Приложение 4.22

Министерство сельского хозяйства Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный аграрный университет»

Факультет экономики и управления в АПК
Кафедра прикладной информатики, статистики и математики

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
текущего контроля/промежуточной аттестации обучающихся при освоении ОПОП ВО, реализующей ФГОС ВО

по дисциплине
«*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»

Уровень высшего образования
БАКАЛАВРИАТ

Направление подготовки
09.03.03 Прикладная информатика

Направленность (профиль) образовательной программы
Информационные технологии в агробизнесе

Очная форма обучения

Санкт-Петербург
2023

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Таблица 1

№	Формируемые компетенции	Контролируемые разделы (темы) дисциплины	Оценочное средство
1.	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Уметь: демонстрировать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Владеть: навыками демонстрировать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Раздел 1. Обеспечение информационной безопасности Раздел 2. Стандарты и специфики в области информационной безопасности Раздел 3. Аппаратные и программные средства защиты компьютерной информации	Коллоквиум Реферат/доклад Устный опрос Контрольная работа ТЕСТ
2.	ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.		

	Знать: основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы Уметь: демонстрировать знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы Владеть: навыками демонстрировать знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы		

2. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

Таблица 2

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1.	Коллоквиум	Форма контроля, важная при формировании универсальных компетенций обучающегося, при развитии навыков самостоятельного творческого мышления и письменного изложения собственных умозаключений на основе изученного или прочитанного материала	Вопросы по темам/разделам дисциплины
2.	Реферат/ доклад	Форма контроля, используемая для привития студенту навыков краткого, грамотного и лаконичного представления собранных материалов и фактов в соответствии с требованиями	Вопросы по темам/разделам дисциплины
3.	Устный опрос	Средство для проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект вопросов
4.	Контрольная работа	Средство для проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Комплект контрольных заданий по вариантам

5	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося	Фонд тестовых заданий

3. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Таблица 3

Планируемые результаты освоения компетенции	**Уровень освоения**				**Оценочное средство**
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**	
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности					
ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности					
Знать решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Уровень знаний ниже минимальных требований, имели место грубые ошибки	Минимально допустимый уровень знаний, допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Реферат, Доклад, Коллоквиум Контрольная работа
Уметь демонстрировать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	При решении стандартных задач не продемонстрированы основные умения, имели место грубые ошибки	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Реферат, Доклад, Коллоквиум Контрольная работа
Владеть навыками демонстрировать принципы, методы и средства решения стандартных задач профессиональной деятельности на	При решении стандартных задач не продемонстриров	Имеется минимальный набор навыков для решения стандартных	Продемонстрированы базовые навыки при решении стандартных задач с	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Реферат, Доклад, Коллоквиум

основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	аны базовые навыки, имели место грубые ошибки	задач с некоторыми недочетами	некоторыми недочетами		Контрольная работа
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью					
ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.					
Знать основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы	Уровень знаний ниже минимальных требований, имели место грубые ошибки	Минимально допустимый уровень знаний, допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Реферат, Доклад, Коллоквиум Контрольная работа
Уметь демонстрировать знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы	При решении стандартных задач не продемонстрированы основные умения, имели место грубые ошибки	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Реферат, Доклад, Коллоквиум Контрольная работа
Владеть навыками демонстрировать знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы	При решении стандартных задач не продемонстрированы базовые навыки, имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Реферат, Доклад, Коллоквиум

4. ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ЗАДАНИЙ И ИНЫХ МАТЕРИАЛОВ, НЕОБХОДИМЫХ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ

4.1. Типовые задания для текущего контроля успеваемости

4.1.1. Вопросы для коллоквиума

Вопросы для оценки компетенции

Тема 1. Обеспечение информационной безопасности.

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.

Знать:

1. Содержание и структуру правового обеспечения.
2. Содержание и структуру законодательства.
3. Термины и определения в области защиты информации.
4. Задачи органов Государственной системы защиты информации.
5. Руководящие документы и методические указания в сфере защиты информации.
6. Цели и задачи защиты информации.
7. Руководящие документы и методические указания в сфере защиты информации
8. Виды угроз информационных систем и методы обеспечения информационной безопасности

Уметь:

1. Использовать Нормативно-методические документы по обеспечению безопасности информации.
2. Проводить служебные расследования.
3. Организовывать подготовку кадров и повышения квалификации в области обеспечения информационной безопасности.
4. Разрабатывать и внедрять системы управления информационной безопасности.
5. Создавать и оценивать информационную систему персональных данных.

