МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«Казанский государственный аграрный университет»
(ФГБОУ ВО Казанский ГАУ)

Институт экономики
Кафедра экономики и информационных технологий

УТВЕРЖДАЮ
Проректор по учебно-
воспитательной работе, доцент
_____ А.В. Дмитриев
«20» мая 2021г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

«Информационные технологии в управлении качеством и защита информации»
(Оценочные средства и методические материалы)

приложение к рабочей программе дисциплины (к рабочей программе практики)

Направление подготовки
27.03.02 Управление качеством

Направленность (профиль) подготовки
Управление качеством в производственно-технологических системах

Форма обучения
Очная

Казань – 2021

Составитель: Доцент, к.э.н., доцент _____ Газетдинов Шамиль Миршарипович
Подпись

Оценочные средства обсуждены и одобрены на заседании кафедры экономики и информационных технологий «28» апреля 2021 года (протокол № 14)

Заведующий кафедрой, д.э.н., профессор _____ Газетдинов Миршарип Хасанович
Подпись

Рассмотрены и одобрены на заседании методической комиссии института экономики «11» мая 2021 года (протокол № 13)

Председатель методической комиссии:
Доцент, к.э.н., доцент _____ Авхадиев Фаяз Нурисламович
Подпись

Согласовано:
Директор _____ Низамутдинов Марат Мингалиевич
Подпись

Протокол ученого совета института экономики № 9 от «11» мая 2021 года

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения ОПОП бакалавриата по направлению обучения 27.03.02 Управление качеством, обучающийся должен овладеть следующими результатами обучения по дисциплине «Информационные технологии в управлении качеством и защита информации»:

Таблица 1.1 – Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения по дисциплине
ОПК-5. Способен решать задачи развития науки, техники и технологии в области управления качеством с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	ОПК-5.1. Применяет информационные технологии в управлении качеством и защиты информации с учетом нормативно-правового регулирования в сфере интеллектуальной собственности.	***Знать:*** методы решения стандартных задач профессиональной деятельности; информационно-коммуникационные технологии в области управления качеством; основные требования информационной безопасности. ***Уметь***: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ***Владеть:*** информационно-коммуникационными технологиями, необходимыми для решения задач в области управления качеством процессов, продукции и услуг.
ОПК-10. Способен разрабатывать техническую документацию (в том числе и в электронном виде) в области управления качеством в условиях цифровой экономики, с учетом действующих стандартов качества	ОПК-10.1. Разрабатывает и ведет необходимую техническую документацию, обеспечивает защиту информации с использованием современных информационных технологий.	***Знать:*** содержание документации систем управления качеством продукции; сущность и принципы информационных технологий в управление качеством; способы и формы защиты информации ***Уметь:*** вести необходимую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации ***Владеть:*** способностью вести необходимую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты ин-формации

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Таблица 2.1 – Показатели и критерии определения уровня сформированности компетенций

Код и наименование индикатора достижения компетенции	Планируемые результаты обучения	Оценка уровня сформированности			
		неудовлетворительно	удовлетворительно	хорошо	отлично
ОПК-5.1. Применяет информационные технологии в управлении качеством и защиты информации с учетом нормативно-правового регулирования в сфере интеллектуальной собственности.	***Знать:*** методы решения стандартных задач профессиональной деятельности; информационно-коммуникационные технологии в области управления качеством; основные требования информационной безопасности.	Отсутствуют представления о методах решения стандартных задач профессиональной деятельности; информационно-коммуникационные технологии в области управления качеством; основные требования информационной безопасности.	Неполные представления о методах решения стандартных задач профессиональной деятельности; информационно-коммуникационные технологии в области управления качеством; основные требования информационной безопасности.	Сформированные, но содержащие отдельные пробелы представления о методах решения стандартных задач профессиональной деятельности; информационно-коммуникационные технологии в области управления качеством; основные требования информационной безопасности.	Сформированные систематические представления о методах решения стандартных задач профессиональной деятельности; информационно-коммуникационные технологии в области управления качеством; основные требования информационной безопасности.
	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	Не умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных	В целом успешно, но с отдельными пробелами решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информацион-	В целом успешно, решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-	Сформировано умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-

