой либо проблемы с выдачей программой информации, которая должна быть скрыта, либо с выполнением ряда действий иначе, чем это было запланировано разработчиком программы.

Выберите один из 4 вариантов ответа:

1) Дизассемблеры

2) Программы повышения прав
3) Атаки на переполнение буфера
4) Программы подбора паролей

2.2 Объект оценивания «Умение»: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, применять основные правила и документы системы сертификации Российской Федерации, классифицировать основные угрозы безопасности информации.

Контрольные вопросы из практических занятий:

Практическая работа 1

Контрольные вопросы:

1) Что такое тайна?

2) Виды тайн?

Практическая работа 2

Контрольные вопросы:

1) На что подразделяются угрозы безопасности?

2) Опишите ситуацию, которая повлечет за собой угрозу и методы по ее устранению?

Практическая работа 3

Контрольные вопросы:

1) Что такое копирование?

2) Что необходимо сделать, чтобы данные сохранились?

Практическая работа 4

Контрольный вопрос:

1) Примеры защищенных программ?

2) Что должно входить в программу защиты?

Практическая работа 5

Контрольные вопросы:

1) Что такое криптография?

2) Виды шифрования?

Практическая работа 6

Контрольные вопросы:

1) Что такое антивирусная программа?

2) Примеры антивирусных программ?

Практическая работа 7

Контрольные вопросы:

1) Основные угрозы безопасности информации.

2) Виды угроз безопасности.

Практическая работа 8

Контрольные вопросы:

1) Разграничение доступа – это?

2) Что необходимо использовать для защиты?

Практическое занятие 9

Контрольные вопросы:

1) Что такое фаервол?

2) Для чего необходимо использовать эту программу?

Практическое занятие 10

Контрольные вопросы:

1) Резервное копирование – это?
2) Восстановление системы– это?

Практическое занятие 11

Контрольные вопросы:

1) Что такое шифрование данных?
2) Что можно зашифровать?
3) Какой самый эффективный выбор шифрования?

Практическое занятие 12

Контрольные вопросы:

1) Что такое риск?
2) Какие бывают риски?

Вопросы к экзамену по учебной дисциплине ОП.06 Основы информационной безопасности

1) Сущность и понятие информационной безопасности, характеристика ее составляющих
2) Место информационной безопасности в системе национальной безопасности страны
3) Понятие защиты информации. Основные предметные направления защиты информации
4) Предмет и объекты защиты информации в автоматизированных системах обработки данных
5) Элементы и объекты АСОД
6) Функции и задачи защиты информации
7) Методы и системы защиты информации
8) Криптология и основные этапы ее развития
9) Методы криптографического преобразования данных
10) Проблемы реализации методов криптографической защиты в АСОД
11) Особенности защиты информации в персональных ЭВМ
12) Защита ПК от несанкционированного доступа
13) Вредоносные закладки в ПК и борьба с ними
14) Компьютерный вирус, их классификация, признаки проявления вирусов
15) Методы защиты от вирусов. Виды антивирусов
16) Привести примеры антивирусных программ (не менее 3) и их основные функции
17) Сети ЭВМ – построение и использование
18) Цели, функции и задачи защиты информации в сетях ЭВМ
19) Архитектура механизмов защиты информации в сетях ЭВМ
20) Понятие технических средств защиты информации, их классы, типы систем защиты
21) Описание комплексного подхода к обеспечению безопасности на примере охраняемого объекта
22) Основы информационных систем как объекта защиты
23) Понятие операционных систем и их защита
24) Примеры базовых приложений информационных систем
25) Угрозы и задачи сетевой безопасности
26) Понятие глобальной сети Интернет. Возможные угрозы возникновения в сети
27) Структура и функциональность стека протоколов TCP/IP
28) Анализ угроз сетевой безопасности, проблемы безопасности IP-сетей

29) Задачи обеспечения информационной безопасности сетей
30) Технологии безопасности данных
31) Наиболее распространенные угрозы информационной безопасности для предприятия
32) Базовые технологии сетевой безопасности
33) Понятие законодательного уровня информационной безопасности
34) Задачи управления системой сетевой безопасности ее и архитектура
35) Стандарты и спецификации в области информационной безопасности
36) Понятие административного уровня информационной безопасности
37) Возможные риски для предприятия и их управление
38) Протоколы защиты на канальном и сеансовом уровнях
39) Основные понятия политики безопасности
40) Структура политики безопасности организации
41) Понятия информационного оружия и войны
42) Описание шифра Цезаря
43) Описание шифра Вижинера
44) Технологии аутентификации
45) Классификация преднамеренных угроз безопасности АСОД
46) Правовые основы защиты информации

3 Пакет экзаменатора

3.1 УСЛОВИЯ

Количество вариантов: 28

Время выполнения каждого задания: 30

Оборудование: ПК

Вариант 1
Вопрос №1 (теоретический).
Текст вопроса: Сущность и понятие информационной безопасности, характеристика ее составляющих
Вопрос №2 (теоретический).
Текст вопроса: Задачи обеспечения информационной безопасности сетей
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, зашифровать следующую фразу (ROT5):
Шифрование – это преобразование информации из открытой формы в закрытую.