Владеть:

1. Принципами обработки персональных данных
2. Навыками самостоятельного информационно-коммуникационных технологий с учетом основных правил защиты информации.
3. Опытом использования основы знаний в системе правовой охраны информации.
4. навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах.
5. Навыками управления информационной безопасностью.

Тема 2. Стандарты и специфики в области информационной безопасности.

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.

Знать:

1. Основные правила защиты информации
2. Основы использования нормативно-правовых актов в сфере защиты информации;
3. Организацию работы и нормативные правовые акты по сертификации средств защиты информации.
4. Организацию работы подразделений (служб) обеспечения информационной безопасности
5. Стандарты в области информационной безопасности;

Уметь:

1. Проводить оценку работоспособности программного продукта
2. Создавать резервные копии программ и данных
3. Выполнять восстановление, обеспечивать целостность программного продукта и данных
4. Оценивать и выбирать необходимые средства защиты;
5. Осуществлять мониторинг состояния информационной безопасности объекта;
6. Обеспечивать противодействие атакам на информационную систему;
7. Выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности;

Владеть:

1. Навыками определения актуальности нормативно-правовой документации в профессиональной деятельности.
2. Информацией о технических спецификациях, регламентирующих различные аспекты реализации средств защиты.
3. Информацией об оценочных стандартах, направленных на классификацию информационных систем и средств защиты по требованиям безопасности
4. Навыками разработки и внедрение системы управления информационной безопасности.

Тема 3. Аппаратные и программные средства защиты компьютерной информации.

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.

Знать:

1. Современные средства и устройства информатизации;
2. Порядок применения и программное обеспечение в профессиональной деятельности современных средств и устройств информатизации.
3. Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
4. Типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
5. Основные понятия криптографии и типовых криптографических методов и средств защиты информации

Уметь:

1. Применять средства информационных технологий для решения профессиональных задач;
2. Применять программные и программно-аппаратные средства для защиты информации в базах данных;
3. Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
4. Применять математический аппарат для выполнения криптографических преобразований;

5. Определять классы угроз информационной безопасности.
6. Осуществлять криптографическую защиту данных

Владеть:

1. Навыками решения задач защиты от несанкционированного доступа к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;
2. Навыками организации и обеспечения режима секретности.
3. Навыками проведения категорирования объектов на предприятии.
4. Навыками сертификации и аттестации средств защиты информации.
5. Навыками защиты конфиденциальной информации

4.1.2. Темы контрольных работ

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.

Знать

1. Теоретические и концептуальные основы защиты информации.
2. Принципы защиты информации.
3. Цели и значение защиты информации.
4. Задачи защиты информации и функции по их реализации.
5. Виды, методы и средства защиты информации.
6. Кадровое и ресурсное обеспечение защиты информации.
8. Источники дестабилизирующего воздействия на информацию.

Уметь

1. Понятие утечки информации, виды и причины утечки информации.
2. Каналы утечки информации ограниченного доступа.
3. Аналитическая работа по предотвращению утраты и утечки информации.
4. Современные подходы к понятию угрозы защищаемой информации.
5. Объекты защиты информации.
6. Структура системы защиты информации, назначение составных частей системы.

7. Понятие «носитель защищаемой информации». Соотношение между носителем и источником информации.

Владеть

1. Состав и классификация носителей защищаемой информации.
2. Понятие и назначение технологического обеспечения защиты информации.
3. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.
4. Полномочия руководства предприятия в области защиты информации.
5. Полномочия специальных комиссий по защите информации.
6. Полномочия пользователей защищаемой информации.

