Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования

«Академия маркетинга и социально-информационных технологий – ИМСИТ»

(г. Краснодар)

Академический колледж

УТВЕРЖДАЮ
Проректор по учебной работе,
доцент Н.И. Севрюгина
08 апреля 2024 г.

ОП. 01 Основы информационной безопасности

Рабочая программа учебной дисциплины

Для студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

технический профиль

квалификация выпускника - Техник по защите информации

Краснодар, 2024

Рассмотрено
на заседании предметно цикловой комиссии
Протокол № 9 от 05 апреля 2024 г.
Председатель ПЦК Куценко А.А.
Зав отделением Борей Т.В.

Принято
педагогическим советом
Академического колледжа
Протокол № 9
от 05 апреля 2024 г.

Рабочая программа разработана на основе основной профессиональной образовательной программы среднего профессионального образования программы подготовки специалистов среднего звена, специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, Федерального закона Российской Федерации от 29 декабря 2012 г. № 273- ФЗ Об образовании в Российской Федерации (редакция от 25.12.2018 г.) и требований ФГОС среднего профессионального образования (приказ от 09.12.2016г. № 1553 Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Зарегистрировано в Минюсте России 26 декабря 2016 г. N 44938) технического профиля профессионального образования.

Содержание программы реализуется в процессе освоения студентами основной профессиональной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем технического профиля (на базе основного общего образования) в соответствии с требованиями ФГОС СПО на 2 курсе (ах) в 3 семестре (ах).

Рецензенты:

Ким Т. И./ Заместитель директора по учебно-методической работе ЧУ ПОО КТУИС г. Краснодар

Директор ООО «НТП» г. Краснодар, Поташкова Н.И.

Генеральный директор АО «Опытное конструкторское бюро «Икар» г. Краснодар,

А.Н. Качковский

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре примерной основной профессиональной образовательной программы:

Дисциплина *ОП.01 Основы информационной безопасности* входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

1.2. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК	Умения	Знания
ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4	– классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации;	– сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности;

2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Обязательная учебная нагрузка	66
в том числе:	
теоретическое обучение	32
практические занятия (если предусмотрено)	32
Самостоятельная работа[29]	2
Промежуточная аттестация[30]	

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности		**33**	
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	**6**	ОК 3, ОК 6, ОК 9, ПК.2.4
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.		
	Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.		
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	**14**	ОК 3, ОК 6, ОК 9, ПК 2.4
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.	10	
	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.		
	Цели и задачи защиты информации. Основные понятия в области защиты информации.		
	Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.		
	Практические занятия	**4**	
	Определение объектов защиты на типовом объекте информатизации.		
	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.		
Тема 1.3. Угрозы	**Содержание учебного материала**	**13**	ОК 3, ОК 6,

безопасности защищаемой информации.	Понятие угрозы безопасности информации	**7**	ОК 9, ПК.2.4
	Системная классификация угроз безопасности информации.		
	Каналы и методы несанкционированного доступа к информации		
	Уязвимости. Методы оценки уязвимости информации		
	Практическое занятие	**6**	
	Определение угроз объекта информатизации и их классификация		
Раздел 2. Методология защиты информации		**33**	
Тема 2.1. Методологические подходы к защите информации	**Содержание учебного материала**	**10**	ОК 3, ОК 6, ОК 9, ПК 2.4
	Анализ существующих методик определения требований к защите информации.	10	
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.		
	Виды мер и основные принципы защиты информации.		
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание учебного материала**	**11**	ОК 3, ОК 6, ОК 9, ОК 10
	Организационная структура системы защиты информации	5	
	Законодательные акты в области защиты информации.		
	Российские и международные стандарты, определяющие требования к защите информации.		
	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации		
	Практическое занятие	**6**	
	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности		
Тема 2.3. Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала**	**12**	ОК 3, ОК 6, ОК 9, ОК 10
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	6	
	Программные и программно-аппаратные средства защиты информации		
	Инженерная защита и техническая охрана объектов информатизации		
	Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.		

