Федеральное государственное бюджетное образовательное учреждение высшего образования
«Бурятская государственная сельскохозяйственная академия имени В.Р. Филиппова»

Экономический факультет

СОГЛАСОВАНО
Заведующий выпускающей кафедрой
Информатика и информационные технологии в экономике

_____
уч. ст., уч. зв.

_____
ФИО

_____
подпись

«__» _____20__ г.

УТВЕРЖДАЮ
Декан экономического факультета

_____
уч. ст., уч. зв.

_____
ФИО

_____
подпись

«__» _____20__ г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

дисциплины (модуля)

Б1.В.20 Информационная безопасность

Направление подготовки
09.03.03 Прикладная информатика

Направленность (профиль)
Прикладная информатика в экономике АПК
бакалавр

Обеспечивающая преподавание дисциплины кафедра — Информатика и информационные технологии в экономике

Разработчик (и)

_____ _____ _____
подпись уч.ст., уч. зв. И.О.Фамилия

Внутренние эксперты:
Председатель методической комиссии экономического факультета

_____ _____ _____
подпись уч.ст., уч. зв. И.О.Фамилия

Заведующий методическим кабинетом УМУ

_____ _____
подпись И.О.Фамилия

Улан – Удэ, 2022

ВВЕДЕНИЕ

1. Оценочные материалы по дисциплине (модулю) является обязательным обособленным приложением к Рабочей программе дисциплины (модуля) и представлены в виде оценочных средств.

2. Оценочные материалы является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися указанной дисциплины (модуля).

3. При помощи оценочных материалов осуществляется контроль и управление процессом формирования обучающимися компетенций, из числа предусмотренных ФГОС ВО в качестве результатов освоения дисциплины (модуля.

4. Оценочные материалы по дисциплине (модулю) включает в себя:

- оценочные средства, применяемые при промежуточной аттестации по итогам изучения дисциплины (модуля).

- оценочные средства, применяемые в рамках индивидуализации выполнения, контроля фиксированных видов ВАРО;

- оценочные средства, применяемые для текущего контроля;

5. Разработчиками оценочных материалов по дисциплине (модулю) являются преподаватели кафедры, обеспечивающей изучение обучающимися дисциплины (модуля) в Академии. Содержательной основой для разработки оценочных материалов является Рабочая программа дисциплины (модуля).

1. ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ИЗУЧЕНИЯ
учебной дисциплины (модуля), персональный уровень достижения которых проверяется с использованием представленных в п. 3 оценочных материалов

Компетенции, в формировании которых задействована дисциплина		**Код и наименование индикатора достижений компетенции**	**Компоненты компетенций,** формируемые в рамках данной дисциплины (как ожидаемый результат ее освоения)		
код	наименование		знать и понимать	уметь делать (действовать)	владеть навыками (иметь навыки)
1		2	3	4	5
Профессиональные компетенции					
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	ИД-1$_{ОПК-3.1}$ Знает 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. ИД-2$_{ОПК-3.2}$ Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ИД-3$_{ОПК-3.3}$ Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Знает способы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Владеет навыками 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	ИД-1$_{ОПК-4.1}$ Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ИД-2$_{ОПК-4.2}$ Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ИД-3$_{ОПК-4.3}$ Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Знает способы участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Умеет участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Владеет навыками участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

РЕЕСТР
элементов оценочных материалов по дисциплине (модулю)

Группа оценочных средств	Оценочное средство или его элемент
	Наименование
1	2
1. Средства для промежуточной аттестации по итогам изучения дисциплины	Перечень вопросов к экзамену
	Критерии оценки к экзамену
2. Средства для индивидуализации выполнения, контроля фиксированных видов (ВАРО), включая самостоятельную работу	Не предусмотрено учебным планом
3. Средства для текущего контроля	Комплект контрольных вопросов для проведения устных опросов
	Критерии оценивания устных опросов
	Шкала оценивания устных опросов
	Комплект заданий для лабораторных работ
	Критерий оценивания лабораторных работ
	Шкала оценивания лабораторных работ
	Комплект заданий для самостоятельной работы обучающихся
	Критерии оценивания самостоятельной работы
	Шкала оценивания самостоятельной работы
	Кейс-задания
	Критерий оценивания кейс-задания
	Шкала оценивания кейс-задания
	Комплект тестовых заданий
	Критерии оценивания тестовых заданий
	Шкала оценивания тестовых заданий