	основных требований информационной безопасности.	технологий и с учетом основных требований информационной безопасности.	но-коммуникационных технологий и с учетом основных требований информационной безопасности.	коммуникационных технологий и с учетом основных требований информационной безопасности.	коммуникационных технологий и с учетом основных требований информационной безопасности.
	Владеть: информационно-коммуникационными технологиями, необходимыми для решения задач в области управления качеством процессов, продукции и услуг.	Не владеет информационно-коммуникационными технологиями, необходимыми для решения задач в области управления качеством процессов, продукции и услуг.	В целом успешно, но с отдельными пробелами владеет информационно-коммуникационными технологиями, необходимыми для решения задач в области управления качеством процессов, продукции и услуг.	В целом успешно владеет информационно-коммуникационными технологиями, необходимыми для решения задач в области управления качеством процессов, продукции и услуг.	Успешно владеет информационно-коммуникационными технологиями, необходимыми для решения задач в области управления качеством процессов, продукции и услуг.
ОПК-10.1. Разрабатывает и ведет необходимую техническую документацию, обеспечивает защиту информации с использованием современных информационных технологий.	**Знать:** содержание документации систем управления качеством продукции; сущность и принципы информационных технологий в управление качеством; способы и формы защиты информации	Отсутствуют представления о содержании документации систем управления качеством продукции; сущности и принципах информационных технологий в управление качеством; способах и формах защиты информации	Неполные представления о содержании документации систем управления качеством продукции; сущности и принципах информационных технологий в управление качеством; способах и формах защиты информации	Сформированные, но содержащие отдельные пробелы представления о содержании документации систем управления качеством продукции; сущности и принципах информационных технологий в управление качеством; способах и формах защиты информации	Сформированные систематические представления о содержании документации систем управления качеством продукции; сущности и принципах информационных технологий в управление качеством; способах и формах защиты информации
	Уметь: вести необходимую документацию по управле-	Не умеет вести необходимую документацию по управлению	В целом успешное, но не систематическое умение вести необхо-	В целом успешное, но содержащее отдельные пробелы в уме-	Сформированное умение вести необходимую документацию

	нию качеством при помощи информационных технологий и с учетом способов и форм защиты информации	качеством при помощи информационных технологий и с учетом способов и форм защиты информации	димую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации	нии вести необходимую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации	по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации
	Владеть: способностью вести необходимую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации	Не владеет способностью вести необходимую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации	В целом успешное, но не систематическое владение способностью вести необходимую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации	В целом успешное, но содержащее отдельные пробелы в способности вести необходимую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации	Успешное и систематическое владение способностью вести необходимую документацию по управлению качеством при помощи информационных технологий и с учетом способов и форм защиты информации

Описание шкалы оценивания

1. Оценка «неудовлетворительно» ставится студенту, не овладевшему ни одним из элементов компетенции, т.е. обнаружившему существенные пробелы в знании основного программного материала по дисциплине, допустившему принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине.

2. Оценка «удовлетворительно» ставится студенту, овладевшему элементами компетенции «знать», т.е. проявившему знания основного программного материала по дисциплине в объеме, необходимом для последующего обучения и предстоящей практической деятельности, знакомому с основной рекомендованной литературой, допустившему неточности в ответе на экзамене, но в основном обладающему необходимыми знаниями для их устранения при корректировке со стороны экзаменатора.

3. Оценка «хорошо» ставится студенту, овладевшему элементами компетенции «знать» и «уметь», проявившему полное знание программного материала по дисциплине, освоившему основную рекомендованную литературу, обнаружившему стабильный характер знаний и умений и способному к их самостоятельному применению и обновлению в ходе последующего обучения и практической деятельности.

4. Оценка «отлично» ставится студенту, овладевшему элементами компетенции «знать», «уметь» и «владеть», проявившему всесторонние и глубокие знания программного материала по дисциплине, освоившему основную и дополнительную литературу, обнаружившему творческие способности в понимании, изложении и практическом использовании усвоенных знаний.

5. Оценка «зачтено» соответствует критериям оценок от «отлично» до «удовлетворительно».

6. Оценка «не зачтено» соответствует критерию оценки «неудовлетворительно».

3. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Таблица 3.1 – Типовые контрольные задания соотнесенные с индикаторами достижения компетенций

Индикатор достижения компетенции	№№ заданий (вопросов, билетов, тестов и пр.) для оценки результатов обучения по соотнесенному индикатору достижения компетенции
ОПК-5.1. Применяет информационные технологии в управлении качеством и защиты информации с учетом нормативно-правового регулирования в сфере интеллектуальной собственности.	Вопросы для подготовки к промежуточной аттестации: № 1-50 Задачи для лабораторных занятий: №1-40
ОПК-10.1. Разрабатывает и ведет необходимую техническую документацию, обеспечивает защиту информации с использованием современных информационных технологий.	Вопросы для подготовки к промежуточной аттестации: № 51-10 Задачи для лабораторных занятий: №41-80 Тест: №1-25

Темы лабораторных занятий

Введение в проблему информационной безопасности

Проблемы обеспечения информационной безопасности. Актуальность проблемы обеспечения информационной безопасности. Принципы обеспечения информационной безопасности в автоматизированных системах. Основные понятия и определения. Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности.

