Министерство образования, науки и молодежной политики
Краснодарского края
Государственное бюджетное профессиональное образовательное учреждение
Краснодарского края «Пашковский сельскохозяйственный колледж»

УТВЕРЖДАЮ
Зам директора по УМР
_____ Е.П. Ольховская
«28» 09 2022 г

Комплект контрольно-оценочных средств
для проведения текущей промежуточной аттестации студентов в рамках
основной профессиональной образовательной программы
по учебной дисциплине
ОП.01 Основы информационной безопасности

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Краснодар, 2022

Комплект контрольно-оценочных средств для проведения аттестации студентов по учебной дисциплине ОП.01 Основы информационной безопасности разработан на основании рабочей программы образовательной учебной дисциплины, которая входит в структуру основной образовательной программы и предназначена для ее реализации в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (приказ Минобрнауки России от 09.12.2016.г. №1553, зарегистрировано в Минюсте России 26.12.2016 г., № 44938 (ред. 17.12.2020 г.))

Организация разработчик: ГБПОУ КК ПСХК

Разработчик:

Н.Я. Пушкарева	Преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, высшая квалификационная категория, математик, преподаватель информатики и ИКТ

Рассмотрен на заседании методического объединения
Информационных технологий
Протокол № 1 от «28» сент 2022 г.
_____/Пушкарева Н.Я/

СОДЕРЖАНИЕ

1. Паспорт комплекта контрольно-оценочных средств.

В результате освоения образовательной учебной дисциплины ЕН.02 Информатика обучающийся должен обладать предусмотренными ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденной директором колледжа, общими компетенциями, знаниями и умениями:

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;

Формой промежуточной аттестации по общеобразовательной учебной дисциплине является дифференцированный зачет.

2. Результаты освоения образовательной учебной дисциплины, подлежащие проверке

2.1. В результате аттестации по образовательной учебной дисциплине осуществляется комплексная проверка освоенных знаний, умений:

Результаты обучения: освоенные знания, умения	Показатели оценки результата	Форма контроля и оценивания
Общие компетенции (ОК)		
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Знать: возможные траектории профессионального развития и самообразования Уметь: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование. Устные опросы. Проверка конспектов, рефератов,

	траектории профессионального и личностного развития Владеть: навыками определения актуальности нормативно-правовой документации в профессиональной деятельности; выстраивания траектории профессионального и личностного развития	творческих работ, презентаций, выполнения домашних работ, выполнения самостоятельных работ.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Знать: сущность гражданско-патриотической позиции, общечеловеческие ценности, правила поведения в ходе выполнения профессиональной деятельности Уметь: описывать значимость своей профессии, презентовать структуру профессиональной деятельности по специальности. Владеть: навыками представления структуры профессиональной деятельности по специальности	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование. Устные опросы. Проверка конспектов, рефератов, творческих работ, презентаций, выполнения домашних работ, выполнения самостоятельных работ.
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности. Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение. Владеть: навыками применения средств информационных технологий для решения профессиональных задач.	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование. Устные опросы. Проверка конспектов, рефератов, творческих работ, презентаций, выполнения домашних работ, выполнения самостоятельных работ.
ОК 10. Пользоваться профессиональной документацией на	Знать: правила построения простых и сложных	Экспертная оценка результатов деятельности обучающегося при

государственном и иностранном языке.	предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения. Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые). Владеть: навыками понимания общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые), на базовые профессиональные темы; участия в диалогах на знакомые общие и профессиональные темы; построения простых высказываний о себе и о своей профессиональной деятельности; обоснования и объяснения своих действий (текущих и планируемых).	выполнении и защите результатов практических занятий. Тестирование. Устные опросы. Проверка конспектов, рефератов, творческих работ, презентаций, выполнения домашних работ, выполнения самостоятельных работ.
Профессиональные компетенции (ПК)		

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации. Уметь: применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись владеть: навыками решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование. Устные опросы. Проверка конспектов, рефератов, творческих работ, презентаций, выполнения домашних работ, выполнения самостоятельных работ.

3. Оценка освоения учебной дисциплины:

3.1. Формы и методы оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС СПО ППССЗ, приказ Минобрнауки России от 09.12.2016.г. №1553, зарегистрировано в Минюсте России 26.121.2016 г., № 44938 (ред. 17.12.2020 г.) и профессиональным стандартом по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем по дисциплине ОП.01 Основы информационной безопасности, направленные на формирование общих и профессиональных компетенций.

