МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(ДГТУ)

Авиационный колледж

УТВЕРЖДАЮ
Директор АК ДГТУ
_____ А.И. Азарова
«____» _____ 2020 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

ОП.10 Информационная безопасность

основной профессиональной образовательной программы (ООП)

по специальности СПО

09.02.03 Программирование в компьютерных системах

базовой подготовки

Ростов-на-Дону
2020 г.

Содержание

1 Паспорт Фонда оценочных средств

1.1 Область применения Фонда оценочных средств

Фонд оценочных средств разработан в соответствии с требованиями ФГОС специальности СПО 09.02.03 «Программирование в компьютерных системах» и рабочей программой учебной дисциплины «Информационная безопасность».

Фонд оценочных средств предназначен для оценки результатов освоения учебной дисциплины «Информационная безопасность» среднего профессионального образования в пределах ОПОП СПО.

Учебная дисциплина, в соответствии с учебным планом, изучается на втором курсе в четвертом семестре и завершается формой промежуточной аттестацией – другие формы (устный опрос).

Фонд контрольно-оценочных средств включает в себя контрольно-измерительные материалы, позволяющие оценить знания, умения и уровень сформированных компетенций.

1.2 Перечень компетенций формируемых в процессе изучения дисциплины.

Рабочей программой дисциплины «Информационная безопасность» предусмотрено формирование следующих компетенций:

ОК-1: Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес

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-6: Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК-7: Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

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-1.2: Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля...

ПК-1.3. Выполнять отладку программных модулей с использованием специализированных программных средств.

ПК-1.5: Осуществлять оптимизацию программного кода модуля

ПК-2.4: Реализовывать методы и технологии защиты информации в базах данных.

2. Результаты освоения учебной дисциплины, подлежащие проверке

2.1 Показатели оценки результатов обучения

Основные показатели и критерии оценки результата сформированности компетенций и результатов обучения представлены в таблице 1.

Результаты освоения (объекты оценивания)	**Основные показатели оценки результата.**	**Критерии оценки результата**	**Тип задания;**	**Форма аттестации (в соответствии с учебным планом)**
ОК 1, ОК 2, ОК3	воспроизведение: базовых теоретических знаний значимости своей будущей профессии, цели и методы при решении профессиональных задач; особенностей профессиональной деятельности программиста; содержания и назначение важнейших правовых и законодательных актов программиста, место и роль профессии в структуре организации	рассуждать о социальной значимости своей будущей профессии; использовать принципы теоретического мышления; рационально планировать и организовывать деятельность своей будущей профессии; применять полученные знания в профессии, анализировать ситуации и использовать в практической деятельности нормативные документы; владеть: навыками определения социальной значимости профессии; принципами теоретического мышления в	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	Другие формы (устный опрос)

		профессиональной деятельности; анализировать и принимать самостоятельно решения, как в стандартных так и нестандартных ситуациях		
ОК 4, ОК 5	владение различными способами поиска информации, различными видами технологий, применяемых в профессиональной деятельности; применение способов работы с информационными технологиями; использование телекоммуникационных средств для обеспечения работы предприятия	уметь использовать найденную информацию в результативном выполнении профессиональных задач, для профессионального роста и личностного развития; осуществлять поиск информации в сети Интернет и различных электронных носителях с использованием средств ИТ для обработки и хранения информации; анализировать способы информационной безопасности.	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	
ОК6, ОК7	знание приемов организации работы в группе, ведения дискуссии; содержания личностной, социальной и предметной составляющих взаимодействия субъектов профессиональной деятельности; знание методов принятия решений и механизмы взаимопонимания в общении; применение факторов, влияющих на совместную профессиональную деятельность	применять методы делового общения в профессиональной деятельности; оценивать свою работу, работу других обучающихся; выявлять главные факторы, влияющие на успешную коммуникацию; проводить самоанализ профессиональной деятельности, следовать указаниям руководства и соблюдать установленные правила и процедуры; анализировать методы принятия решений в профессиональной деятельности; владеть методами объяснения подчиненным профессиональных	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	