	Практическое занятие	**6**	
	Выбор мер защиты информации для автоматизированного рабочего места		
Промежуточная аттестация по учебной дисциплине			
Всего		***66***	

2.4 Оценочные средства и контрольные вопросы

1. Что такое информационная безопасность и почему она важна для организаций?
2. Какие угрозы могут возникать в области информационной безопасности?
3. Какие основные принципы информационной безопасности существуют?
4. Что такое конфиденциальность информации и как ее обеспечить?
5. Какие методы шифрования используются для защиты данных?
6. Каким образом можно защитить себя от кибератак и вирусов?
7. Что такое аутентификация и какие методы аутентификации существуют?
8. Какие меры безопасности следует принять при использовании общественных Wi-Fi сетей?
9. Что такое уязвимость в системе информационной безопасности и как их можно обнаружить?
10. Каким образом можно защитить свои пароли и учетные данные?
11. Что такое социальная инженерия и как ей противостоять?
12. Какие меры безопасности следует принять при работе с электронной почтой?
13. Каким образом можно обезопасить свои данные при использовании облачных сервисов?
14. Что такое бэкап данных и почему он важен для информационной безопасности?
15. Какие риски существуют при использовании нелицензионного программного обеспечения?
16. Что такое двухфакторная аутентификация и как она повышает безопасность?
17. Каким образом можно защитить свои устройства от физического доступа несанкционированных лиц?
18. Что такое защита от вредоносного программного обеспечения и какие существуют типы вредоносных программ?
19. Какие меры безопасности следует принять при использовании общественных компьютеров или интернет-кафе?
20. Что такое политика информационной безопасности и почему она важна для организации?
21. Каким образом можно защитить свою личную информацию в социальных сетях?
22. Что такое защищенное соединение по протоколу HTTPS и как оно обеспечивает безопасность данных?
23. Каким образом можно обеспечить безопасность при онлайн-платежах и интернет-банкинге?
24. Что такое фишинг и как его можно распознать?
25. Каким образом можно защитить сеть Wi-Fi дома от несанкционированного доступа?
26. Что такое многофакторная аутентификация и как она повышает безопасность доступа к данным?
27. Какие рекомендации можно дать по созданию надежных паролей?
28. Что такое DDoS-атака и как ей противостоять?
29. Каким образом можно обеспечить безопасность мобильных устройств и приложений?
30. Что такое информационная безопасность на рабочем месте и какие правила следует соблюдать?

2.5 Фонд оценочных средств

1. Информация это -
1 сведения, поступающие от СМИ
2 только документированные сведения о лицах, предметах, фактах, событиях
3 сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
4 только сведения, содержащиеся в электронных базах данных

2. Информация
1 не исчезает при потреблении
2 становится доступной, если она содержится на материальном носителе
3 подвергается только "моральному износу"
4 характеризуется всеми перечисленными свойствами

3. Какими официальными документами информация отнесена к объектам гражданских прав?

1 УК РФ
2 Законом РФ "О праве на информацию"
3 ГК и законом РФ "Об информации, информатизации и защите информации"
4 Конституцией РФ

4. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
1 достоверной
2 конфиденциальной
3 документированной
4 коммерческой тайной

5. Формы защиты интеллектуальной собственности -
1 авторское, патентное право и коммерческая тайна
2 интеллектуальное право и смежные права
3 коммерческая и государственная тайна
4 гражданское и административное право

6. По принадлежности информационные ресурсы подразделяются на
1 государственные, коммерческие и личные
2 государственные, не государственные и информацию о гражданах
3 информацию юридических и физических лиц
4 официальные, гражданские и коммерческие

7. К негосударственным относятся информационные ресурсы
1 созданные, приобретенные за счет негосударственных учреждений и организаций
2 созданные, приобретенные за счет негосударственных предприятий и физических лиц
3 полученные в результате дарения юридическими или физическими лицами
4 указанные в п.1-3

8. По доступности информация классифицируется на
1 открытую информацию и государственную тайну
2 конфиденциальную информацию и информацию свободного доступа
3 информацию с ограниченным доступом и общедоступную информацию
4 виды информации, указанные в остальных пунктах

9. К конфиденциальной информации относятся документы, содержащие
1 государственную тайну
2 законодательные акты
3 "ноу-хау"
4 сведения о золотом запасе страны

10. Запрещено относить к информации ограниченного доступа
1 информацию о чрезвычайных ситуациях
2 информацию о деятельности органов государственной власти
3 документы открытых архивов и библиотек
4 все, перечисленное в остальных пунктах

11. Какие методы обеспечения информационной безопасности Российской Федерации направлены на создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи?
1 правовые
2 организационно-технические