Типы (виды) заданий для текущего контроля

№	Тип (вид) задания	Проверяемые знания и умения	Критерии оценки
1	Тесты	Знание основ информационной безопасности в соответствии с темой занятия	«5» - 100 – 90% правильных ответов «4» - 89 - 75% правильных ответов «3» - 74 – 55% правильных ответов «2» - 54% и менее правильных ответов
2	Устные ответы	Знание основ информационной безопасности в соответствии с темой занятия	Устные ответа на вопросы должны соответствовать учебному материалу, изученному на уроке
3	Практическая работа на компьютере	Умения самостоятельно выполнять практические задания на компьютере, сформированность общих компетенций.	Выполнение практически всей работы (не менее 80%) – положительная оценка
4	Текущий контроль в форме защиты практических занятий	Знание основ информационной безопасности в соответствии с темой занятия и умение применять их при практической работе на компьютере	Устные ответы и демонстрация практических умений работы на компьютере в соответствии с темой занятия: «5» - 100 – 90% правильных ответов и заданий «4» - 89 - 80% правильных ответов и заданий «3» - 79 – 70% правильных ответов и заданий «2» - 69% и менее правильных ответов и заданий
5	Проверка конспектов (рефератов, докладов, сообщений, понятийных	Умение ориентироваться в информационном пространстве, составлять конспект. Знание правил оформления рефератов, творческих работ.	Соответствие содержания работы, заявленной теме, правилам оформления работы.

	словарей, таблиц соответствия)		
6	Дифференцированный зачет	Знание основ информационной безопасности	Устные ответы и демонстрация практических умений работы на компьютере в соответствии с темой занятия: «5» - 100 – 90% правильных ответов и заданий «4» - 89 - 80% правильных ответов и заданий «3» - 79 – 70% правильных ответов и заданий «2» - 69% и менее правильных ответов и заданий

Промежуточный контроль по результатам освоения обучающимися учебной дисциплины проводится в форме дифференцированного зачёта (зачёт с оценкой).

3.2. Типовые задания для оценки освоения образовательной учебной дисциплины

Раздел 1. Теоретические основы информационной безопасности

Тема 1.1. Основные понятия и задачи информационной безопасности

1. Примерный перечень вопросов для устного или письменного опроса по теме:

1. Понятие информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации».
5. Понятие «риска информационной безопасности».
6. Примеры преступлений в сфере информации и информационных технологий.
7. Сущность функционирования системы защиты информации.
8. Защита человека от опасной информации и от не информированности в области информационной безопасности.

2. Тестовые задания по теме:

1. В Законе РФ "Об участии в международном информационном обмене" информационная безопасность определяется как …	*2. Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:* а) конфиденциальность б) целостность в) доступность г) учет д) неотрекаемость е) мобильность

3. *Сопоставьте понятия и их определения.*
Укажите соответствие для всех 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.

а) конфиденциальность
б) учет
в) доступность
г) целостность
д) неотрекаемость

1	2	3	4	5

4. ... - распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности.
а) Политика
б) Идентификация
в) Аутентификация
г) Контроль доступа
д) Авторизация

5. ... - это набор формальных правил, которые регламентируют функционирование механизма информационной безопасности.
а) Политика
б) Идентификация
в) Аутентификация
г) Контроль доступа
д) Авторизация

Ответы к тесту:

1. *По доступности информация классифицируется на*
а) открытую информацию и государственную тайну
б) конфиденциальную информацию и информацию свободного доступа
в) **информацию с ограниченным доступом и общедоступную информацию**
г) виды информации, указанные в остальных пунктах

2. *Запрещено относить к информации ограниченного доступа*
а) информацию о чрезвычайных ситуациях
б) информацию о деятельности органов государственной власти
в) документы открытых архивов и библиотек
г) **все, перечисленное в остальных пунктах**

3. *К конфиденциальной информации относятся документы, содержащие*
а) **государственную тайну**
б) законодательные акты
в) "ноу-хау"
г) сведения о золотом запасе страны

4. *Вопросы информационного обмена регулируются (...) правом*
а) **гражданским**
б) информационным
в) конституционным
г) уголовным

5. *Согласно ст.132 ГК РФ интеллектуальная собственность это*
а) информация, полученная в результате интеллектуальной деятельности индивида

6. *Какая информация подлежит защите?*
а) информация, циркулирующая в системах и сетях связи
б) зафиксированная на материальном носителе информация с реквизитами,