		задач, согласно их компетенции;		
ОК8, ОК9	знание основных направлений профессиональной деятельности в сфере информационных технологий; определение взаимосвязи между самоорганизацией и саморегуляцией в практической области.; знание методов и методики направленных на улучшение производительности труда; осуществление взаимосвязи между использованием современных средств телекоммуникации и эффективностью работы предприятия.	сопоставлять профессиональную деятельность и современные информационные технологии; применять правовые нормативные документы при выполнении практических работ; формулировать выводы, оценивать соответствие выводов полученным результатам; стойкой мотивацией к профессиональной деятельности; уметь вычленять главные факторы, влияющие на успешность профессиональной деятельности; использовать основное программное обеспечение; применять способы работы с информационными технологиями; анализировать производственную ситуацию.	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	
ПК1.2	определение терминов, основных понятий спецификаций компонентов компьютерных систем и программных продуктов; методов и процедур разработки кода программного продукта на основе готовых спецификаций компонент на уровне модуля; определение главных факторов, влияющих на разрабатываемый программный код модуля на основе готовых спецификаций модуля с целью повышения его эффективности и	сопоставлять разработанный код программного модуля на основе спецификаций исходному техническому заданию; выявлять взаимосвязь между изменением спецификации модуля и кода программного модуля; разрабатывать план разработки кода программного модуля, направленного на структуризацию входных данных и времени его выполнения; владеть навыками	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	

	технологичности	изменения разработанной структуры программного кода модуля в зависимости от изменения спецификации; навыками разработки кода программного модуля на основе его спецификации.		
ПК1.3	знание терминов, основных понятий отладки программных модулей компьютерных систем и программных продуктов; методов и процедур отладки модулей программного продукта	сопоставлять работу отдельных конструкций языка программирования алгоритму работы разработанного код программного модуля во время отладки; выявлять взаимосвязь между изменением конструкций языка программирования разработанного кода модуля и процессом его отладки; навыками изменения конструкций языка программирования разработанного кода модуля в зависимости от хода его отладки.	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	
ПК1.5	определение методов оптимизации модулей программного продукта, умение воспроизводить термины, основные понятия оптимизации программного кода модулей компьютерных систем и программных продуктов; определение главных факторов процесса оптимизации программного кода модуля, влияющие на эффективность и технологичность, объемную и временную сложность модуля.	сопоставлять требования к эффективности программного кода временным и трудовым затратам, не приводящим к существенным ухудшениям его технологических свойств; выявлять взаимосвязь оптимизации программного кода модуля и программированием «с защитой от ошибок», способов экономии памяти и уменьшения времени выполнения.; владеть навыками использования инструментальных средств на этапе отладки программного продукта, навыками применения полученных знаний,	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	

		умений для оптимизации программного модуля на языке		
ПК2.4	описание технологии и методов защиты информации в базах данных; воспроизведение терминов, основных понятий защиты информации в базах данных; главных факторов процесса защиты информации базы данных в конкретной СУБД	сопоставлять уровень ценности информации с уровнем степени методов ее защиты; выявлять взаимосвязь между уровнем требований к защите информации в базе данных и применяемыми методами и технологиями по их защите; применять стандартные методы для защиты объектов базы данных; владеть практическим опытом применения основных операций по защите информации в базе данных в соответствии с правами доступа к объектам, владеть практическим опытом использования стандартных методов защиты объектов базы данных.	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	
З 1, З 2, З 3	изложение основ информационной безопасности и защиты информации; принципов криптографических преобразований; типовых программно-аппаратные средств и систем защиты информации от несанкционированного доступа	проводить анализ основ информационной безопасности и защиты информации; формулировать принципы криптографических преобразований; типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	
У 1	использование средств защиты информации и системы защиты информации от несанкционированного доступа	использовать средства защиты информации и системы защиты информации от несанкционированного доступа	устные опросы; письменные опросы; решение тестовых заданий, выполнение практических работ, подготовка кратких сообщений по темам	

2.2 Общая процедура и сроки проведения оценочных мероприятий.

Оценивание результатов обучения обучающихся по дисциплине «Информационная безопасность» осуществляется по регламенту текущего контроля и промежуточной аттестации.

Текущий контроль в семестре проводится с целью обеспечения своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающегося. Результаты текущего контроля подводятся по шкале балльно-рейтинговой системы, реализуемой в ИСОиП (филиале) ДГТУ.

Текущий контроль осуществляется два раза в семестр по календарному графику учебного процесса в рамках проведения контрольных точек.

Формы текущего контроля знаний:

- устный опрос;
- письменный опрос;
- тестирование;
- выполнение и защита практических работ.

Проработка конспекта лекций и учебной литературы осуществляется обучающимися в течение всего семестра, после изучения новой темы.