3 экономические
4 стратегические

12. Что использует системы защиты информации Secret Disk для хранения паролей?
1 накопители на магнитных дисках
2 оперативную память компьютера
3 электронные ключи
4 бумажные носители

13. С какой целью используется теория информации при рассмотрении каналов передачи информационных потоков?
1 для повышения эффективности работы каналов связи
2 для анализа качества передаваемой информации
3 для вычисления количества информации в потоке и пропускной способности канала
4 для шифровки передаваемых сообщений

14. Какие преобразования шифра выполняются при операции рассеивания?
1 сжатие шифра
2 передача текста небольшими частями
3 наложение ложных сообщений
4 изменение любого знака открытого текста или ключа

15. Сколько типов архитектуры используется при создании системы сертификации в инфраструктуре с открытыми ключами?
1 один
2 два
3 три
4 четыре

16. Какой уровень контроля достаточен для ПО, используемого при защите информации с грифом «ОВ»?
1 первый
2 второй
3 третий
4 четвертый

17. С какой целью выполняется шифрование кода программ?
1 для противодействия дизассемблированию
2 для ускорения работы программ
3 в целях повышения надежности программного обеспечения
4 для упрощения работы пользователей

18. Какая система обеспечивает защиту информации?
1 система разграничения доступа субъектов к объектам
2 система кодирования информации
3 система управления потоками данных
4 система идентификации

19. Сколько существует классов, на которые подразделяются носители информации на предприятии?
1 два
2 три
3 пять

20. В чем заключается сущность приема "Троянский конь"?

1 это тайное введение в чужую программу команд, которые позволяют ей осуществлять новые, не планировавшиеся владельцем функции, но одновременно сохранять и прежнюю работоспособность
2 это тайное введение в чужую программу команд, которые позволяют ей осуществлять новые, не планировавшиеся владельцем функции
3 это тайное проникновение в чужую программу

21. RAID-массив это
1 набор жестких дисков, подключенных особым образом
2 антивирусная программа
3 вид хакерской утилиты
4 база защищенных данных

22. Вирус внедряется в исполняемые файлы и при их запуске активируется. Это…
1 загрузочный вирус
2 макровирус
3 файловый вирус
4 сетевой червь

23. В каких основных форматах существует симметричный алгоритм?
1 блока и строки
2 потока и блока
3 потока и данных
4 данных и блока

24. Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:
1 шифр функциональных преобразований
2 шифр замен
3 шифр перестановок

25. Возможно ли, вычислить закрытый ключ ассиметричного алгоритма, зная открытый?
1 нет
2 да
3 в редких случаях

26. Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им массива открытых данных размера n используется в анализе:
1 на основе произвольно выбранного шифротекста
2 на основе произвольно выбранного открытого текста
3 правильного ответа нет

27. Отметьте составные части современного антивируса
1 модем
2 принтер
3 сканер
4 межсетевой экран
5 монитор

28. К вредоносным программам относятся:
1 потенциально опасные программы
2 вирусы, черви, трояны
3 шпионские и рекламные программы
4 вирусы, программы-шутки, антивирусное программное обеспечение

5 межсетевой экран, брандмауэр

29. К биометрической системе защиты относятся:
1 защита паролем
2 физическая защита данных
3 антивирусная защита
4 идентификация по радужной оболочке глаз
5 идентификация по отпечаткам пальцев

30. Компьютерные вирусы – это:
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

31. К конфиденциальной информации не относится
1 коммерческая тайна
2 персональные данные о гражданах
3 государственная тайна
4 "ноу-хау"

32. Вопросы информационного обмена регулируются (...) правом
1 гражданским
2 информационным
3 конституционным
4 уголовным

33. Согласно ст.138 ГК РФ интеллектуальная собственность это
1 информация, полученная в результате интеллектуальной деятельности индивида
2 литературные, художественные и научные произведения
3 изобретения, открытия, промышленные образцы и товарные знаки
4 исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

34. Интеллектуальная собственность включает права, относящиеся к
1 литературным, художественным и научным произведениям, изобретениям и открытиям
2 исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
3 промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям
4 всему, указанному в остальных пунктах

35. Конфиденциальная информация это
1 сведения, составляющие государственную тайну
2 сведения о состоянии здоровья высших должностных лиц
3 документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
4 данные о состоянии преступности в стране

36. Какая информация подлежит защите?
1 информация, циркулирующая в системах и сетях связи
2 зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать

3 только информация, составляющая государственные информационные ресурсы
4 любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