Угрозы информационной безопасности и методы их реализации

Анализ угроз информационной безопасности. Причины, виды и каналы утечки информации. Основные методы реализации угроз информационной безопасности. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Основные направления использования средств и методов защиты информации

Программные средства обнаружения и отражения угроз. Средства и методы обеспечения целостности информации. Средства и методы обеспечения конфиденциальности информации. Оценка рисков и политика безопасности. Компьютерные средства реализации защиты в информационных системах.

Парольные системы

Общие подходы к построению парольных систем. Выбор паролей. Хранение паролей. Понятие разрушающего программного воздействия. Методы перехвата и навязывания информации. Компьютерные вирусы. Понятия о видах вирусов. Современные антивирусные программы

Шифрование данных. Алгоритмы шифрования

Особенности криптографического и стеганографического преобразований информации. Стойкость алгоритмов шифрования. Типы алгоритмов шифрования. Примеры криптографических алгоритмов. Вопросы реализации криптографических алгоритмов. Электронная подпись. Технология использования электронно-цифровой подписи.

Безопасность работы в сети Интернет
Особенности защиты при работе с сетевыми сервисами. Основные виды нарушения сетевой безопасности. Защита удаленного доступа к локальной сети. Безопасность работы с электронной почтой. Использование ключей и цифровых подписей. Сертификация серверов Интернет. Безопасность работы в Интернет с использованием броузера.
Средства предотвращения утечки информации с помощью закладных подслушивающих устройств
Классификация средств обнаружения и локализации закладных подслушивающих устройств. Аппаратура радиоконтроля. Средства контроля телефонных линий и цепей электропитания. Технические средства подавления сигналов закладных устройств. Нелинейные локаторы. Обнаружители пустот, металлодетекторы и рентгеновские аппараты. Средства контроля помещений на отсутствие закладных устройств
Общие требования к защищенности КС от несанкционированного изменения структур
Современные технологии программирования. Разграничение доступа к оборудованию. Противодействие несанкционированному подключению устройств. Особенности защиты в операционных системах. Подходы к построению защищенной операционной системы. Административные меры защиты. Стандарты защищенности операционных систем. Классификация угроз безопасности операционной системы.

Примерные темы курсовых работ

Концепция информационной безопасности Российской Федерации
Основные принципы правового регулирования в информационной сфере.
Правовой статус и виды обладателей информации.
Ограничение доступа к информации.
Документированная информация как объект информационных правоотношений.
Место информационной безопасности в системе национальной безопасности
Электронный документ и электронно-цифровая подпись.
Правовое регулирование отношений, возникающих при работе в сети Интернет.
Защита прав на результаты интеллектуальной деятельности в сети Интернет.
Принципы биометрической аутентификации
Принципы традиционного шифрования
Основные типы криптоанализа
Принципы хэширования сообщений
Принципы криптографии с открытым ключом
Основы цифровых подписи и сертификатов
Принципы функционирования межсетевых экранов
Системы обнаружения вторжений

Вопросы к защите курсовой работы

1. Программа информационной безопасности России и пути ее реализации.
2. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности.
3. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена.
4. Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.
5. Современное состояние правового регулирования в информационной сфере.
6. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

7. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
8. Компьютерные преступления.
9. Принципы обеспечения информационной безопасности в автоматизированных системах
10. Организационное обеспечение информационной безопасности.
11. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации.
12. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.
13. Понятие разрушающего программного воздействия. Методы перехвата и навязывания информации.
14. Компьютерные вирусы. Понятия о видах вирусов. Современные антивирусные программы.
15. Шифрование данных. Алгоритмы шифрования
16. Общие подходы к построению парольных систем.
17. Выбор паролей. Хранение паролей. Передача пароля по сети.
18. Средства обеспечения информационной безопасности от вредоносного ПО
19. Основы информационной безопасности криптографии (Целостность данных)
20. Понятие информационной безопасности. Цифровая подпись
21. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств
22. Защита информации в Internet. Защита Web-Серверов
23. Особенности защиты при работе с сетевыми сервисами. Безопасность работы с электронной почтой
24. Общие требования к защищенности КС от несанкционированного изменения структур

Пример тестовых заданий к экзамену

Вопрос 1. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?
1) получить, изменить, а затем передать ее конкурентам;
2) размножить или уничтожить ее;
3) получить, изменить или уничтожить;
4) изменить и уничтожить ее;
5) изменить, повредить или ее уничтожить.

Вопрос 2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?
1) любая информация;
2) только открытая информация;
3) запатентованная информация;
4) закрываемая собственником информация;
5) коммерческая тайна.