Защита практических работ производится в день их выполнения в соответствии с планом-графиком. Преподаватель проверяет правильность выполнения практической работы обучающимся, контролирует знание обучающегося пройденного материала с помощью контрольных вопросов или тестирования.

Оценка компетентности осуществляется следующим образом: по окончании выполнения задания обучающийся оформляют отчет, который затем выносится на защиту. В процессе защиты выявляется информационная компетентность в соответствии с заданием на практической работы, затем преподавателем дается комплексная оценка деятельности обучающегося.

Критерии оценивания:

Оценка 5 «отлично» обучающийся показывает глубокие осознанные знания по освещаемому вопросу, владение основными понятиями, терминологией; владеет конкретными знаниями, умениями по данной теме; ответ полный доказательный, четкий, грамотный.

Оценка 4 «хорошо» обучающийся показывает глубокое и полное усвоение содержания материала, умение правильно и доказательно излагать материал, допускает отдельные незначительные неточности в форме и стиле ответа.

Оценка 3 «удовлетворительно» обучающийся понимает основное содержание практической работы. Допускает отдельные ошибки, неточности в содержании и оформлении ответа; ответ недостаточно последователен, доказателен и грамотен.

Оценка 2 «неудовлетворительно» обучающийся имеет существенные пробелы в знаниях, допускает ошибки, неточности в содержании рассказываемого материала, не выделяет главного, существенного в ответе. Ответ поверхностный, бездоказательный, допускаются речевые ошибки.

Обучающимся, проявившим активность во время практических занятий, общий балл по текущему контролю может быть увеличен на 10-15%.

3. Комплект оценочных средств

3.1 Промежуточная аттестация

Учебным планом специальности 09.02.03 Программирование в компьютерных системах предусмотрена форма промежуточной аттестации по дисциплине «Информационная безопасность» - другие формы (устный опрос)

Итоговое занятие проводится за счет времени отведенного на изучение дисциплины. Проводится одновременно для всей учебной группы в форме устного опроса**.** Допускаются обучающиеся, сдавшие практические задания. Оценка может быть выставлена по рейтингу текущего контроля, если он не ниже 60.

Вопросы для промежуточного контроля:

1. Понятия «информационная безопасность» и «защита информации».
2. Основные положения системы защиты информации.
3. Условия удовлетворяющие СЗИ.
4. Основные требования систем защиты информации
5. Требования безопасности к информационным системам
6. Концептуальная модель информационной безопасности.
7. Угрозы конфиденциальной информации.
8. Стандарты информационной безопасности «Общие критерии»
9. Стандарты и спецификации в области информационной безопасности
10. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
11. Направления обеспечения информационной безопасности (правовая защита).
12. Страховая и лицензионная защита информации.
13. Направления обеспечения информационной безопасности (организационная защита).
14. Направления обеспечения информационной безопасности (инженерно-техническая защита).
15. Физические средства защиты информации.
16. Защита информации от утечки по техническим каналам.
17. Классификация угроз "информационной безопасности
18. Аппаратные средства защиты информации.
19. Профилактика компьютерных вирусов
20. Обнаружение неизвестного вируса
21. Архитектурная безопасность СВТ.
22. Технические средства несанкционированного доступа.
23. Программные средства защиты информации.
24. Основные направления использования программной защиты информации.
25. Защита информации от несанкционированного доступа.
26. Защита информации от копирования.

27. Защита информации от изменения и разрушения.
28. Криптографические средства защиты. Технологии шифрования.
29. Способы защиты информации.
30. Общая характеристика защитных действий.
31. Пресечение разглашения конфиденциальной информации.
32. Экранирование и анализ защиты
33. Технология виртуальных частных сетей
34. Противодействие несанкционированному доступу к источникам конфиденциальной информации.
35. Способы несанкционированного доступа.
36. Возможности типичных систем управления безопасностью.
37. Регистрация и аудит. Межсетевое экранирование
38. Характеристика "вирусоподобных" программ Антивирусные программы
39. Нормативно-законодательная база в области информационной безопасности

Критерии оценки:

Оценка 5 «отлично»	обучающийся показывает глубокие осознанные знания по освещаемому вопросу, владение основными понятиями, терминологией; владеет конкретными знаниями, умениями по данной дисциплине; ответ полный доказательный, четкий, грамотный, иллюстрирован практическим опытом профессиональной деятельности
Оценка 4 «хорошо»	обучающийся показывает глубокое и полное усвоение содержания материала, умение правильно и доказательно излагать программный материал, допускает отдельные незначительные неточности в форме и стиле ответа.
Оценка 3 «удовлетворительно»	обучающийся понимает основное содержание учебной программы, умеет показывать практическое применение полученных знаний. Вместе с тем допускает отдельные ошибки, неточности в содержании и оформлении ответа; ответ недостаточно последователен, доказателен и грамотен.
Оценка 2 «неудовлетворительно»	обучающийся имеет существенные пробелы в знаниях, допускает ошибки, неточности в содержании рассказываемого материала, не выделяет главного, существенного в ответе. Ответ поверхностный, бездоказательный, допускаются речевые ошибки.

3.2 Текущий контроль успеваемости

Тема: «Обеспечение информационной безопасности»
Форма проведения - тестирование.

1. Что такое "компьютерный вирус"?

А) это программы, активизация которых вызывает уничтожение программ и файлов;
Б) это совокупность программ, находящиеся на устройствах долговременной памяти;
В) это программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы;
Г) это программы, передающиеся по Всемирной паутине в процессе загрузки Web-страниц.

2. Какие файлы заражают макро-вирусы?

А) исполнительные;
Б) графические и звуковые;
В) файлы документов Word и элект. таблиц Excel;
Г) html документы.

3. Неопасные компьютерные вирусы могут привести

А) к сбоям и зависаниям при работе компьютера;
Б) к потере программ и данных;
В) к форматированию винчестера;
Г) к уменьшению свободной памяти компьютера.

4. Какой вид компьютерных вирусов внедряются и поражают исполнительный файлы с расширением *.exe, *.com?

А) файловые вирусы;
Б) загрузочные вирусы;
В) макро-вирусы;
Г) сетевые вирусы.

5. Основные типы компьютерных вирусов:

А) Аппаратные, программные, загрузочные
Б) Программные, загрузочные, макровирусы.
В) Файловые, сетевые, макровирусы, загрузочные.

6. На чем основано действие антивирусной программы?

А) На ожидании начала вирусной атаки.
Б) На сравнении программных кодов с известными вирусами.
В) На удалении зараженных файлов.

7. Какие программы относятся к антивирусным

А) AVP, DrWeb, Norton AntiVirus.
Б) MS-DOS, MS Word, AVP.
В) MS Word, MS Excel, Norton Commander.

8. Какие существуют вспомогательные средства защиты?

А) Аппаратные средства.
Б) Программные средства.
В) Аппаратные средства и антивирусные программы.

9. Вставь пропущенное слово, определив тип антивирусной программы

Антивирусные ... - это программы, перехватывающие «вирусноопасные» ситуации и сообщающие об этом пользователю.

10. Основные меры по защите информации от повреждения вирусами:

А) проверка дисков на вирус
Б) создавать архивные копии ценной информации
В) не пользоваться "пиратскими" сборниками программного обеспечения
Г) передавать файлы только по сети

Тема: «Антивирусная защита»
Форма проведения - тестирование.

1. Выберите правильный ответ из предложенных вариантов. Что такое компьютерный вирус?

1) Прикладная программа.
2) Системная программа.
3) Программы, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.
4) База данных.

2. Завершите предложение, выбрав из предложенных вариантов верный. *Основные типы компьютерных вирусов:*

1) Аппаратные, программные, загрузочные;
2) Файловые, загрузочные, макровирус, сетевые;
3) Файловые, программные, макровирусы.

3. Выберите правильный ответ из предложенных вариантов. Какие существуют основные средства защиты?

1) Резервное копирование наиболее ценных данных.
2) Аппаратные средства.
3) Программные средства.

4. Выберите правильный ответ из предложенных вариантов. Какие существуют вспомогательные средства защиты?

1) Аппаратные средства.
2) Программные средства.
3) Аппаратные средства и антивирусные программы.

5. Выберите правильный ответ из предложенных вариантов. На чем основано действие антивирусной программы?

1) На ожидании начала вирусной атаки.
2) На сравнение программных кодов с известными вирусами.
3) На удалении зараженных файлов.

6. Выберите правильный ответ из предложенных вариантов. Какие программы относятся к антивирусным?

1) AVP, DrWeb, Norton AntiVirus.
2) MS-DOS, MS Word, AVP.
3) MS Word, MS Excel, Norton Commander.