4.1.3. Примерные темы курсовых работ

«Курсовые работы не предусмотрены в РПД»)

4.1.4. Темы реферата, доклада

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Виды защищаемой информации.
4. Основные понятия и общеметодологические принципы теории информационной безопасности.
5. Роль информационной безопасности в обеспечении национальной безопасности государства.
6. Интересы личности в информационной сфере.
7. Интересы общества в информационной сфере.
8. Интересы государства в информационной сфере.
9. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

10. Направления обеспечения информационной безопасности государства.
11. Проблемы региональной информационной безопасности.
12. Уровни ведения информационной войны. Информационные операции. Психологические операции.
13. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
14. Основные положения государственной информационной политики Российской Федерации.
15. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
16. Виды защищаемой информации в сфере государственного и муниципального управления.
17. Обеспечение информационной безопасности организации.
18. Характеристика эффективных стандартов по безопасности.
19. Преступления в сфере компьютерной информации
20. Системы обнаружения атак. (Анализаторы сетевых протоколов и сетевые мониторы)

Комплект тестов

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1.	К негативным последствиям развития современных информационных и коммуникационных технологий можно отнести:	
	А)	формирование единого информационного пространства
	Б)	работа с информацией становится главным содержанием профессиональной деятельности
	В)	организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации
	Г)	широкое использование информационных технологий во всех сферах человеческой деятельности
	Д)	доступность личной информации для общества и государства, вторжение информационных технологий в частную жизнь людей
2.	Термин «информатизация общества» обозначает:	
	А)	целенаправленное и эффективное использование информации во всех областях человеческой деятельности на основе современных информационных и коммуникационных технологий
	Б)	увеличение избыточной информации, циркулирующей в обществе
	В)	увеличение роли средств массовой информации
	Г)	введение изучения информатики во все учебные заведения страны
	Д)	организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации

3.	Развитый рынок информационных продуктов и услуг, изменение в структуре экономики, массовое использование информационных и коммуникационных технологий являются признаками:	
	А)	информационной культуры
	Б)	высшей степени развития цивилизации
	В)	информационного кризиса
	Г)	информационного общества
	Д)	информационной зависимости
4.	Методы обеспечения информационной безопасности делятся (указать неправильные ответ):	
	А)	правовые
	Б)	организационно-технические
	В)	политические
	Г)	экономические
	Д)	все перечисленные выше
5.	Обеспечение защиты информации проводится конструкторами и разработчиками программного обеспечения в следующих направлениях (указать неправильный ответ):	
	А)	защита от сбоев работы оборудования
	Б)	защита от случайной потери информации
	В)	защита от преднамеренного искажения
	Г)	разработка правовой базы для борьбы с преступлениями в сфере информационных технологий
	Д)	защита от несанкционированного доступа к информации
6.	Компьютерные вирусы – это:	
	А)	вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера
	Б)	программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК
	В)	программы, являющиеся следствием ошибок в операционной системе
	Г)	пункты А) и В)
	Д)	вирусы, сходные по природе с биологическими вирусами
7.	Отличительными особенностями компьютерного вируса являются:	
	А)	значительный объем программного кода
	Б)	способность к самостоятельному запуску и многократному копированию кода
	В)	способность к созданию помех корректной работе компьютера
	Г)	легкость распознавания
	Д)	Пункты Б) и В)
8.	Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?	
	А)	Уголовный кодекс РФ
	Б)	Гражданский кодекс РФ
	В)	Доктрина информационной безопасности РФ
	Г)	Постановления Правительства
	Д)	Указ Президента РФ
9.	Что не относится к объектам информационной безопасности Российской Федерации?	
	А)	природные и энергетические ресурсы
	Б)	информационные ресурсы всех видов
	В)	информационные системы различного класса и назначения, информационные технологии