Вопрос 3. Кто может быть владельцем защищаемой информации?
1) только государство и его структуры;
2) предприятия акционерные общества, фирмы;
3) общественные организации;
4) только вышеперечисленные;

5) кто угодно.

Вопрос 4. Какие сведения на территории РФ могут составлять коммерческую тайну?
1) учредительные документы и устав предприятия;
2) сведенья о численности работающих, их заработной плате и условиях труда;
3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
4) другие;
5) любые.
Вопрос 5. Какой самый прямой и эффективный способ склонения к сотрудничеству?
1) психическое давление;
2) подкуп;
3) преследование;
4) шантаж;
5) угрозы.

Вопрос 6. Завершающим этапом любого сбора конфиденциальной информации является
1) копирование;
2) подделка;
3) аналитическая обработка;
4) фотографирование;
5) наблюдение.

Вопрос 7. Причины связанные с информационным обменом приносящие наибольшие убытки?
1) остановка или выход из строя информационных систем;
2) потери информации;
3) неискренность;
4) проникновение в информационную систему;
5) перехват информации.

Вопрос 8. Какие цели преследуются при активном вторжении в линии связи?
1) анализ информации (содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
2) воздействие на поток сообщений(модификация, удаление и посылка ложных сообщений) или восприпятствие передаче сообщений;
3) инициализация ложных соединений;
4) варианты 1 и 2;
5) варианты 2 и 3.

Вопрос 9. Что определяет модель нарушителя?
1) категории лиц, в числе которых может оказаться нарушитель;
2) возможные цели нарушителя и их градации по степени важности и опасности;
3) предположения о его квалификации и оценка его технической вооруженности;
4) ограничения и предположения о характере его действий;
5) все выше перечисленные.

Вопрос 10. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.
1) ознакомление с информационной системой или вычислительной сетью;
2) похитить программу или иную информацию;

3) оставить записку, выполнить, уничтожить или изменить программу;
4) вариант 2 и 3;
5) вариант 1, 2 и 3.

Вопрос 11. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?
1) скрытие;
2) дезинформация;
3) дробление;
4) кодирование;
5) шифрование.

Вопрос 12. Что в себя включают морально-нравственные методы защиты информации?
1) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений;
2) контроль работы сотрудников, допущенных к работе с секретной информацией;
3) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;
4) вариант ответа 1 и 3;
5) вариант ответа 1, 2 и 3.

Вопрос 13. Что включают в себя технические мероприятия по защите информации?
1) поиск и уничтожение технических средств разведки;
2) кодирование информации или передаваемого сигнала;
3) подавление технических средств постановкой помехи;
4) применение детекторов лжи;
5) все вышеперечисленное.

Вопрос 14. Какие основные направления в защите персональных компьютеров от несанкционированное доступа Вы знаете?
1) недопущение нарушителя к вычислительной среде;
2) защита вычислительной среды;
3) использование специальных средств защиты информации ПК от несанкционированного доступа;
4) все вышеперечисленные;
5) правильного ответа нет.

Вопрос 15. Какие средства защиты информации в ПК наиболее распространены?
1) применение различных методов шифрования, не зависящих от контекста информации;
2) средства защиты от копирования коммерческих программных продуктов;
3) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
4) защита от компьютерных вирусов и создание архивов;
5) все вышеперечисленные.

Вопрос № 16. На какие группы делятся информационные ресурсы государства?
1) информация открытая, информация запатентованная и информация, "закрываемая" ее собственником, владельцем и защищаемая им с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны
2) информация открытая и информация запатентованная
3) отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны

Вопрос № 17. Кто является собственником защищаемой информации?
1) юридическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией
2) юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией
3) физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией

Вопрос № 18. Одной из проблем защиты информации является…
1) классификация возможных каналов утечки информации
2) ее разнообразие
3) ее доступность

Вопрос № 19. К каналам утечки относятся…
1) хищение носителей информации; чтение информации с экрана ПЭВМ посторонним лицом; чтение информации из оставленных без присмотра распечаток программ; подключение к устройствам ПЭВМ специальных аппаратных средств, обеспечивающих доступ к информации;
2) использование технических средств для перехвата электромагнитных излучений технических средств ПЭВМ; несанкционированный доступ программ к информации; расшифровка программой зашифрованной информации; копирование программой информации с носителей.
3) все вышеперечисленное

Вопрос № 20. Известно, что информация - это сведения о…
1) предметах, объектах
2) явлениях и процессах, отображаемые в сознании человека или на каком-либо носителе, для последующего их восприятия человеком
3) все вышеперечисленное

Вопрос № 21. Информационная коммуникация предполагает…
1) обмен между субъектами отношений в виде совокупности процессов представления, передачи и получения информации
2) доступность информации и ее разнообразие
3) все вышеперечисленное