3. Описание показателей, критериев и шкал оценивания компетенций в рамках дисциплины (модуля)

Код и название компетенции	Код индикатора достижений компетенции	Индикаторы компетенции	Показатель оценивания - знания, умения, навыки (владения)	Уровни сформированности компетенций				Формы и средства контроля формирования компетенций
				компетенция не сформирована	минимальный	средний	высокий	
				Оценки сформированности компетенций				
				2	3	4	5	
				Оценка «неудовлетворительно»	*Оценка «удовлетворительно»*	*Оценка «хорошо»*	*Оценка «отлично»*	
				Характеристика сформированности компетенции				
				Компетенция в полной мере не сформирована. Имеющихся знаний, умений и навыков недостаточно для решения практических (профессиональных) задач	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач	
1	2	3	4	5	6	7	8	9
Критерии оценивания								
ОПК-3. способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информацио	ИД-1$_{ОПК-3}$	Полнота знаний	Знает способы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	не знает способы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знает частично способы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знает достаточно хорошо способы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знает в полном объѐме способы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Перечень вопросов к зачету, комплект контрольных вопросов для проведения устных опросов, комплект заданий для лабораторных работ, комплект заданий для самостоятельной работы обучающихся, кейс-задания комплект тестовых заданий
	ИД-2$_{ОПК-3}$	Наличие умений	умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	не умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	умеет частично решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	умеет хорошо решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	умеет в полной мере решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	

нной безопасности			информационной безопасности	информационной безопасности	основных требований информационной безопасности	информационной безопасности	основных требований информационной безопасности	
		Наличие **навыков** (владение опытом)	Владеет навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	не владеет навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	владеет частично решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	владеет хорошо навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	владеет свободно навыками 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	ИД-1$_{ОПК-4}$	Полнота знаний	знает способы участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	не знает способы участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Знает частично способы участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	знает достаточно хорошо способы участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	знает в полном объѐме способы участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Перечень вопросов к зачету, комплект контрольных вопросов для проведения устных опросов, комплект заданий для лабораторных работ, комплект заданий для самостоятельной работы обучающихся, кейс-задания комплект тестовых заданий
	ИД-2$_{ОПК-4}$	Наличие умений	умеет участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	не умеет участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	умеет частично участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	умеет хорошо участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	умеет в полной мере участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	
	ИД-3$_{ОПК-4}$	Наличие навыков (владение опытом)	Владеет навыками участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	не владеет навыками участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	владеет частично навыками участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	владеет хорошо навыками участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	владеет свободно навыками участия в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	

4.Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

4.1. Типовые контрольные задания, необходимые для оценки знаний, умений, навыков
4.1.1. Средства для промежуточной аттестации по итога м изучения дисциплины

6.1 Нормативная база проведения промежуточной аттестации обучающихся по результатам изучения дисциплины: Б1.О.20 Информационная безопасность	
1) действующее «Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся ФГБОУ ВО Бурятская ГСХА»	
6.2 Основные характеристики промежуточной аттестации обучающихся по итогам изучения дисциплины	
1	2
Цель промежуточной аттестации -	установление уровня достижения каждым обучающимся целей и задач обучения по данной дисциплине, изложенным в п.2.2 настоящей программы
Форма промежуточной аттестации -	дифференцированный зачет
Место процедуры получения зачѐта в графике учебного процесса	1) участие обучающегося в процедуре получения зачѐта осуществляется за счѐт учебного времени (трудоѐмкости), отведѐнного на изучение дисциплины
	2) процедура проводится в рамках ВАРО, на последней неделе семестра
Основные условия получения обучающимся зачѐта:	1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине
Процедура получения зачѐта -	Представлены в оценочных материалах по данной дисциплине
Методические материалы, определяющие процедуры оценивания знаний, умений, навыков:	