Вариант 2
Вопрос №1 (теоретический).
Текст вопроса: Место информационной безопасности в системе национальной безопасности страны
Вопрос №2 (теоретический).
Текст вопроса: Технологии безопасности данных
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, зашифровать следующую фразу (ROT4):
Криптоанализ – это процесс расшифрования закрытой информации без знания ключа.

Вариант 3
Вопрос №1 (теоретический).
Текст вопроса: Понятие защиты информации. Основные предметные направления защиты информации
Вопрос №2 (теоретический).
Текст вопроса: Наиболее распространенные угрозы информационной безопасности для предприятия
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, зашифровать следующую фразу (ROT3):
Подстановка-способ шифрования, при котором производится замена каждой буквы открытого текста на символ шифрованного текста.

Вариант 4
Вопрос №1 (теоретический).
Текст вопроса: Предмет и объекты защиты информации в автоматизированных системах обработки данных
Вопрос №2 (теоретический).
Текст вопроса: Базовые технологии сетевой безопасности
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, зашифровать следующую фразу (ROT2):

Перестановки - способ шифрования, при котором буквы открытого текста не замещаются на другие, а меняется порядок их следования

Вариант 5
Вопрос №1 (теоретический).
Текст вопроса: Элементы и объекты АСОД
Вопрос №2 (теоретический).
Текст вопроса: Понятие законодательного уровня информационной безопасности
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, зашифровать следующую фразу (ROT3):
Гаммирование-способ шифрования, заключающийся в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа

Вариант 6
Вопрос №1 (теоретический).
Текст вопроса: Функции и задачи защиты информации
Вопрос №2 (теоретический).
Текст вопроса: Задачи управления системой сетевой безопасности ее и архитектура
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, зашифровать следующую фразу (ROT2):
Сжатие-расширение представляет собой замену часто встречающихся одинаковых строк данных или последовательностей одинаковых символов некоторыми заранее выбранными символами.

Вариант 7
Вопрос №1 (теоретический).
Текст вопроса: Методы и системы защиты информации
Вопрос №2 (теоретический).
Текст вопроса: Стандарты и спецификации в области информационной безопасности
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT9):
Ци аьпчт уищикит – щчычу цн щирнкит.

Вариант 8
Вопрос №1 (теоретический).
Текст вопроса: Криптология и основные этапы ее развития
Вопрос №2 (теоретический).
Текст вопроса: Понятие административного уровня информационной безопасности
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT16):
С тюбвое еюаюзю, п уюьп ыгжзф.

Вариант 9
Вопрос №1 (теоретический).
Текст вопроса: Методы криптографического преобразования данных
Вопрос №2 (теоретический).
Текст вопроса: Возможные риски для предприятия и их управление
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT14):
Щбеёт яцыцдн п юбшнг, етъ фбюнпщй п ытот.

Вариант 10
Вопрос №1 (теоретический).

Текст вопроса: Проблемы реализации методов криптографической защиты в АСОД
Вопрос №2 (теоретический).
Текст вопроса: Протоколы защиты на канальном и сеансовом уровнях
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT14):
П хсьюыпъ атщт хсьюыпич сбг.

Вариант 11
Вопрос №1 (теоретический).
Текст вопроса: Примеры базовых приложений информационных систем
Вопрос №2 (теоретический).
Текст вопроса: Базовые приложения информационных систем
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT15):
Атуъоъ туъэ — свънш аыуъэ.

Вариант 12
Вопрос №1 (теоретический).
Текст вопроса: Защита ПК от несанкционированного доступа
Вопрос №2 (теоретический).
Текст вопроса: Структура и функциональность стека протоколов TCP/IP
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT10):
Йщщоьть щътяшнть лш лъоци оне.

Вариант 13
Вопрос №1 (теоретический).
Текст вопроса: Вредоносные закладки в ПК и борьба с ними
Вопрос №2 (теоретический).
Текст вопроса: Основные понятия политики безопасности
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT8):
Имп ъшылз хм йгуцйрад р шгиты рп чшылз.

Вариант 14
Вопрос №1 (теоретический).
Текст вопроса: Компьютерный вирус, их классификация, признаки проявления вирусов
Вопрос №2 (теоретический).
Текст вопроса: Структура политики безопасности организации
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT13):
Нсюьшмяъзц юзэ нзомся яышичы о щзесшыючс.

Вариант 15
Вопрос №1 (теоретический).
Текст вопроса: Методы защиты от вирусов. Виды антивирусов
Вопрос №2 (теоретический).
Текст вопроса: Описание шифра Вижинера
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT20):
Фвяплваж ювдуфяс – фвяплвш гяухубыш.

Вариант 16
Вопрос №1 (теоретический).
Текст вопроса: Привести примеры антивирусных программ (не менее 3) и их основные функции
Вопрос №2 (теоретический).
Текст вопроса: Понятия информационного оружия и войны
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующую фразу (ROT22):
Чдщх ахвъгс здмюз.