	Г)	система формирования общественного сознания
	Д)	права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности
10.	Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?	
	А)	Неправомерный доступ к компьютерной информации
	Б)	Создание, использование и распространение вредоносных программ для ЭВМ
	В)	Умышленное нарушение правил эксплуатации ЭВМ и их сетей
	Г)	Все перечисленное выше
	Д)	Пункты Б) и В)
11.	Какой законодательный акт регламентирует отношения в области защиты авторских и имущественных прав в области информатизации?	
	А)	Доктрина информационной безопасности РФ
	Б)	Закон «О правовой охране программ для ЭВМ и баз данных»
	В)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Г)	Указ Президента РФ
	Д)	Закон «Об информации, информатизации и защите информации»
12.	Какой законодательный акт регулирует отношения в области защиты информационных ресурсов (личных и общественных) от искажения, порчи и уничтожения?	
	А)	Закон «Об информации, информатизации и защите информации»
	Б)	Закон «О правовой охране программ для ЭВМ и баз данных»
	В)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Г)	Пункты А) и В)
	Д)	Указ Президента РФ
13.	Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан:	
	А)	Указ Президента РФ
	Б)	Закон «Об информации, информатизации и защите информации»
	В)	Закон «О правовой охране программ для ЭВМ и баз данных»
	Г)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Д)	Доктрина национальной безопасности РФ
14.	Для написания самостоятельной работы Вы скопировали из Интернет полный текст нормативно-правового акта. Нарушили ли Вы при этом авторское право?	
	А)	да, нарушено авторское право владельца сайта
	Б)	нет, так как нормативно-правовые акты не являются объектом авторского права
	В)	нет, если есть разрешение владельца сайта
	Г)	да, нарушено авторское право автора документа
	Д)	нет, если истек срок действия авторского права
15.	Можно ли разместить на своем сайте в Интернет опубликованную в печати статью какого-нибудь автора?	
	А)	можно, с указанием имени автора и источника заимствования
	Б)	можно, с разрешения и автора статьи, и издателя
	В)	можно, но исключительно с ведома автора и с выплатой ему авторского вознаграждения
	Г)	можно, поскольку опубликованные статьи не охраняются авторским правом
	Д)	можно, с разрешения издателя, издавшего данную статью, или автора статьи

16.	Что необходимо указать при цитировании статьи, размещенной на чьем-то сайте?	
	А)	имя автора, название статьи, адрес сайта, с которого заимствована статья
	Б)	адрес сайта и имя его владельца
	В)	имя автора и название статьи
	Г)	электронный адрес сайта, с которого заимствована статья
	Д)	название статьи и название сайта
17.	Можно ли использовать статьи из разных журналов и газет на политические, экономические, религиозные или социальные темы для подготовки с их использованием учебного материала?	
	А)	нет
	Б)	да, получив согласие правообладателей
	В)	да, указав источники заимствования
	Г)	да, не спрашивая согласия правообладателей, но с обязательным указанием источника заимствования и имен авторов
	Д)	да, указав ФИО авторов и название статей
18.	Считается ли статья, обнародованная в Интернет, объектом авторского права?	
	А)	нет, если статья впервые обнародована в сети Интернет
	Б)	да, при условии, что эта же статья в течение 1 года будет опубликована в печати
	В)	да, так как любая статья является объектом авторского права как произведение науки или литературы
	Г)	да, если указан год первого опубликования
	Д)	да, если автор использует знак охраны авторского права
19.	В каких случаях при обмене своими компьютерными играми с другими людьми, не будут нарушаться авторские права?	
	А)	если экземпляры этих компьютерных игр были выпущены в свет и введены в гражданский оборот с согласия автора
	Б)	если обладатели обмениваемых экземпляров компьютерных игр приобрели их по договору купли-продажи/мены
	В)	если одновременно соблюдены условия, указанные в пунктах А) и Б)
	Г)	если они распространяются путем сдачи в прокат
	Д)	если автору выплачивается авторское вознаграждение
20.	В каких случаях правомерно используются фотографии из коллекции одного из Интернет-сайтов для иллюстрирования своего материала, подготавливаемого в образовательных целях?	
	А)	если тематика фото-сюжетов соответствует теме всего материала
	Б)	в любом случае, т.к. факт размещения фотографии в Интернет означает согласие автора на ее дальнейшее свободное использование
	В)	если такое использование прямо разрешено правилами Интернет-сайта
	Г)	если фотографии размещены на сайте Интернет с согласия их авторов
	Д)	Если соблюдаются условия В) и Г)
21	Информационная безопасность зависит от:	
	А)	компьютеров, поддерживающей инфраструктуры +
	Б)	пользователей
	В)	информации
22	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 +
23	Для чего создаются информационные системы:	