Перечень вопросов к зачету с оценкой по дисциплине (модулю)

1. Основные предметные направления защиты информации. Составляющие информационной безопасности. (ОПК-3, ОПК-4)
2. Межсетевое экранирование (ОПК-3, ОПК-4)
3. Вирусы как угроза информационной безопасности (ОПК-3, ОПК-4)
4. Несанкционированный доступ. Понятие и классификация способов несанкционированного доступа к информации (ОПК-3, ОПК-4)
5. Политика безопасности информационных систем (ОПК-3, ОПК-4)
6. Способы защиты информации от случайных воздействий (ОПК-3, ОПК-4)
7. Нормативно-правовые основы информационной безопасности (ОПК-3, ОПК-4)
8. Технические средства защиты информации при ее обработке на средствах вычислительной техники (ОПК-3, ОПК-4)
9. Защита информации. Виды профессиональных тайн (ОПК-3, ОПК-4)
10. Основные каналы утечки информации (ОПК-3, ОПК-4)
11. Основные предметные направления защиты информации. Составляющие информационной безопасности. (ОПК-3, ОПК-4)
12. Вирусы как угроза информационной безопасности (ОПК-3, ОПК-4)
13. Несанкционированный доступ. Понятие и классификация способов несанкционированного доступа к информации (ОПК-3, ОПК-4)
14. Способы защиты информации от случайных воздействий (ОПК-3, ОПК-4)
15. Доктрина информационной безопасности Российской Федерации (ОПК-3, ОПК-4)
16. Технические средства защиты информации при ее обработке на средствах вычислительной техники (ОПК-3, ОПК-4)
17. Защита информации. Виды профессиональных тайн (ОПК-3, ОПК-4)
18. Основные каналы утечки информации (ОПК-3, ОПК-4)
19. Угрозы информационной безопасности Российской Федерации (ОПК-3, ОПК-4)
20. Криптография с закрытым ключом (ОПК-3, ОПК-4)
21. Основные виды угроз безопасности информации (ОПК-3, ОПК-4)
22. Информационная безопасность вычислительных сетей (ОПК-3, ОПК-4)
23. Электронно - цифровая подпись (ОПК-3, ОПК-4)
24. Классы защищенности автоматизированных систем от несанкционированного доступа (НСД) (ОПК-3, ОПК-4)
25. Информационная безопасность. Содержание понятия, существенные признаки понятия, объем понятия. (ОПК-3, ОПК-4)
26. Информационная безопасность вычислительных сетей (ОПК-3, ОПК-4)
27. Утечка информации. Каналы утечки информации (ОПК-3, ОПК-4)
28. Стандарты информационной безопасности (ОПК-3, ОПК-4)

29. Случайные угрозы безопасности информации. Классификация, происхождение, воздействие на информационную систему (ОПК-3, ОПК-4)
30. Использование схем защиты данных с использованием паролей (ОПК-3, ОПК-4)
31. Правила защиты от компьютерных вирусов (ОПК-3, ОПК-4)
32. Типовые удаленные атаки и их характеристика (ОПК-3, ОПК-4)
33. Методы защиты документальной информации. (ОПК-3, ОПК-4)
34. Криптографические методы защиты информации (ОПК-3, ОПК-4)
35. Основные предметные направления защиты информации (ОПК-3, ОПК-4)
36. Принципы организации обмена данными в вычислительных сетях (ОПК-3, ОПК-4)
37. Алгоритмы обнаружения различных типов вирусов (ОПК-3, ОПК-4)
38. Исторические аспекты возникновения и развития информационной безопасности (ОПК-3,ОПК-4)
39. Программно-аппаратные защиты информационных ресурсов в Интернет (ОПК-3, ОПК-4)
40. Симметричное и асимметричное шифрование (ОПК-3, ОПК-4)

4.1.2. Средства для индивидуализации выполнения, контроля фиксированных видов ВАРО

Фиксированные виды внеаудиторных самостоятельных работ не предусмотрены

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

5.2. Критерии оценки к зачету

зачет (86-100 баллов) ставится обучающемуся, обнаружившему систематические и глубокие знания учебно-программного материала, умения свободно выполнять задания, предусмотренные программой в типовой ситуации (с ограничением времени) и в нетиповой ситуации, знакомство с основной и дополнительной литературой, усвоение взаимосвязи основных понятий дисциплины в их значении приобретаемой специальности и проявившему творческие способности и самостоятельность в приобретении знаний.