б) литературные, художественные и научные произведения в) изобретения, открытия, промышленные образцы и товарные знаки г) **исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности**	в) позволяющими ее идентифицировать г) только информация, составляющая государственные информационные ресурсы д) **любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу**
7. *Система защиты государственных секретов определяется Законом* а) "Об информации, информатизации и защите информации" б) "Об органах ФСБ" в) **"О государственной тайне"** г) "О безопасности"	8. *Классификация и виды информационных ресурсов определены* а) **Законом "Об информации, информатизации и защите информации"** б) Гражданским кодексом в) Конституцией г) всеми документами, перечисленными в остальных пунктах
9. *Государственные информационные ресурсы не могут принадлежать* а) физическим лицам б) коммерческим предприятиям в) негосударственным учреждениям г) всем **перечисленным субъектам**	10. *К информации ограниченного доступа не относится* а) государственная тайна б) размер золотого запаса страны в) **персональные данные** г) коммерческая тайна
11. *Система защиты государственных секретов* а) основывается на Уголовном Кодексе РФ б) регулируется секретными нормативными документами в) **определена Законом РФ "О государственной тайне"** г) осуществляется в соответствии с п. а) - в)	12. *Действие Закона "О государственной тайне" распространяется* а) на всех граждан и должностных лиц РФ б) только на должностных лиц в) на граждан, которые взяли на себя обязательство выполнять требования г) законодательства о государственной тайне д) **на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения**

Тема 1.2. Основы защиты информации

1. Примерный перечень вопросов для устного или письменного опроса по теме:

1. Целостность, доступность и конфиденциальность информации.
2. Классификация информации по видам тайны и степеням конфиденциальности.
3. Понятия государственной тайны и конфиденциальной информации.
4. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
5. Цели и задачи защиты информации.
6. Основные понятия в области защиты информации.
7. Элементы процесса менеджмента ИБ.
8. Модель интеграции информационной безопасности в основную деятельность организации.
9. Понятие Политики безопасности.

2. Тестовые задания по теме:

1. Под информационной безопасностью понимается… а. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре б. программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия в. нет правильного ответа	2. Защита информации – это а. комплекс мероприятий, направленных на обеспечение информационной безопасности б. процесс разработки структуры базы данных в соответствии с требованиями пользователей в. небольшая программа для выполнения определенной задачи
3. Угроза – это… а. потенциальная возможность определенным образом нарушить информационную безопасность б. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных в. процесс определения отвечает на текущее состояние разработки требованиям данного этапа	4. Источник угрозы – это а. потенциальный злоумышленник б. злоумышленник в. нет правильного ответа
5. Цель защиты информации первого уровня –	6. Цель защиты информации второго уровня –
7. Решение первой группы задач —	8. Вторая группа задач —

Ответы к тесту:

1. *Под информационной безопасностью понимается…* г. **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре.** д. программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия е. нет правильного ответа	2. *Защита информации – это...* г. **комплекс мероприятий, направленных на обеспечение информационной безопасности.** д. процесс разработки структуры базы данных в соответствии с требованиями пользователей е. небольшая программа для выполнения определенной задачи

3. Угроза – это… г. **потенциальная возможность определенным образом нарушить информационную безопасность** д. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных е. процесс определения отвечает на текущее состояние разработки требованиям данного этапа	4. Источник угрозы – это... г. **потенциальный злоумышленник** д. злоумышленник е. нет правильного ответа
5. Цель защиты информации первого уровня – безопасность информации.	6. Цель защиты информации второго уровня – безопасность субъектов информационных отношений.
7. Решение **первой группы задач — обеспечение специалистов информацией**	8. **Вторая группа задач — это ограждение защищаемой информации от несанкционированного доступа к ней соперника**

3. Тематика практических работ:

Практическая работа № 1

Определение объектов защиты на типовом объекте информатизации. Анализ структуры предприятия, размещения средств вычислительной техники, ресурсов информационной системы, технологии обработки информации, подлежащие защите.

Цель работы: освоение приемов и методов осуществления анализа структуры предприятия, размещения средств вычислительной техники, ресурсов информационной системы, технологии обработки информации, подлежащие защите

Практическая работа №2.

Определение целей защиты информации на предприятии.

Цель работы: освоение приемов и методов определения целей защиты информации на предприятии.

Практическая работа №3.

Разработка программы безопасности предприятия на процедурном и программно-техническом уровне.

Цель работы: освоение приемов и методов разработки программы безопасности предприятия на процедурном и программно-техническом уровне.

Тема 1.3. Угрозы безопасности защищаемой информации

1. Примерный перечень вопросов для устного или письменного опроса по теме:

1. Понятие угрозы безопасности информации
2. Системная классификация угроз безопасности информации.
3. Каналы и методы несанкционированного доступа к информации.
4. Уязвимости.
5. Методы оценки уязвимости информации.