Вопрос № 22. Основные положения современной концепции защиты информации можно свести к следующим положениям:
1) защита информации в государстве должна обеспечить информационную безопасность личности, общества и государства
2) защита должна обеспечить охрану информационных ресурсов страны
3) все вышеперечисленное

Вопрос № 23. Особенности защиты персональных компьютеров (ПК) обусловлены…
1) спецификой их использования
2) частотой процессора
3) все вышеперечисленное

Вопрос № 24. Среди стандартных защитных средств персонального компьютера наибольшее распространение получили…

1) средства, использующие парольную идентификацию и методы шифрования; средства защиты от копирования программных продуктов; защита от компьютерных вирусов и создание архивов.
2) ограничение доступа к персональному компьютеру
3) все вышеперечисленное

Вопрос № 25. Вирусы условно подразделяются на классы по следующим признакам:
1) по среде обитания; по способу заражения; по возможностям
2) по среде обитания, по скорости распространения, по названию
3) по способу заражения, по названию

Вопросы для лабораторных работ

Для выполнения выбирается один вопрос из каждой темы по указанию преподавателя.

1. Актуальность информационной безопасности, понятия и определения.

1. Особенностями современных информационных технологий?
2. Когда появились первые преступления с использованием компьютерной техники в России?
3. Сколько уголовных дела по ст.272 УК РФ («Неправомерный доступ к компью терной информации») и ст. 165 УК РФ ("Причинение имущественного ущерба путем обмана и злоупотребления доверием") было возбуждено в 2003 году в России?
4. Какой ущерб нанесли компьютерные вирусы за последние 5 лет?
5. Что понимается под информационной безопасностью Российской Федерации?
6. Первая составляющая национальных интересов Российской Федерации в ин формационной сфере?
7. Вторая составляющая национальных интересов Российской Федерации в ин формационной сфере?
8. Третья составляющая национальных интересов Российской Федерации в инфор мационной сфере?
9. Четвертая составляющая национальных интересов Российской Федерации в ин формационной сфере?
10. Классификация компьютерных преступлений?
11. Экономические компьютерные преступления?
12. Компьютерными преступлениями против личных прав и частной сферы?
13. Компьютерные преступления против государственных и общественных интере сов?
14. Основные виды преступлений, связанных с вмешательством в работу компьюте ров?
15. Способы совершения компьютерных преступлений?
16. Методы перехвата компьютерной информации?
17. Пользователи и злоумышленники в Метет?
18. Кто такие хакеры?
19. Кто такие фракеры?
20. Защита инфо
21. Кто такие кракеры?
22. Кто такие фишеры?
23. Кто такие скамеры?
24. Кто такие спамеры?
25. Причины уязвимости сети 1п1егпег?
26. Защищаемая информация это?

27. Защита информации это?
28. Защита информации от утечки это?
29. Защита информации от несанкционированного воздействия это?
30. Защита информации от непреднамеренного воздействия это?
31. Защита информации от разглашения это?
32. Защита информации от несанкционированного доступа это?
33. Защита информации от иностранной разведки это?
34. Защита информации от иностранной технической разведки это?
35. Защита информации от агентурной разведки это?
36. Цель защиты информации?
37. Эффективность защиты информации это?
38. Показатель эффективности защиты информации это?
39. Нормы эффективности защиты информации это?
40. Организация защиты информации это?
41. Система защиты информации это?
42. Мероприятие по защите информации это?
43. Мероприятие по контролю эффективности защиты информации это?
44. Техника защиты информации это?
45. Объект защиты это?
46. Способ защиты информации это?
47. Категорирование защищаемой информации это?
48. Метод контроля эффективности защиты информации это?
49. Контроль состояния защиты информации это?
50. Средство защиты информации это?
51. Средство контроля эффективности защиты информации это?
52. Контроль организации защиты информации это?
53. Контроль эффективности защиты информации это?
54. Организационный контроль эффективности защиты информации это?
55. Технический контроль эффективности защиты информации это?
56. Информация это?
57. Доступ к информации это?
58. Субъект доступа к информации это?
59. Носитель информации это?
60. Собственник информации это?
61. Владелец информации это?
62. Пользователь (потребитель) информации это?
63. Право доступа к информации это?
64. Правило доступа к информации это?

64. Орган защиты информации это?
65. Информационные процессы это?
66. Информационная система это?
67. Информационными ресурсами это?
68. Что понимают под утечкой информации?
69. Несанкционированный доступ это?
70. Несанкционированное воздействие это?
71. Что понимается под непреднамеренным воздействием на защищенную инфор мацию?
72. Что понимается под эффективностью защиты информации?

73. Конфиденциальность информации это?
74. Шифрование информации это?
75. Уязвимость информации это?