зачет (71-85 баллов) ставится обучающемуся, обнаружившему полное знание учебно-программного материала, успешное выполнение заданий, предусмотренных программой в типовой ситуации (с ограничением времени), усвоение материалов основной литературы, рекомендованной в программе, способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей работы над литературой и в профессиональной деятельности.

зачет (56-70 баллов) ставится обучающемуся, обнаружившему знание основного учебно - программного материала в объеме, достаточном для дальнейшей учебы и предстоящей рабо ты по специальности, знакомство с основной литературой, рекомендованной программой, умение выполнять задания, предусмотренные программой.

незачет (менее 56 баллов) ставится обучающемуся, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, слабые побуждения к самостоятельной работе над рекомендованной основной литературой. Оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании академии без дополнительных занятий по соответствующей дисциплине.

6. Оценочные материалы для организации текущего контроля успеваемости обучающихся

Форма, система оценивания, порядок проведения и организация *текущего контроля успеваемости* обучающихся устанавливаются Положением об организации текущего контроля успеваемости обучающихся.

Комплект контрольных вопросов для проведения устных опросов

Тема. Информационная безопасность, как определяющий компонент национальной безопасности России.

Задание. Ответить на вопросы.

1. Охарактеризуйте информацию и ее основные показатели.

2. Какие существуют подходы к определению понятия «информация».
3. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.
4. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
5. Назовите основные виды конфиденциальной информации.
6. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
7. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?
8. В чем заключается национальная безопасность России, еѐ определения?
9. Каковы принципы, основные задачи и функции обеспечения информационной безопасности?
10. В чем заключаются функции государственной системы по обеспечению информационной безопасности?
11. Что такое уровни обеспечения национальной безопасности России?
12. Что такое информационная война?
13. Что такое информационное превосходство?
14. Что такое информационное оружие, каковы его разновидности?

Тема. Основные направления обеспечения безопасности информационных ресурсов

Задание. Ответить на вопросы.

1. Дайте определение системы защиты государственной тайны и укажите ее составляющие.
2. Что в соответствии с законодательством РФ представляет собой засекречивание информации.
3. Перечислите основные принципы засекречивания информации.
4. Что понимается под профессиональной тайной?
5. Какие виды профессиональных тайн вам известны?
6. В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?
7. В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?
8. Что понимается под профессиональной тайной?
9. Какие виды профессиональных тайн вам известны?
10. В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?

Тема. Нормативно-правовые основы информационной безопасности РФ

Задание 1. Ответить на вопросы.

1. Охарактеризуйте место правовых мер в системе комплексной защиты информации.
2. Назовите основные цели государства в области обеспечения информационной безопасности.
3. Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
4. Какой закон определяет понятие «официальный документ»?
5. Какой закон определяет понятие «электронный документ»?
6. В тексте какого закона приведена классификация средств защиты информации?
7. Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?
8. Назовите основные положения Доктрины информационной безопасности РФ.
9. Назовите составляющие правового института государственной тайны.

Тема. Стандарты информационной безопасности.

Задание. Ответить на вопросы.

1. Общие требования безопасности к информационным системам.
2. Что такое стандарт информационной безопасности?
3. Чем отличаются функциональные требования от требований доверия?
4. В чем заключается иерархический принцип «класс-семейство-компонент-элемент»?
5. Сколько классов функциональных требований?
6. Сколько классов защищенности СВТ от НСД к и нформации устанавливает руководящий документ «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?

7. Дайте характеристику уровням защиты СВТ от НСД к информации по РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?

Тема. Уровни обеспечения ИБ

Задание. Ответить на вопросы.