2. Тестовые задания по теме:

1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это: а) Электронное сообщение б) Распространение информации в) Предоставление информации г) Конфиденциальность информации д) Доступ к информации	***2. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:*** а) Уничтожение информации б) Распространение информации в) Предоставление информации г) Конфиденциальность информации д) Доступ к информации
3. Возможность получения информации и ее использования это: а) Сохранение информации б) Распространение информации в) Предоставление информации г) Конфиденциальность информации д) Доступ к информации	***4. Хищение информации – это…*** а) Несанкционированное копирование информации б) Утрата информации в) Блокирование информации г) Искажение информации д) Продажа информации
5. Несанкционированный доступ к информации это: а) Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально б) Работа на чужом компьютере без разрешения его владельца в) Вход на компьютер с использованием данных другого пользователя г) Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей д) Доступ к СУБД под запрещенным именем пользователя	***6. Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:*** а) Нет, только к административной ответственности б) Нет, если это государственное предприятие в) Да г) Да, но только в случае, если действия сотрудника нанесли непоправимый вред д) Да, но только в случае осознанных неправомочных действий сотрудника
7. Наиболее опасным источником угроз информационной безопасности предприятия являются: а) Другие предприятия (конкуренты) б) Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам в) Рядовые сотрудники предприятия г) Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных д) Хакеры	***8. Доступ к информации – это:*** а) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя б) Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц в) Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц г) Информация, переданная или полученная пользователем информационно-телекоммуникационной сети д) Возможность получения информации и ее использования
9. Информационная безопасность обеспечивает… а) Блокирование информации б) Искажение информации в) Сохранность информации г) Утрату информации	***10. Система обеспечения информационной безопасности информации должна базироваться на следующих принципах:*** а) непрерывность б) комплексность

д) Подделку информации	в) системность г) законность

Ответы к тесту:

1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это: е) Электронное сообщение ж) Распространение информации з) Предоставление информации и) **Конфиденциальность информации** к) Доступ к информации	*2. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:* е) Уничтожение информации ж) **Распространение информации** з) Предоставление информации и) Конфиденциальность информации к) Доступ к информации
3. Возможность получения информации и ее использования это: е) Сохранение информации ж) Распространение информации з) Предоставление информации и) Конфиденциальность информации к) **Доступ к информации**	*4. Хищение информации – это…* е) **Несанкционированное копирование информации** ж) Утрата информации з) Блокирование информации и) Искажение информации к) Продажа информации
5. Несанкционированный доступ к информации это: е) **Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально** ж) Работа на чужом компьютере без разрешения его владельца з) Вход на компьютер с использованием данных другого пользователя и) Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей к) Доступ к СУБД под запрещенным именем пользователя	*6. Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:* е) Нет, только к административной ответственности ж) Нет, если это государственное предприятие з) **Да** и) Да, но только в случае, если действия сотрудника нанесли непоправимый вред к) Да, но только в случае осознанных неправомочных действий сотрудника
7. Наиболее опасным источником угроз информационной безопасности предприятия являются: е) Другие предприятия (конкуренты) ж) Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам з) **Рядовые сотрудники предприятия** и) Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных к) Хакеры	*8. Доступ к информации – это:* е) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя ж) Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц з) Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц и) Информация, переданная или полученная пользователем информационно-телекоммуникационной сети к) **Возможность получения информации и ее использования**

9. Информационная безопасность обеспечивает… е) Блокирование информации ж) Искажение информации з) **Сохранность информации** и) Утрату информации к) Подделку информации	*10. Система обеспечения информационной безопасности информации должна базироваться на следующих принципах:* д) непрерывность е) комплексность ж) системность з) законность

2-1. Тестовые задания по теме:

1. Угроза информационной безопасности:
   а) Слабое место в инфраструктуре организации, включая систему обеспечения информационной безопасности (СОИБ);
   б) Потенциальная возможность нарушения свойств информационной безопасности: доступности, целостности или конфиденциальности информационных активов организации;
   в) Это потенциальная причина инцидента, который может нанести ущерб системе или организации;
   г) Это возможность реализации воздействия на информацию, обрабатываемую в АС.
2. Окно опасности это:
   а) Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется;
   б) Промежуток времени, за который злоумышленник проводит атаку;
   в) Промежуток времени, в течении которого устанавливается новое ПО;
   г) Промежуток времени от момента, когда администратор безопасности узнает об угрозе, и до момента, когда департаментом информационной безопасности будет разработано решение.
3. Окно опасности перестает существовать, когда:
   а) Администратор безопасности узнает об угрозе;
   б) Заплата устанавливается в защищаемой ИС;
   в) Производитель ПО выпускает заплату;
   г) Администратор безопасности узнает об утечке конфиденциальной информации.
4. Как часто должно происходить отслеживание окон опасности?
   а) Пару раз в неделю;
   б) Пару раз в месяц;
   в) Каждый квартал;
   г) Постоянно.
5. К искусственным угрозам информационной безопасности относятся: (выберете один или несколько вариантов).
   а) Авария на линиях электропередачи микрорайона;
   б) Отказы вычислительной и коммуникационной техники;
   в) Неправомерный доступ к информации;
   г) Разработка и распространение вирусных программ.
6. Самыми опасными источниками угроз являются:
   а) Внешние;
   б) Внутренние;
   в) Пограничные;
   г) Локальные.
7. Угрозы нарушения конфиденциальности.
   а) В результате реализации информация становится не доступной субъекту, располагающему полномочиями для ознакомления с ней;
   б) Любое злонамеренное искажение информации, обрабатываемой с использованием АС;

в) Возникают в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется;
г) В результате реализации информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.