Вариант 17
Вопрос №1 (теоретический).
Текст вопроса: Сети ЭВМ – построение и использование
Вопрос №2 (теоретический).
Текст вопроса: Описание шифра Цезаря
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующие фразы (ROT21):
Цёщбз ёцгъ цещбу.

Вариант 18
Вопрос №1 (теоретический).
Текст вопроса: Цели, функции и задачи защиты информации в сетях ЭВМ
Вопрос №2 (теоретический).
Текст вопроса: Технологии аутентификации
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующие фразы (ROT17):
Уягятм врющ ьхгяэ, р гхьхуд шщэяъ.

Вариант 19
Вопрос №1 (теоретический).
Текст вопроса: Архитектура механизмов защиты информации в сетях ЭВМ
Вопрос №2 (теоретический).
Текст вопроса: Классификация преднамеренных угроз безопасности АСОД
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующие фразы (ROT20):
Чшяж хдшат, гвёшиш куе.

Вариант 20
Вопрос №1 (теоретический).
Текст вопроса: Понятие технических средств защиты информации, их классы, типы систем защиты
Вопрос №2 (теоретический).
Текст вопроса: Правовые основы защиты информации
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующие фразы (ROT18):
Хвещнр бащяспдгр у тцхц.

Вариант 21
Вопрос №1 (теоретический).
Текст вопроса: Описание комплексного подхода к обеспечению безопасности на примере охраняемого объекта

Вопрос №2 (теоретический).
Текст вопроса: Угрозы и задачи сетевой безопасности
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующие фразы (ROT17):
Шр фхбхтмпэщ ьхвр юх тщфргм.

Вариант 22
Вопрос №1 (теоретический).
Текст вопроса: Основы информационных систем как объекта защиты
Вопрос №2 (теоретический).
Текст вопроса: Анализ угроз сетевой безопасности, проблемы безопасности IP-сетей
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующие фразы (ROT21):
Эь дщёвэ ёагцф вщ цпяэвщмр.

Вариант 23
Вопрос №1 (теоретический).
Текст вопроса: Понятие операционных систем и их защита
Вопрос №2 (теоретический).
Текст вопроса: Понятие глобальной сети Интернет. Возможные угрозы возникновения в сети
Вопрос №3 (практический).
Текст вопроса: Используя шифр Цезаря, дешифровать следующие фразы (ROT17):
Ырид эрвьяэ юх щваябгщим.

3.2 КРИТЕРИИ ОЦЕНКИ

№	Тип (вид) задания	Проверяемые знания и умения	Критерии оценки
1	Тесты	Знание основ информационной безопасности	«5» - 100 – 90% правильных ответов «4» - 89 - 80% правильных ответов «3» - 79 – 70% правильных ответов «2» - 69% и менее правильных ответов
2	Устные ответы	Знание основ информационной безопасности	Устные ответа на вопросы должны соответствовать материалам учебника Информатика для студентов учреждений среднего профессионального образования
3	Практические занятия на компьютере	Умения самостоятельно выполнять практические задания на компьютере, сформированность общих компетенций.	Выполнение практически всей работы (не менее 80%) – положительная оценка
4	Контрольная (самостоятельная) работа	Знание основ информационной безопасности в соответствии пройденной темой.	Контрольная (самостоятельная) работа состоит из 10 заданий «5» - 10 – 9 правильных заданий «4» - 8 - 7 правильных заданий «3» - 6 – 5 правильных заданий «2» - 5 и менее правильных заданий

5	Проверка конспектов	Умение ориентироваться в информационном пространстве, составлять конспект. Знание правил оформления работ.	Соответствие содержания работы, заявленной теме, правилам оформления работы.
6	Экзамен	Знание различных подходов к определению понятия «информация» Знание методов измерения количества информации, единиц измерения информации Знание назначения наиболее распространенных средств автоматизации информационной деятельности (текстовых редакторов, текстовых процессоров, графических редакторов, электронных таблиц, баз данных, компьютерных сетей); Знание алгоритмов как способа автоматизации деятельности Знание назначение и функции операционных систем	**Отметка «5»**: ответ полный и правильны на основании изученных теорий; материа изложен в определенной логическо последовательности, литературны языком. Ответ самостоятельный. **Отметка «4»**: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя. **Отметка «3»**: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный. **Отметка «2»**: при ответе обнаружено непонимание обучающимся основного содержания учебного материала или допущены существенные ошибки, которые он не смог исправить при наводящих вопросах преподавателя.

ЛИСТ ОЗНАКОМЛЕНИЯ ОБУЧАЮЩИХСЯ
с формами, процедурой текущего, рубежного контроля знаний, промежуточной аттестации по дисциплинам, профессиональным модулям, содержанием комплекта оценочных средств

Дисциплина ОП.06.Основы информационной безопасности
Группа 3-ОТ-1,3-ОТ-2,3-ОТ-3
Специальность 10.02.01 Организация и технология защиты информации
Преподаватель

№	ФИО обучающихся	Подпись	Примечание
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

Преподаватель _____ _____
Председатель УМО _____ О.А. Афиногенова