1. Цели и задачи административного уровня обеспечения информационной безопасности
2. Содержание административного уровня
3. Дайте определение политике информационной безопасности
4. Направления разработки политики безопасности
5. Основные требования к политике безопасности
6. Жизненный цикл политики безопасности
7. Содержание политики безопасности

Тема. Обеспечение информационной безопасности с помощью антивирусных программ

Задание. Ответить на вопросы.

1. Дайте определение программного вируса.
2. Характерные черты компьютерных вирусов.
3. Какие трудности возникают при определении компьютерного вируса?
4. Какие типы компьютерных вирусов существуют?
5. Укажите основные признаки заражения компьютера?
6. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
7. Укажите пути проникновения компьютерного вируса в компьютер?
8. Что такое троянская программа?

Тема. Каналы утечки информации

Задание. Ответить на вопросы.

1. Какие технические средства защиты информации вам известны?
2. Классификация технических каналов утечки информации
3. Перечислите основные показатели технического канала утечки информации?
4. Какие технические средства охранной сигнализации вам известны?
5. Что представляют с собой инфраакустические датчики?

Критерии оценивания устных опросов:

- правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);
- полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);
- сознательность ответа (учитывается понимание излагаемого материала);
- логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения задания, устного ответа во времени, с учетом индивидуальных особенностей обучающихся).

Шкала оценивания

Баллы для учета в рейтинге (оценка)	Степень удовлетворения критериям
86-100 баллов «отлично»	Обучающийся полно и аргументировано отвечает по содержанию вопроса (задания); обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; излагает материал последовательно и правильно.
71-85 баллов «хорошо»	Обучающийся достаточно полно и аргументировано отвечает по содержанию вопроса (задания); обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; излагает материал последовательно. Допускает 1-2 ошибки, исправленные с помощью наводящих вопросов.
56-70 баллов «удовлетворительно»	Обучающийся обнаруживает знание и понимание основных положений данного задания, но излагает материал неполно и допускает неточности в определении понятий или формулировке

	правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки.
менее 56 баллов «неудовлетворительно»	Обучающийся обнаруживает незнание ответа на соответствующее задание (вопрос), допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Отмечаются такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному овладению последующим материалом.

Комплект заданий для лабораторных работ

Тема. Классификация угроз информационной безопасности

Задание 1. Ответить на вопросы.

1. Дайте определение угрозам информационной безопасности
2. Перечислите классы угроз информационной безопасности
3. Дайте характеристику преднамеренным угрозам
4. Перечислите каналы несанкционированного доступа к информации
5. Назовите причины и источники случайных воздействий на информационные системы

Задание 2.

Классифицировать нижеперечисленные угрозы информационной безопасности:

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (не умышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2) неправомерное отключение оборудования или изменение режимов рабо ты устройств и программ;

3) неумышленная порча носителей информации;

4) запуск программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих не обратимые изменения в системе (форматирование носителей информации, удаление данных и т.п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

7) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

8) физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

9) отключение или вывод из строя подсистем обеспечения функционирования вы - числительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

10) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

11) хищение носителей информации;

12) несанкционированное копирование носителей информации;

13) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

14) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

Тема. Нормативно-правовые основы информационной безопасности РФ

Задание 1.

При решении приведенных ниже ситуационных задач студенты должны ответить на вопрос: «Имеет ли место в данной ситуации нарушение авторского права гражданина (граждан)?», а также обосновать свой ответ, указав наименование соответствующего нормативного документа, его ста тьи и пункта статьи.

Задача 2.1.

Гражданин Иванов предложил гражданам Шаталову и Моисееву идею создания информационно-справочной системы «Альбомы рок-музыкантов» в среде программирования Delphi 6.0, лицензионная версия которой была приобретена Моисеевым. Граждане Шаталов и Моисеев создали такую систему и зарегистрировали свое авторство на нее без участия гражданина Иванова. Имеет ли место в данной ситуации нарушение авторского права гражданина Иванова?

Задача 2.2.