8. К государственной тайне относится (выберете один или несколько вариантов).
а) Сведения, содержащие банковскую тайну;
б) Сведения в военной области;
в) Сведения в области экономики, науки и техники;
г) Сведения, содержащие ПДн.

9. Обладатель информации – это …
а) Лицо или подразделение организации, отвечающее за сбор, фиксацию и хранение данных;
б) Руководство или другая заинтересованная сторона, запрашивающая или требующая информацию об эффективности СУИБ;
в) Лицо или подразделение организации, владеющее информацией об объекте измерения и его атрибутах и ответственное за измерения;
г) Лицо или подразделение организации, отвечающее за сбор, фиксацию и хранение данных.

10. Утечка информации – это …
а) Непреднамеренная утрата носителя информации;
б) Процесс раскрытия секретной информации;
в) Неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к ней или получения защищаемой информации;
г) Процесс уничтожения информации.

11. Угрозы нарушения целостности.
а) В результате реализации информация становится не доступной субъекту, располагающему полномочиями для ознакомления с ней;
б) любое злонамеренное искажение информации, обрабатываемой с использованием АС;
в) Возникают в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется;
г) В результате реализации информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.

12. Угрозы нарушения доступности.
а) В результате реализации информация становится не доступной субъекту, располагающему полномочиями для ознакомления с ней;
б) Любое злонамеренное искажение информации, обрабатываемой с использованием АС;
в) Возникают в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется;
г) В результате реализации информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.

13. Под внутренними угрозами информационной безопасности понимаются:
а) Угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию;
б) Угрозы, созданные сторонними лицами и исходящие из внешней среды;
в) Угрозы, возникшие в результате сбоя оборудования;
г) Угрозы, возникшие в результате стихийных бедствий.

14. Под внешними угрозами информационной безопасности понимаются:
а) Угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию;

б) Угрозы, созданные сторонними лицами и исходящие из внешней среды;
в) Угрозы, возникшие в результате сбоя оборудования;
г) Угрозы, возникшие в результате стихийных бедствий.

15. К внешним угрозам безопасности относятся: (выберите один или несколько вариантов).
    а) Распространение вредоносного программного обеспечения;
    б) Нежелательные рассылки (спам);
    в) Ошибки в работе обслуживающего персонала и пользователей;
    г) помехи в линии связи из-за воздействия внешней среды, а также вследствие плотного трафика в системе (характерно для беспроводных решений).
16. К основным действиям, в результате которых осуществляется преднамеренное разглашение сведений ограниченного доступа, НЕ относится (выберите один или несколько вариантов).
    а) Разговор с посторонними лицами по закрытой тематике;
    б) Разговор с коллегами на личные темы;
    в) Публичное выступление;
    г) Распространение сведений через Интернет и т.п.

Тематика практических работ:

Практическая работа №4.

Определение угроз объекта информатизации и их классификация.

Цель работы: освоение приемов и методов определения угроз объекта информатизации и их классификации.

Практическая работа №5.

Анализ рисков для безопасности информационной системы и ее ресурсов предприятия, определение степени их допустимости.

Цель работы: освоение приемов и методов анализа и определения рисков для безопасности информационной системы и ее ресурсов предприятия, определение степени их допустимости.

Практическая работа №6.

Составление модели нарушителей информационной безопасности, актуальных для данного предприятия.

Цель работы: освоение приемов и методов составления модели нарушителей информационной безопасности, актуальных для данного предприятия.

Раздел 2. Методология защиты информации

Тема 2.1. Методологические подходы к защите информации

1. Примерный перечень вопросов для устного или письменного опроса по теме:

1. Анализ существующих методик определения требований к защите информации.
2. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
3. Виды мер и основные принципы защиты информации.