7. Выберите правильный ответ из предложенных вариантов. Определите тип антивирусной программы. DrWeb относится: (1б)

1) Полифаги.
2) Ревизоры.
3) Блокировщики.

8. Вставь пропущенное слово, определив тип антивирусной программы:

Антивирусная программа ADinf относится к…….

9. Вставь пропущенное слово, определив тип антивирусной программы:

Антивирусные … - это программы, перехватывающие «вирусноопасные» ситуации и сообщающие об этом пользователю.

10. По предложенному описанию определите тип вируса.

Заражают файлы документов Word и Excel. Являются фактически макрокомандами, которые встраиваются в документ.

Задача. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Таблица 3. Варианты заданий

Вариант	P	V	T
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней

4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя

Критерии оценки: (за правильный ответ дается 1 балл)

от 0 % до 40 % включительно – оценка «**неудовлетворительно**»;
от 41% до 60% включительно – оценка «**удовлетворительно**»;
от 61 % до 80 % включительно – оценка «**хорошо**»;
от 81 % до 100 % включительно – оценка «**отлично**»

Контрольная точка №1

Форма проведения - тестирование.

Тема: Основные понятия защиты информации и информационной безопасности. Сетевые модели передачи данных.

1 ВАРИАНТ

Добавить недостающие фразы:

1. деятельность по предотвращению утечки защищаемой информации, несанкционированных и не преднамеренных воздействий на защищаемую информацию. ЭТО — _____

2. ***Составляющие ИБ:***

a) _____
b) _____.
c) _____-

3 Целостность – состояние информации, при котором _____

4 Статическая целостность информации предполагает _____определяемого автором или источником информации.

5 Конфиденциальность – состояние информации, при котором _____

6 Угроза _____

7 Авария – неумышленное происшествие с деструктивным _____.

8 по характеру воздействия угрозы бывают:

a) _____
b) _____

Выберете правильные ответы*:*

9 ***Причинами случайных воздействий могут быть***

a) аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
b) отказы и сбои аппаратуры;
c) любопытство;
d) конкурентная борьба;

10 по расположению источника угроз, бывают:

a) _____-

b) _____-.

11 ***Добавить не достающие признаки***: **Угрозы информационной безопасности** классифицируются по нескольким признакам:

a) по составляющим информационной безопасности;
b) по компонентам информационных систем;
c) по _____-;
d) по _____.

12 Назовите два принципа организации обмена данными:

a) _____
b) _____

13Модель TCP/IP иерархическая и включает четыре уровня:

a) _____
b) _____
c) _____-
d) _____

Выбрать правильный ответ:

14 Какой уровень определяет способ общения пользовательских приложений:

a) Прикладной уровень
b) Транспортный уровень
c) сетевой уровень
d) канальный уровень

15 На каком уровне определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними:

a) на сетевом уровне
b) прикладном
c) транспортном
d) канальном

Контрольная точка №1

Форма проведения - тестирование.

Тема: Основные понятия защиты информации и информационной безопасности. Сетевые модели передачи данных.

2 ВАРИАНТ

Добавить не достающие признаки

1 ***Защита информации (ЗИ)*** *– комплекс мероприятий по обеспечению:*

a) конфиденциальности,
b) целостности,
c) доступности,
d) _____
e) _____-.

2 защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера___*ЭТО–* _____

3 TCP/IP – это _____-

4 Динамическая целостность информации включает вопросы

_____

5 Ошибка это _____

6 Уязвимость это _____

Выберете правильные ответы:

7 ***Преднамеренные воздействия*** **вызваны**,

a) недовольством служащего служебным положением;
b) уязвленным самолюбием

c) ошибки в программном обеспечении;
d) ошибки в работе персонала;
e) любопытство

8 Каналы НСД классифицируются по компонентам автоматизированных информационных систем:

a) Через _____-
b) Через _____:
c) Через _____--:

9 Атака – попытка практической реализации угрозы (успешная или нет).

10 *Добавить не достающие протоколы* TCP/IP –

a) межсетевой протокол управления сообщениями (ICMP),
b) протокол разрешения адресов (ARP),
c) _____-- (UDP)
d) _____-- (TCP).