Гражданин Алексеев создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Alex 3D» и зарегистрировал на него свои права. 20.09. 06 этот гражданин заключил договор с компанией « Moscow Technology» и передал свои имущественные права на распространение своего программного продукта сроком на один год (т. е. до 19.09. 07). После заключения договора компания «Moscow Technology» распространила версию программы «Alex 3D» с предварительной модификацией данного программного продукта без ведома автора.

Тема. Нормативно-правовые основы информационной безопасности РФ

Задание. При решении приведенных ниже ситуационных задач студенты должны ответить на вопрос: «Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?» Ответ необходимо обосновать, указав соответствующий нормативный документ, его статью и пункт статьи.

Задача 1

Бывший сотрудник химико-биологического предприятия вместе со своим приятелем-программистом скопировали конфиденциальную информацию: состав ингредиентов, их пропорции и формулу нового лекарственного препарата — с целью продажи этой информации конкурирующей организации.

Задача 2

П. П. Андреев, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые фа йлы (файлы с расширением *.exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 750 000 рублей.

Задача 3

Сотрудник Научно-исследовательского института приборостроения скопировал схемы, чертежи и графики прибора с целью продажи этой информации зарубежной фирме-производителю.

Тема. Криптографические методы защиты информации

Задание 1. Ответить на вопросы.

1. Что такое криптология?
2. Что такое ключ?
3. Что из себя представляет криптосистема?
4. Объясните суть преобразований - перестановка и замена?

Задание 2.

1. Зашифровать «Французский математик Пьер Ферма по образованию был юрист».
2. Зашифровать «Леонардо Пизанского математики знают под именем "сын добряка" или Фибоначчи».
3. Дешифровать (восстановить сообщение, зная ключ) Ключ 8.
   Чинои сечем лчгмс хыеоо еаитн ккыин лтсбч втрйы еоосс ееорс неомв бадер покп.
   (Примечание: АБ - дополнительные буквы)
4. Расшифровать (восстановить сообщение, не зная ключа).
   Осуз уаан евем исчи тдьм одоа ьлвь рдво быи.
5. Расшифровать: Етгртуой дкмиуиав цлишлаег врныинис аяоплыдб аанполбр.

Задание 3. Ответить на вопросы.

1. Что из себя представляет система шифрования с использованием таблицы Вижинера?
2. Что из себя представляет симметричная криптографическая система?
3. Что из себя представляет симметричная криптографическая система?

4. Какими характеристиками оценивается стойкость криптосистемы?

Задание 4. Шифр Вижнера.

Ключ ВАЗА: /3 1 8 1/. Сдвиг осуществляется не на постоянную величину, а на номер буквы в ключевом слове. КРИПТОГРАФИЯ => НСРРХПЛСГХРА.

Сложность при расшифровке в том, что одинаковые буквы переходят в разные, а разные - в одинаковые => частотный анализ не применим.

Зашифровать фразу: Математика - царица наук.

Тема. Электронно-цифровая подпись. Алгоритмы шифрования электронно-цифровой подписи

Задание 1. Ответить на вопросы.

1. Дайте общее определение цифровой подписи
2. Какие основные задачи решает цифровая подпись?
3. Особенности электронно-цифровой подписи
4. Законодательные основы использования ЭЦП
5. Что такое квалифицированный сертификат ключа проверки ЭЦП?
6. Что такое электронный идентификатор Rutoken?
7. Особенности etoken

Задание 2.

Вы обратились в удостоверяющий центр для создания своей электронной цифровой подписи. Будет ли действителен ваш сертификат ключа подписи, если он содержит следующие сведения:

- вашу фамилию, имя и отчество;
- даты начала и окончания срока действия сертификата ключа подписи;
- название и место нахождения удостоверяющего центра;
- открытый ключ ЭЦП?

Тема. Обеспечение информационной безопасности с помощью антивирусных программ

Задание. Ответить на вопросы.