Тема 2.2. Нормативно правовое регулирование защиты информации

1. Примерный перечень вопросов для устного или письменного опроса по теме:

1. Организационная структура системы защиты информации

2. Законодательные акты в области защиты информации.
3. Российские и международные стандарты, определяющие требования к защите информации.
4. Система сертификации РФ в области защиты информации.
5. Основные правила и документы системы сертификации РФ в области защиты информации

2. Тестовые задания по теме:

1. *По доступности информация классифицируется на* д) открытую информацию и государственную тайну е) конфиденциальную информацию и информацию свободного доступа ж) информацию с ограниченным доступом и общедоступную информацию з) виды информации, указанные в остальных пунктах	2. *Запрещено относить к информации ограниченного доступа* д) информацию о чрезвычайных ситуациях е) информацию о деятельности органов государственной власти ж) документы открытых архивов и библиотек з) все, перечисленное в остальных пунктах
3. *К конфиденциальной информации относятся документы, содержащие* д) государственную тайну е) законодательные акты ж) "ноу-хау" з) сведения о золотом запасе страны	4. *Вопросы информационного обмена регулируются (...) правом* д) гражданским е) информационным ж) конституционным з) уголовным
5. *Согласно ст.132 ГК РФ интеллектуальная собственность это* д) информация, полученная в результате интеллектуальной деятельности индивида е) литературные, художественные и научные произведения ж) изобретения, открытия, промышленные образцы и товарные знаки з) исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности	6. *Какая информация подлежит защите?* е) информация, циркулирующая в системах и сетях связи ж) зафиксированная на материальном носителе информация с реквизитами, з) позволяющими ее идентифицировать и) только информация, составляющая государственные информационные ресурсы к) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу
7. *Система защиты государственных секретов определяется Законом* д) "Об информации, информатизации и защите информации" е) "Об органах ФСБ" ж) "О государственной тайне" з) "О безопасности"	8. *Классификация и виды информационных ресурсов определены* д) Законом "Об информации, информатизации и защите информации" е) Гражданским кодексом ж) Конституцией з) всеми документами, перечисленными в остальных пунктах
9. *Государственные информационные ресурсы не могут принадлежать* д) физическим лицам е) коммерческим предприятиям ж) негосударственным учреждениям з) всем перечисленным субъектам	10. *К информации ограниченного доступа не относится* д) государственная тайна е) размер золотого запаса страны ж) персональные данные з) коммерческая тайна

11. *Система защиты государственных секретов* д) основывается на Уголовном Кодексе РФ е) регулируется секретными нормативными документами ж) определена Законом РФ "О государственной тайне" з) осуществляется в соответствии с п. а) - в)	12. *Действие Закона "О государственной тайне" распространяется* е) на всех граждан и должностных лиц РФ ж) только на должностных лиц з) на граждан, которые взяли на себя обязательство выполнять требования и) законодательства о государственной тайне к) на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

Ключ к тесту:

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
в	г	а	а	г	д	в	а	г	в	в	д

2-1. Тестовые задания по теме:

1. *Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на:* а) цели б) взгляды в) задачи г) принципы	2. *Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных:* а) угрозах б) интересов личности в) общества г) государства
3. *Источники угроз информационной безопасности Российской Федерации подразделяются на:* а) внешние б) основные в) внутренние	4. *Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют системы:* а**)** государственная система защиты информации б) система зашиты президента в) система защиты государственной тайны г) системы сертификации средств защиты информации
5. *Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются:* а) принцип законности б) Президент Российской Федерации в) Совет Безопасности РФ г) Государственная Дума Федерального Собрания РФ	6. *Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:* а) создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере б) обеспечение безопасности компьютерного пиратства в) разработка нормативной правовой базы в области обеспечения информационной безопасности РФ г) предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере

Ключ к тесту:

1.	2.	3.	4.	5.	6.
а, в, г	б, в, г	а, в	а, в, г	б, в, г	а, в, г

Тематика практических работ:
Практическая работа № 7.
Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.
Цель работы: освоение приемов и методов работы в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.

Тема 2.3. Защита информации в автоматизированных (информационных) системах
1. Примерный перечень вопросов для устного или письменного опроса по теме:

1. Основные механизмы защиты информации.
2. Система защиты информации.
3. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
4. Программные и программно-аппаратные средства защиты информации.
5. Инженерная защита и техническая охрана объектов информатизации
6. Организационно-распорядительная защита информации.
7. Работа с кадрами и внутри объектовый режим.
8. Принципы построения организационно-распорядительной системы.

2. Тестовые задания по теме:
1.Программный комплекс, включающий в себя массив правовой информации и инструменты, позволяющие специалисту организовывать поиск нужной информации.

а. документальные системы
б. гипертекстовые системы
в. справочно-правовые системы
г. АИС электронной коммерции
д. САПР

2.Назовите достоинство справочно-правовых систем.

а. удобный интерфейс
б. возможность составления отчетов
в. наличие русификатора
г. быстрый поиск нужных документов и их фрагментов

3.Назовите достоинство справочно-правовых систем.