11 Какой уровень_позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами

a) Прикладной уровень
b) Транспортный уровень
c) сетевой уровень
d) канальный уровень

12 Что происходит при передаче датаграммы - _____

13 Протокол сетевого обмена информацией – это перечень _____

14 На каком уровне определяется адресация физических интерфейсов сетевых устройств:

a) на сетевом уровне
b) прикладном
c) транспортном
d) канальном

15 Злоумышленник – это субъект, _____

Критерии оценки:

(за правильный ответ дается 1 балл)

от 0 % до 40 % включительно – оценка «**неудовлетворительно**»;

от 41% до 60% включительно – оценка «**удовлетворительно**»;

от 61 % до 80 % включительно – оценка «**хорошо**»;

от 81 % до 100 % включительно – оценка «**отлично**»

Контрольная точка №2
Форма проведения - тестирование.

1. Кто является ответственным за определение уровня классификации информации?
A. Руководитель среднего звена
B. Высшее руководство
C. Владелец
D. Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

A. Сотрудники
B. Хакеры
C. Атакующие
D. Контрагенты (лица, работающие по договору)

3. **Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?**
A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства ее использования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
C. Улучшить контроль за безопасностью этой информации
D. Снизить уровень классификации этой информации

4. что самое главное должно продумать руководство при классификации данных?
A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
B. Необходимый уровень доступности, целостности и конфиденциальности
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
A. Владельцы данных
B. Пользователи
C. Администраторы
D. Руководство

6. Что такое протокол обмена данными?
A. Правила использования аппаратного и программного обеспечения в компании
B. Пошаговая инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные
C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
D. Обязательные действия

7. Когда целесообразно не предпринимать никаких действий в отношении выявления рисков?
A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
B. Когда риски не могут быть приняты во внимание по политическим соображениям
C. Когда необходимые защитные меры слишком сложны
D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

8.Что такое политическая безопасность?
A. Пошаговая инструкция по выполнению задач безопасности
B. Общие руководящие требования по достижению определенного уровня безопасности
C. Набор законов правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию
D. Детализированные документы по обработке инцидентов безопасности

9.Что такое уровень гарантийности?
A. Пошаговая инструкция по выполнению задач безопасности
B. Общие руководящие требования по достижению определенного уровня безопасности
C. Мера доверия, которая может быть оказана архитектуре и реализации ИС
D. Доверие безопасности

10. **Какая из приведенных техник является самой важной при выборе конкретных защитных мер?**
A. Анализ рисков
B. Анализ затрат\выгоды

C. Результаты ALE
D. Выявление уязвимости и угроз являющейся причиной риска

11. какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность
B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные - о конфиденциальности
C. Военным требуется большой уровень безопасности, т.к их риски существенно выше
D. Коммерческая компания обычно больше заботиться о доступности и конфиденциальности своих данных, а военные – о целостности

12. Степень доверия оценивается по:

A. политике безопасности
B. Уровню гарантийности
C. По конфиденциальности
D. по доступности

13. **Согласно «Оранжевой книге» политика безопасности должна включать:**

A. произвольное управление доступом
B. Метки безопасности
C. Изолированность
D. Полнота

14. Оранжевая книга была опубликована впервые:

A. в августе 1983
B. в июле 1983
C. в августе 1984
D. в августе 1982

15. Процедурный уровень ориентирован на :

A. технические средства
B. на нарушение режима безопасности
C. людей

16.Что является задачей административного уровня?

A. разработка и реализация практических мероприятий по созданию системы ИБ, учитывающие особенности защищаемых ИС
B. реагировать на нарушение режима безопасности
C. управление персоналом и поддержание работоспособности ИС
D. планирование восстановительных работ

17. **Сколько существует общих принципов при отборе персонала?**

A. три
B. четыре
C. два

17.**Вставьте пропущенное слово**

Принцип разделения _____предписывает распределять роли и ответственность так, чтобы один человек не мог нарушить критически важный для организации процесс.

18. **Вставьте пропущенное слово**

Принцип минимизации _____ предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей.

19. **Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:**

A.гаммирование
B. подстановки
C. кодирование

D. Перестановки

20. **Проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение подлинности это** – _____

21. **Присвоение субъекта и объекта доступа личного идентификатора и сравнения его с заданием это** –_____

Критерии оценки: (за правильный ответ дается 1 балл)

от 0 % до 40 % включительно – оценка «**неудовлетворительно**»;
от 41% до 60% включительно – оценка «**удовлетворительно**»;
от 61 % до 80 % включительно – оценка «**хорошо**»;
от 81 % до 100 % включительно – оценка «**отлично**»