1. Какие классы антивирусных программ вам известны?
2. Какие вредоносные программные закладки, кроме вирусов, вам известны?
3. Какие существуют методы борьбы с компьютерными вирусами?
4. Какие антивирусные программы вы знаете?
5. Каким образом производится лечение зараженных дисков?
6. Что такое программа – полифаг?
7. Что такое программа – детектор?

Задание 2. Осуществить в сети Интернет поиск готовых антивирусных программ. Представить результат в виде списка программных продуктов (таблица 1).

Таблица 1 -Программные продукты, для борьбы с компьютерными вирусами

№ п/п	Название продукта	Название фирмы	Требования к системе	Возможности	Стоимость, руб
1					
2					

Задание 3. Из представленной выше таблицы выбрать три программных продукта и провести их сравнительный анализ. Результат: характеристики программных продуктов, представить в таблице 2.

Таблица 2 - Сравнение антивирусных программных продуктов

№ п/п	Список характеристик	Название продукта №1	Название продукта №2	Название продукта №3
		Представлена характеристика или нет	Представлена характеристика или нет	Представлена характеристика или нет

Задание 4. На основании таблиц сделать вывод, какой должна быть антивирусная защита организации, чтобы учитывать все достоинства и недостатки имеющихся программных продуктов. Результат представить в

Тема. Основы безопасности сетевых информационных технологий

Задание. Ответить на вопросы.

1. Дайте определение вычислительных сетей и приведите их классификацию
2. Дайте краткую характеристику принципам и методам организации межсетевого взаимодействия
3. Сформулируйте цели и защиты информации в сетях ЭВМ и назовите основные угрозы информации в сетях
4. Приведите перечень основных механизмов защиты информации в сетях и дайте им краткую характеристику.
5. Приведите и охарактеризуйте основные положения концепции защиты информации в эталонной модели взаимодействия открытых сетей
6. Приведите структуру и содержание процедуры взаимной аутентификации пользователей сети

Критерии оценивания лабораторных работ:

– правильность выполнения задания на лабораторную работу в соответствии с вариантом;

– степень усвоения теоретического материала по теме лабораторной работы;

-способность продемонстрировать преподавателю навыки работы в инструментальной программной среде, а также применить их к решению типовых задач, отличных от варианта задания;

– качество подготовки отчета по лабораторной работе;

– правильность и полнота ответов на вопросы преподавателя при защите работы.

Шкала оценивания

Баллы для учета в рейтинге (оценка)	Степень удовлетворения критериям
86-100 баллов «отлично»	Выполнены все задания лабораторной работы, обучающийся четко и без ошибок ответил на все контрольные вопросы
71-85 баллов «хорошо»	Выполнены все задания лабораторной работы; обучающийся ответил на все контрольные вопросы с замечаниями
56-70 баллов «удовлетворительно»	Выполнены все задания лабораторной работы с замечаниями; обучающийся ответил на все контрольные вопросы с замечаниями
менее 56 баллов «неудовлетворительно»	Обучающийся не выполнил или выполнил неправильно задания лабораторной работы; обучающийся ответил на контрольные вопросы с ошибками или не ответил на контрольные вопросы

Комплект заданий для самостоятельной работы обучающихся

Тема Нормативно-правовые основы информационной безопасности РФ.

1. Задача на определение наличия или отсутствия каких -либо нарушений прав личности, связанных с нарушением информационной безопасности

При решении приведенных ниже ситуационных задач студенты должны ответить на вопрос: «Имеет ли место в данной ситуации нарушение авторского права гражданина (г раждан)?», а также обосновать свой ответ, указав наименование соответствующего нормативного документа, его статьи и пункта статьи.

Гражданин Серебренников разработал в соавторстве с гражданином Семеновым информационно-справочную систему «Энциклопедия. Живо тные Крайнего севера». Финансовую поддержку программных разработок вышеупомянутым гражданам оказал гражданин Андреев. Граждане Серебренников и Семенов 13.05.16 оформили свое авторство на данную информационную систему. В марте 2017г. данный программный продукт был выпущен под авторством гражданина Андреева.

Имеет ли место в данной ситуации нарушение авторского права граждан Серебренникова и Семенова?