37. Система защиты государственных секретов определяется Законом
1 "Об информации, информатизации и защите информации"
2 "Об органах ФСБ"
3 "О государственной тайне"
4 "О безопасности"

38. Государственные информационные ресурсы не могут принадлежать
1 физическим лицам
2 коммерческим предприятиям
3 негосударственным учреждениям
4 всем перечисленным субъектам

39. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает
1 Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"
2 ГК РФ
3 Закон "Об информации, информатизации и защите информации"
4 Конституция

40. Классификация и виды информационных ресурсов определены
1 Законом "Об информации, информатизации и защите информации"
2 Гражданским кодексом
3 Конституцией
4 всеми документами, перечисленными в остальных пунктах

41. Какие действия квалифицируются как компьютерное пиратство?
1 незаконное тиражирование лазерных дисков
2 распространение незаконно полученной информации по компьютерным сетям
3 попытка получить санкционированный доступ к компьютерной системе или вычислительной сети
4 попытка получить несанкционированный доступ к компьютерной системе или вычислительной сети

42. Какую задачу решает сертификация средств защиты информации?
1 обеспечения требуемого качества защиты информации
2 повышения квалификации разработчиков средств защиты информации
3 создания надежных средств защиты информации
4 защиты отечественных производителей средств защиты информации

43. Какие задачи решает система антивирусной защиты?
1 предотвращения проникновения вирусов к персональным ресурсам
2 повышения надежности работы программного обеспечения
3 предотвращения поломок технических средств
4 повышения эффективности работы программных средств

44. Что служит мерой опасности незаконного канала передачи информации?
1 пропускная способность незаконного канала
2 количество информации, передаваемой по незаконному каналу
3 время существования незаконного канала
4 число лиц, имеющих доступ к незаконному каналу

45. Какие шифры называются послойными?
1 состоящие из слоев шифрования
2 состоящие из цепочки циклов шифрования
3 выполняющие единственное преобразование информационного сообщения
4 обеспечивающие высокоэффективное шифрование

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Кабинет информационной безопасности

20 столов, 20 стульев, рабочее место преподавателя, 20 шт. персональных компьютеров с выходом в интернет 20 мониторов, 20 комплектов клавиатура+мышь, 1 беспроводная точка доступа TP-Link TL-WA801ND, соответствующее программное обеспечение

Лаборатория «Информационных технологий, программирования и баз данных»

20 столов, 20 стульев, рабочее место преподавателя, 20 шт. персональных компьютеров с выходом в интернет, 20 мониторов, 20 комплектов клавиатура+мышь, 1 беспроводная точка доступа TP-Link TL-WA801ND, соответствующее программное обеспечение.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Бондарев В. В. Введение в информационную безопасность автоматизированных систем. М.: МГТУ им. Н. Э. Баумана. 2024. 252 с.

3.2.2. Дополнительные печатные источники:

1. Барков А.В., Киселев А.С. Влияние цифровизации на правовое обеспечение информационной безопасности государства и бизнеса в условиях современных геополитических вызовов // Безопасность бизнеса. 2022. N 3. С. 3 — 7.
2. Галыгина Л. В., Галыгина И. В. Социальные аспекты информационной безопасности. Лабораторный практикум. М.: Лань. 2021. 64 с.
3. Баланов А. Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. М.: Инфра-Инженерия. 2024. 156 с.
4. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 12.12.2023) "Об информации, информационных технологиях и о защите информации" // "Собрание законодательства РФ", 31.07.2006, N 31 (1 ч.), ст. 3448.
5. Гродзенский Я. С. Информационная безопасность. Учебное пособие. М.: РГ-Пресс. 2024. 144 с.
6. Дубень А.К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению // Международное право и международные организации. 2022. N 1. С. 24 — 30.
7. Зенков А. В. Информационная безопасность и защита информации. М.: Юрайт. 2023. 108 с.
8. Куприянов А. И., Мельников В. П. Информационная безопасность. Учебник. М.: КноРус. 2022. 268 с.
9. Родичев Ю. А. Информационная безопасность. Национальные стандарты Российской Федерации. СПб.: Питер. 2023. 384 с.
10. Прохорова О. В. Информационная безопасность и защита информации. М.: Лань. 2024. 124 с.

3.2.3 Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.3. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: – сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности.	Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование

Умения: – классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации;	Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности	Экспертное наблюдение в процессе практических занятий