Угрозы информации.

1. Виды угроз информационной безопасности Российской Федерации?
2. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности?
3. Угрозы информационному обеспечению государственной политики Российской Федерации?
4. Угрозы развитию отечественной индустрии информации?
5. Угрозы безопасности информационных и телекоммуникационных средств и сис тем?
6. Источники угроз информационной безопасности Российской Федерации?
7. К внешним источникам информационной безопасности Российской Федерации относятся?
8. К внутренним источникам информационной безопасности Российской Федера ции относятся?
9. Угрозы информационной безопасности для автоматизированных систем обра ботки информации (АСОИ)?
10. Уязвимость основных структурно-функциональных элементов распределенных АСОИ?
11. Основные виды угроз безопасности субъектов информационных отношений?
12. Классификация угроз безопасности информации?
13. Естественные угрозы информации это?
14. Искусственные угрозы информации это?
15. Непреднамеренные угрозы информации это?
16. Преднамеренные угрозы информации это?
17. Основные непреднамеренные искусственные угрозы?
18. Основные преднамеренные искусственные угрозы?
19. классификация каналов проникновения в систему и утечки информации?
20. Неформальная модель нарушителя в АС?
21. Удаленные атаки на интрасети?
22. Что принято понимать под удаленной атакой?
23. Классификация удаленных атак?

Вредоносные программы.

1. Какие программы являются вредоносными?
2. Условия существования вредоносных программ?
3. Причины появления вредных программ?
4. Классические компьютерные вирусы?
5. Способы заражения компьютерными вирусами?
6. Загрузочные вирусы?
7. Макро вирусы?
8. Сетевые черви?
9. Классификация сетевых червей?
10. - почтовые черви?
11. - черви, использующие интернет-пейджеры?
12. - черви в каналах?
13. - прочие сетевые черви?

14. - черви для файлообменных сетей?
15. Троянские программы?
16. Классификация троянских программ?
17. - троянские утилиты удаленного администрирования?
18. воровство паролей?
19. - интернет-кликеры?
20. — доставка вредоносных программ?
21. инсталляторы вредоносных программ?
22. - троянские прокси-сервера?
23. - шпионские программы?
24. прочие троянские программы?
25. сокрытие присутствия в операционной системе?
26. «бомбы» в архивах?
27. оповещение об успешной атаке?
28. Спам?
29. Основные виды спама?
30. Хакерские утилиты и прочие вредоносные программы?
31. Основные виды хакерских утилит и прочих вредоносных программ?
32. сетевые атаки?
33. - взломщики удаленных компьютеров?
34. «замусоривание» сети?
35. конструкторы вирусов и троянских программ?
36. - фатальные сетевые атаки?
37. - злые шутки, введение пользователя в заблуждение?
38. - скрытие от антивирусных программ?
39. - полиморфные генераторы?

Защита от компьютерных вирусов.

1. Признаки заражения компьютера?
2. Косвенные признаки заражения компьютера?
3. Действия при появлении признаков заражения вредоносной программой?
4. Источники компьютерных вирусов?
5. Глобальные сети и электронная почта как источник компьютерных вирусов?
6. Электронные конференции как источник компьютерных вирусов?
7. Локальные сети как источник компьютерных вирусов?
8. Пиратское программное обеспечение как источник компьютерных вирусов?
9. Компьютеры общего пользования как источник компьютерных вирусов?
10. Ремонтные службы как источник компьютерных вирусов?
11. Основные правила защиты от компьютерных вирусов?
12. Антивирусные программы?
13. Виды антивирусных программ?
14. Типовой перечень функций, которые способны выполнять антивирусные про граммы?
15. К наиболее мощным и популярным на сегодняшний день в России антивирус ным пакетам относятся?
16. Принцип работы антивирусного сканера?
17. Принцип работы антивирусных программ-детекторов?
18. Принцип работы антивирусных программ-докторов (фагов)?
19. Принцип работы антивирусных программ-ревизоров?
20. Принцип работы антивирусных программ-фильтров (сторожей)?
21. Принцип работы вакцинаторов (иммунизаторов)?

Методы и средства защиты компьютерной информации.