	А)	получения определенных информационных услуг +
	Б)	обработки информации
	В)	оба варианта верны
24	Кто является основным ответственным за определение уровня классификации информации:	
	А)	руководитель среднего звена
	Б)	владелец +
	В)	высшее руководство
25	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:	
	А)	Хакеры
	Б)	контрагенты
	В)	сотрудники +
26	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:	
	А)	снизить уровень классификации этой информации
	Б)	улучшить контроль за безопасностью этой информации +
	В)	требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
27	Что самое главное должно продумать руководство при классификации данных:	
	А)	управление доступом, которое должно защищать данные
	Б)	оценить уровень риска и отменить контрмеры
	В)	необходимый уровень доступности, целостности и конфиденциальности +
28	Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:	
	А)	владельцы данных
	Б)	руководство +
	В)	администраторы
29	Процедурой называется:	
	А)	пошаговая инструкция по выполнению задачи +
	Б)	обязательные действия
	В)	руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
30		Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:
	А)	проведение тренингов по безопасности для всех сотрудников
	Б)	поддержка высшего руководства +
	В)	эффективные защитные меры и методы их внедрения
31	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:	
	А)	когда риски не могут быть приняты во внимание по политическим соображениям
	Б)	для обеспечения хорошей безопасности нужно учитывать и снижать все риски
	В)	когда стоимость контрмер превышает ценность актива и потенциальные потери +
32	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

33	Какая из приведенных техник является самой важной при выборе конкретных защитных мер:	
	А)	анализ рисков
	Б)	результаты ALE
	В)	анализ затрат / выгоды +
34	Что лучше всего описывает цель расчета ALE:	
	А)	количественно оценить уровень безопасности среды
	Б)	оценить потенциальные потери от угрозы в год +
	В)	количественно оценить уровень безопасности среды
35	Тактическое планирование:	
	А)	среднесрочное планирование +
	Б)	ежедневное планирование
	В)	долгосрочное планирование
36	Эффективная программа безопасности требует сбалансированного применения:	
	А)	контрмер и защитных механизмов
	Б)	процедур безопасности и шифрования
	В)	технических и нетехнических методов +
37	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
38	Что из перечисленного не является целью проведения анализа рисков:	
	А)	выявление рисков
	Б)	делегирование полномочий +
	В)	количественная оценка воздействия потенциальных угроз
39	Кто является основным ответственным за определение уровня классификации информации?	
	А)	Руководитель среднего звена
	Б)	Высшее руководство
	В)	Владелец+
	Г)	Пользователь
40	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	
	А)	Сотрудники+
	Б)	Хакеры
	В)	Атакующие
	Г)	Контрагенты (лица, работающие по договору)

ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий

+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных
тест_20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальностьl
23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой
25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети
27) Политика безопасности в системе (сети) – это комплекс:
+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети
28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций
29) Основная масса угроз информационной безопасности приходится на:
а) Троянские программы +
б) Шпионские программы
в) Черви
30. Какой вид идентификации и аутентификации получил наибольшее распространение:
а) системы PKI
б) постоянные пароли +
в) одноразовые пароли
31. Под какие системы распространение вирусов происходит наиболее динамично:
а) Windows
б) Mac OS
в) Android +
32. Заключительным этапом построения системы защиты является:
а) сопровождение +
б) планирование
в) анализ уязвимых мест
33. Какие угрозы безопасности информации являются преднамеренными:
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ +
34. Какой подход к обеспечению безопасности имеет место:
а) теоретический
б) комплексный +
в) логический
35. Системой криптографической защиты информации является:
а) BFox Pro
б) CAudit Pro
в) Крипто Про +
36. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы +
б) троянцы
в) черви
37. Stuxnet — это:
а) троянская программа
б) макровирус
в) промышленный вирус +
38. Таргетированная атака — это:

а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия +
в) атака на конкретный компьютер пользователя
39. 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
40. 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

20.1. Типовые задания для промежуточной аттестации

4.2.1. Вопросы к зачету

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3 ИОПК-3.1. Демонстрирует знание принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ОПК-4 ИОПК-4.1. Демонстрирует знание основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной

Знать:

1. Кто является основным ответственным за определение уровня классификации информации?
2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
3. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
4. Что такое процедура?

5. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
6. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
7. Что такое политики безопасности?
8. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
9. Что является определением воздействия (exposure) на безопасность?
10. Как рассчитать остаточный риск?
11. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
12. Защита информации это?
13. Естественные угрозы безопасности информации вызваны:
14. Искусственные угрозы безопасности информации вызваны:

Уметь:

1. Что понимают под набором норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации?
2. В каких шифрах в качестве ключа используют таблицы?
3. Самый первый шифр перестановки?
4. В каком шифре каждая буква заменялась на другую букву того же алфавита по следующему правилу: заменяющая буква определялась путем смещения по алфавиту от исходной буквы на К букв?
5. Какой шифр основан на подсчете частот появления букв в шифртексте?
6. Какой шифр сложной замены представляет собой модификацию шифра Цезаря числовым ключом?
7. Какой шифр сложной замены описывается таблицей шифрования, и где ключ шифрования меняется от буквы к букве?
8. Какой шифр является абсолютно надежным?

Владеть:

1. Способы несанкционированного доступа
2. Технические средства несанкционированного доступа к информации
3. Защита от наблюдения и фотографирования
4. Защита от подслушивания
5. Противодействие незаконному подключению к линиям связи
6. Направления взаимодействия с зарубежными партнерами
7. Организация работы с зарубежными партнерами
8. Научно-техническое сотрудничество с зарубежными партнерами
9. Научно-техническое сотрудничество. Технологический обмен и его регулирование.
10. Виды коммерческих международных операций
11. Научно-техническая документация - источник конфиденциальной информации

12. Возможные условия разглашения сведений, составляющих коммерческую тайну
13. Экспертиза ценности передаваемой научно-технической документации
14. Порядок защиты конфиденциальной информации при работе с зарубежными партнерами

4.2.2. Вопросы к экзамену

«Экзамен не предусмотрен учебным планом»)

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Критерии оценивания знаний обучающихся при проведении коллоквиума:

- **Отметка «отлично»** - обучающийся четко выражает свою точку зрения по рассматриваемым вопросам, приводя соответствующие примеры.
- **Отметка «хорошо»** - обучающийся допускает отдельные погрешности в ответе.
- **Отметка «удовлетворительно»** - обучающийся обнаруживает пробелы в знаниях основного учебного и нормативного материала.
- **Отметка «неудовлетворительно»** - обучающийся обнаруживает существенные пробелы в знаниях основных положений дисциплины, неумение с помощью преподавателя получить правильное решение конкретной практической задачи.

Критерии оценивания знаний обучающихся при проведении тестирования:

Результат тестирования оценивается по процентной шкале оценки. Каждому обучающемуся предлагается комплект тестовых заданий из 25 вопросов:

- **Отметка «отлично»** – 25-22 правильных ответов.
- **Отметка «хорошо»** – 21-18 правильных ответов.
- **Отметка «удовлетворительно» –** 17-13 правильных ответов.
- **Отметка «неудовлетворительно»** – менее 13 правильных ответов.

Критерии знаний при проведении зачета:

- **Оценка «зачтено»** должна соответствовать параметрам любой из положительных оценок («отлично», «хорошо», «удовлетворительно»).
- **Оценка «не зачтено»** должна соответствовать параметрам оценки «неудовлетворительно».
- **Отметка «отлично»** – выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

• **Отметка «хорошо»** – выполнены все виды учебной работы, предусмотренные учебным планом. Обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, оперирует приобретенными знаниями, умениями, навыками, применяет их в стандартных ситуациях. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

• **Отметка «удовлетворительно»** – не выполнен один или более видов учебной работы, предусмотренных учебным планом. Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется частичное отсутствие знаний, умений, навыков по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

• **Отметка «неудовлетворительно»** – не выполнены виды учебной работы, предусмотренные учебным планом. демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по большему ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

6. ДОСТУПНОСТЬ И КАЧЕСТВО ОБРАЗОВАНИЯ ДЛЯ ЛИЦ С ОВЗ

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачете.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья могут использоваться собственные технические средства.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:	– в печатной форме увеличенным шрифтом, – в форме электронного документа.
Для лиц с нарушениями слуха:	– в печатной форме, – в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата	– в печатной форме, аппарата: – в форме электронного документа.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивает выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются преподавателем);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.