а. наличие мультимедиа
б. возможность работы с MS Word
в. компактное хранение больших объемов информации
г. передача документов в MS Excel

4.Назовите недостаток справочно-правовых систем.

а. сложность организации поиска документа
б. сложность восприятия информации с экрана монитора
в. сложность составления отчетов
г. невозможность работы в программах MS Office

5.Назовите недостаток справочно-правовых систем.

а. сложность пополнения законодательной базы системы
б. низкая скорость передачи информации
в. сложность поиска документов
г. система не является официальным источником опубликования правовых документов

6.Справочно-правовые системы, ориентированные на доступ пользователей любой профессиональной ориентации к нормативно-правовым документам - это…

а. справочно-информационные системы общего назначения
б. глобальные информационные службы
в. системы автоматизации делопроизводства

г. системы поддержки деятельности правотворческих органов

7.Справочно-правовые системы, предоставляющие доступ удаленным пользователям к правовой информации - это…

а. глобальные информационные службы
б. справочно-информационные системы общего назначения
в. системы автоматизации делопроизводства
г. системы поддержки деятельности правотворческих органов

8.Справочно-правовые системы, спецификой которых является необходимость хранения и поиска многих версий и редакций нормативно-правовых документов с учетом вносимых поправок, и изменений - это…

а. справочно-информационные системы общего назначения
б. системы автоматизации делопроизводства
в. системы информационной поддержки деятельности правотворческих органов
г. глобальные информационные службы

9.Наименьшая единица, необходимая для организации поиска информации в справочно-правовых системах – это…

а. предложение
б. слово
в. документ
г. словосочетание

10.Наименьшая единица справочно-правовых систем – это…

а. предложение
б. слово
в. документ
г. словосочетание

11.Справочно-правовая система, которая содержит наибольшее количество правовых документов?

а. Консультант Плюс
б. Гарант
в. Кодекс

12.Одно или несколько слов, являющиеся любыми частями речи, которые в наибольшей степени отражает содержание всего искомого документа – это… (напишите ответ)

_____

13.Процесс присвоения каждому документу определенного набора ключевых слов – это…

а. администрирование
б. инвентаризация
в. индексация
г. инициализация

14.Способность справочно-правовой системы отбирать документы, соответствующие запросу, не включая лишних документов – это…

а. избирательность
б. чувствительность
в. релевантность

15.Способность справочно-правовой системы отбирать документы, соответствующие запросу, не пропуская нужных документов – это…

а. избирательность
б. чувствительность
в. релевантность

16.Способность справочно-правовой системы, определяющая степень соответствия найденного в процессе поиска документа сделанному запросу – это…

а. избирательность
б. чувствительность

в. релевантность

17.Справочно-правовые системы относятся к классу…(укажите все правильные ответы)

а. документальных систем, так как содержат полнотекстовые документы
б. гипертекстовых систем, так как содержат ссылки для перехода между документами
в. мультимедийных систем, так как содержат графические изображения
г. фактографических систем, так как содержат конкретные факты об объектах

Ключи к тесту:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
в	г	в	б	г	а	а	в	б	в	а	ключевое слово	в	а	б	в	а в

2-1. Тестовые задания по теме:

1. Основная масса угроз информационной безопасности приходится на:
а) троянские программы
б) шпионские программы
в) черви
2. Какой вид идентификации и аутентификации получил наибольшее распространение:
а) системы PKI
б) постоянные пароли
в) одноразовые пароли
3. Заключительным этапом построения системы защиты является:
а) сопровождение
б) планирование
в) анализ уязвимых мест
4. Какие угрозы безопасности информации являются преднамеренными:
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ
5. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви
6. Под информационной безопасностью понимается:
а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) нет верного ответа
7. Защита информации:
а) небольшая программа для выполнения определенной задачи
б) комплекс мероприятий, направленных на обеспечение информационной безопасности
в) процесс разработки структуры базы данных в соответствии с требованиями пользователей
8. Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации
9. Конфиденциальностью называется:
а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

б) описание процедур
в) защита от несанкционированного доступа к информации
10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники
11. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы
12. Что такое политика безопасности:
а) детализированные документы по обработке инцидентов безопасности
б) широкие, высокоуровневые заявления руководства
в) общие руководящие требования по достижению определенного уровня безопасности
13. Эффективная программа безопасности требует сбалансированного применения:
а) контрмер и защитных механизмов
б) процедур безопасности и шифрования
в) технических и нетехнических методов
14. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
а) уровень доверия, обеспечиваемый механизмом безопасности
б) внедрение управления механизмами безопасности
в) классификацию данных после внедрения механизмов безопасности

Ключи к тесту:

18	19	20	21	22	23	24	25	26	27	28	29	30	31
а	б	а	в	а	а	б	а	в	в	б	б	в	а

Тематика практических работ:

Практическая работа №8.