1. Методы обеспечения информационной безопасности Российской Федерации?
2. Правовые методы обеспечения информационной безопасности Российской Федерации?
3. Организационно - техническими методами обеспечения информационной безопасности Российской Федерации?
4. Экономические методы обеспечения информационной безопасности Российской Федерации?
5. Основные меры по обеспечению информационной безопасности Российской Федерации в сфере экономики?
6. Наиболее важные объекты обеспечения информационной безопасности Российской Федерации в области науки и техники?
7. Ограничение доступа как метод обеспечения информационной безопасности?
8. Биометрические методы аутентификации человека?
9. Статистика применения биометрических технологий?
10. Отпечатки пальцев как биометрическая характеристика идентификации человека?
11. Глаза как биометрическая характеристика идентификации человека?
12. Лицо как биометрическая характеристика идентификации человека?
    - Ладонь как биометрическая характеристика идентификац
14. Динамические характеристики как биометрическая характеристика идентификации человека?
15. Классификация систем тревожной сигнализации?
16. Контроль доступа к аппаратуре как метод обеспечения информационной безопасности?
17. Разграничение и контроль доступа к информации как метод обеспечения информационной безопасности?
18. Предоставление привилегий на доступ как метод обеспечения информационной безопасности?
19. Идентификация и установление подлинности объекта (субъекта)?
20. Объекты идентификации и установления подлинности в АСОИ?
21. Идентификация и установление подлинности личности?
22. Идентификация и установление подлинности технических средств?
23. Идентификация и установление подлинности документов?
24. Идентификация и установление подлинности информации на средствах ее отображения и печати?
25. Защита информации от утечки за счет побочного электромагнитного излучения и наводок?
26. Методы и средства защиты информации от побочного электромагнитного излучения и наводок информации?
27. Методы и средства защиты информации от случайных воздействий?
28. Методы защиты информации от аварийных ситуаций?
29. Организационные мероприятия по защите информации?
30. Организация информационной безопасности компании?
31. Выбор средств информационной информации?
32. Информационное страхование?

Криптографические методы информационной безопасности.

1. Криптографические методы информационной безопасности?
2. Классификация методов криптографического закрытия информации?

3. Чем занимается наука криптология?
4. Что такое криптоанализ?
5. Стойкость криптографического метода это?
6. Трудоемкость криптографического метода это?
7. Основные требования к криптографическому закрытию информации?
8. Шифрование это?
9. Классификация криптосистем?
10. Симметричные криптосистемы?
11. Классификация симметричных криптосистем?
12. Шифрование методом замены (подстановки)?
13. Одноалфавитная подстановка?
14. Многоалфавитная одноконтурная обыкновенная подстановка?
15. Многоалфавитная одноконтурная монофоническая подстановка?
16. Многоалфавитная многоконтурная подстановка?
17. Шифрование методом перестановки?
18. Шифрование методом гаммирования?
19. Шифрование с помощью аналитических преобразований?
20. Комбинированные методы шифрования?
21. Криптосистемы с открытым ключом (асимметричные)?
22. Характеристики существующих шифров?
23. Кодирование это?
24. Стеганография это?
25. Основные правила криптозащиты?
26. Основные правилами механизма распределения ключей?
27. Электронная цифровая подпись?
28. Технология электронной цифровой подписи?
29. Электронный документ это?
30. Электронная цифровая подпись это?
31. Владелец сертификата ключа подписи это?
32. Средства электронной цифровой подписи это?
33. Сертификат средств электронной цифровой подписи это?
34. Закрытый ключ электронной цифровой подписи это?
35. Открытый ключ электронной цифровой подписи это?
36. Сертификат ключа подписи это?
37. Подтверждение подлинности электронной цифровой подписи в электронном до кументе это?
38. Пользователь сертификата ключа подписи это?
39. Информационная система общего пользования это?
40. Корпоративная информационная система это?

Критерии безопасности компьютерных систем.

1. Критерии безопасности компьютерных систем?
2. Оранжевая книга это?
3. Какие определены в Оранжевой книге группы фундаментальных требований?
4. Требования группы фундаментальных требований Оранжевой книги «Страте гия»?
5. Требования группы фундаментальных требований Оранжевой книги «Подотчет ность»?
6. Требования группы фундаментальных требований Оранжевой книги «Гаран

тии»?

7. На какие группы разделяются автоматизированные системы в Оранжевой книге?
8. Краткая характеристика классов в Оранжевой книге?
9. Основным недостаткам Оранжевой книги?
10. Какие руководящие документы Гостехкомиссии?
11. Руководящий документ «Автоматизированные системы. Защита от несанкцио нированного доступа к информации. Классификация автоматизированных сис тем и требования по защите информации»?

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Лекции оцениваются по посещаемости, активности, умению выделить главную мысль.

Практические занятия оцениваются по самостоятельности выполнения работы, грамотности в оформлении, правильности выполнения.

Самостоятельная работа оценивается по качеству и количеству выполненных домашних работ, грамотности в оформлении, правильности выполнения.

Промежуточная аттестация проводится в форме зачета и экзамена.

Критерии оценки экзамена в тестовой форме: количество баллов или удовлетворительно, хорошо, отлично. Для получения соответствующей оценки на зачете и экзамене по курсу используется накопительная система балльно-рейтинговой работы студентов. Итоговая оценка складывается из суммы баллов или оценок, полученных по всем разделам курса и суммы баллов полученной на зачете или экзамене.

Таблица 4.1 – Критерии оценки уровня знаний студентов с использованием теста на экзамене по учебной дисциплине

Оценка	Характеристики ответа студента
Отлично	86-100 % правильных ответов
Хорошо	71-85 %
Удовлетворительно	51- 70%
Неудовлетворительно	Менее 51 %

Оценка «зачтено» соответствует критериям оценок от «отлично» до «удовлетворительно».

Оценка «не зачтено» соответствует критерию оценки «неудовлетворительно».
Количество баллов и оценка неудовлетворительно, удовлетворительно, хорошо, отлично определяются программными средствами по количеству правильных ответов к количеству случайно выбранных вопросов.

Критерии оценивания компетенций следующие:

1. Ответы имеют полные решения (с правильным ответом). Их содержание свидетельствует об уверенных знаниях обучающегося и о его умении решать профессиональные задачи, оценивается в 5 баллов (отлично);
2. Более 75 % ответов имеют полные решения (с правильным ответом). Их содержание свидетельствует о достаточных знаниях обучающегося и его умении решать профессиональные задачи – 4 балла (хорошо);
3. Не менее 50 % ответов имеют полные решения (с правильным ответом) Их содержание свидетельствует об удовлетворительных знаниях обучающегося и о его ограниченном умении решать профессиональные задачи, соответствующие его будущей квалификации – 3 балла (удовлетворительно);
4. Менее 50 % ответов имеют решения с правильным ответом. Их содержание свидетельствует о слабых знаниях обучающегося и его неумении решать профессиональные задачи – 2 балла (неудовлетворительно.

Критерии оценки уровня усвоения знаний, умений и навыков по результатам экзамена в устной форме:

Оценка «отлично» выставляется, если дан полный, развернутый ответ на поставленный теоретический вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Уме-

ет тесно увязывать теорию с практикой. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью "наводящих" вопросов преподавателя.

Оценка «хорошо» выставляется, если дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен. Ответы на дополнительные вопросы логичны, однако допущены незначительные ошибки или недочеты, исправленные студентом с помощью "наводящих" вопросов преподавателя.

Оценка «удовлетворительно» выставляется, если дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, вследствие непонимания студентом их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции. При ответе на дополнительные вопросы студент начинает понимать связь между знаниями только после подсказки преподавателя.

Оценка «неудовлетворительно» выставляется, если студент испытывает значительные трудности в ответе на экзаменационные вопросы. Присутствует масса существенных ошибок в определениях терминов, понятий, характеристике фактов. Речь неграмотна. На дополнительные вопросы студент не отвечает.

Оценка «зачтено» соответствует критериям оценок от «отлично» до «удовлетворительно».

Оценка «не зачтено» соответствует критерию оценки «неудовлетворительно».

Критерии оценки при решении задач: оценка «отлично» выставляется студенту, если он, решил задачу верно, пришел к верному знаменателю, показал умение логически и последовательно аргументировать решение задачи во взаимосвязи с практической действительностью. Оценка хорошо ставится в том случае если задача решена верно, но с незначительными погрешностями, неточностями. Оценка удовлетворительно ставится если соблюдена общая последовательность выполнения задания, но сделаны существенные ошибки в расчетах. Оценка неудовлетворительно ставится если задача не выполнена.

Практические занятия оцениваются по самостоятельности выполнения работы, активности работы в аудитории, правильности выполнения заданий, уровня подготовки к занятиям.

Самостоятельная работа оценивается по качеству и количеству выполненных домашних работ, грамотности в оформлении, правильности выполнения.

Критерии оценки контрольных работ студентов заочного обучения:

«Зачтено» ставится если контрольная работа выполнена в срок, не требует дополнительного времени на завершение; контрольная работа выполнена полностью: решены все задачи, даны ответы на все вопросы, имеющиеся в контрольной работе; без дополнительных пояснений используются знания, полученные при изучении дисциплин; даны ссылки на источники информации и ресурсы сети Интернет, использованные в работе; контрольная работа аккуратно оформлена, соблюдены требования ГОСТов;

«Не зачтено» ставится если контрольная работа не выполнена в установленный срок, продемонстрировано полное безразличие к работе, требуется постоянная консультация для выполнения задания; в контрольной работе присутствует большое число ошибок; не полностью или с ошибками решены задачи, даны неполные или неправильные ответы на поставленные вопросы; отсутствуют ссылки на источники информации и ресурсы сети Интернет, использованные в работе; контрольная работа выполнена с нарушениями требований ГОСТов; контрольная работа выполнена по неправильно выбранному варианту.