Выбор мер защиты информации для автоматизированного рабочего места. Использование брандмауэров.

Цель работы: освоение приемов и методов выбора мер защиты информации для автоматизированного рабочего места. Использование брандмауэров.

Практическая работа №9.

Антивирусная защита. Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки.

Цель работы: освоение приемов и методов применения антивирусной защиты, специальных антивирусных утилит после вирусных атак.

4. Контрольно-измерительные материалы для промежуточной аттестации по общеобразовательной учебной дисциплине

Предметом оценки являются знания, умения, общие и профессиональные компетенции.

Оценка освоения дисциплины предусматривает проведение дифференцированного зачета.

4.1. ПАСПОРТ

Назначение:

КОС предназначен для контроля и оценки результатов освоения учебной дисциплины ОП.01 Основы информационной безопасности по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

4.2. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ

Вопросы для проведения промежуточной аттестации в форме дифференцированного зачета

1. Понятия информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации».
5. Понятие «риск информационной безопасности».
6. Примеры преступлений в сфере информации и информационных технологий.
7. Сущность функционирования системы защиты информации.
8. Требования к системе защиты информации.
9. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
10. Целостность, доступность и конфиденциальность информации.
11. Классификация информации по видам тайны и степеням конфиденциальности.
12. Понятие государственной тайны.
13. Понятие конфиденциальной информации.
14. Виды конфиденциальной информации.
15. Принципы засекречивания данных.
16. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
17. Цели и задачи защиты информации.
18. Основные понятия в области защиты информации.
19. Элементы процесса менеджмента ИБ.
20. Модель интеграции информационной безопасности в основную деятельность организации.
21. Понятие политики безопасности.
22. Понятие угрозы безопасности информации.
23. Системная классификация угроз безопасности информации.
24. Каналы несанкционированного доступа к информации.
25. Методы несанкционированного доступа к информации.
26. Уязвимости. Методы оценки уязвимости информации.
27. Анализ существующих методик определения требований к защите информации.
28. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
29. Виды мер и основные принципы защиты информации.
30. Организационная структура системы защиты информации.
31. Законодательные акты в области защиты информации.
32. Российские и международные стандарты, определяющие требования к защите информации.
33. Система сертификации РФ в области защиты информации.

34. Основные правила системы сертификации РФ в области защиты информации.
35. Основные документы системы сертификации РФ в области защиты информации.
36. Основные механизмы защиты информации.
37. Система защиты информации.
38. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
39. Программные средства защиты информации.
40. Программно-аппаратные средства защиты информации.
41. Инженерная защита объектов информатизации.
42. Техническая охрана объектов информатизации.
43. Организационно-распорядительная защита информации.
44. Работа с кадрами и внутриобъектовый режим.
45. Принципы построения организационно-распорядительной системы.
46. Доктрина информационной безопасности.
47. Классификация угроз информационной безопасности РФ по общей направленности.
48. Основные положения ФЗ «Об информации, информационных технологиях и защите информации».
49. Каналы утечки информации на защищаемом объекте.
50. Состав информации, необходимость защиты которой обусловлена интересами предприятия.

4.3. ПАКЕТ ЭКЗАМЕНАТОРА

УСЛОВИЯ

Время подготовки к ответу – 30 минут.

4.4. КРИТЕРИИ ОЦЕНКИ

Предметом оценки освоения дисциплины являются знания, умения, общие и профессиональные компетенции и способность применять их в практической, профессиональной деятельности.

Критерии оценок:

– оценка **«отлично»**, если студент обладает глубокими и прочными знаниями программного материала; при ответе на вопросы продемонстрировал исчерпывающее, последовательное и логически стройное изложение; правильно сформулировал понятия и закономерности по вопросам; сделал вывод по излагаемому материалу;

– оценка «**хорошо»**, если студент обладает достаточно полным знанием программного материала; его ответ представляет грамотное изложение учебного материала, но имеются существенные неточности в формулировании понятий и закономерностей по вопросам; не полностью сделаны выводы по излагаемому материалу;

– оценка **«удовлетворительно»**, если студент имеет общие знания основного материала без усвоения некоторых существенных положений; формулирует основные понятия с некоторой неточностью; затрудняется в приведении примеров, подтверждающих теоретические положения;

– оценка **«неудовлетворительно»**, если студент не знает значительную часть программного материала; допустил существенные ошибки в процессе изложения; не умеет

выделить главное и сделать вывод; приводит ошибочные определения; ни один вопрос не рассмотрен до конца, наводящие вопросы не помогают.