Тема: Криптографические методы защиты информации

1. «Шифры замены». Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

2.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения закодированы с помощью этой таблицы?

16	55	54	10	69	09	61	89	29	90	49	44	10	08	02	73	21	32	83	54	74
41	55	77	10	23	68	08	20	66	90	76	44	21	61	90	55	21	61	83	54	42
57	30	27	10	91	68	32	20	80	02	49	45	40	32	46	55	40	08	83	27	17

3. «Шифр Цезаря». Этот шифр реализует следующее преобразование текста: каждая буква исходного текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу. Используя этот шифр, зашифруйте слова информация, компьютер, человек.

4. Расшифруйте слово НУЛТХСЁУГЧЛВ, закодированное с помощью шифра Цезаря. (см. задачу №2).

5. «Шифр Вижинера». Этот шифр представляет шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста:
3 1 9 1 3 1 9 1 и т.д. Используя в качестве ключевого слово ВАГОН, закодируйте слова: АЛГОРИТМ, ПРАВИЛА. ИНФОРМАЦИЯ.

6. Слово НССРХПЛСГХСА получено с помощью шифра Вижинера с ключевом словом ВАЗА. Восстановите исходное слово.

7. «Шифр перестановки». Кодирование осуществляется перестановкой букв в слове по одному и тому же общему правилу. Восстановите слова и определите правило перестановки: ЛБКО, ЕРАВШН, УМЫЗАК, АШНРРИ, РКДЕТИ.

8. Правило кодирования: после каждой гласной буквы вставляется буква А. а после согласной - Т. Расшифруйте слова: иантфтоартмтааттиак таа, птртиантттеарт.

9. Угадайте правило шифровки и расшифруйте слова: ткафетра, ткнитсни, тицартна, ланигиро.

10. Пользуясь правилом из предыдущей задачи, зашифруйте фразу: ИНФОРМАТИКА – ЭТО НАУКА О СПОСОБАХ ПОЛУЧЕНИЯ, НАКОПЛЕНИЯ, ОБРАБОТКИ, ПЕРЕДАЧИ И ПРЕДСТАВЛ ЕНИЯ ИНФОРМАЦИИ.

11. Определите правило шифровки и расшифруйте слова:

АКРОЛДИИТРБОФВНАЗНГИЦЕШ
ЩИККНГФЗОЕРУМЦАЫЦГИХИ

Тема: Обеспечение информационной безопасности с помощью антивирусных программ

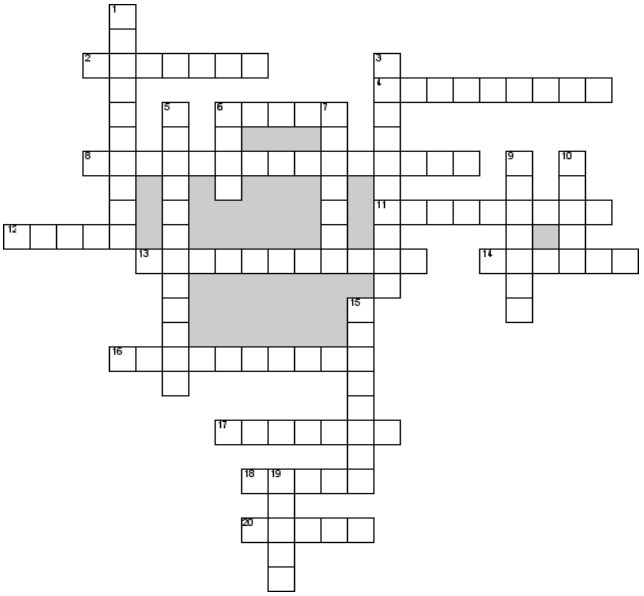
Задание. Отгадать кроссворд

По горизонтали

2. Программы, которые используются для обработки файлов и загрузочных секторов с целью преждевременного выявления вирусов
4. Любая программа для обнаружения вирусов
6. Вирус невидимка
8. Одно из главных свойств вирусов, способность к созданию себе подобных
11. Постоянная последовательность программного кода, специфичная для конкретной вредоносной программы
12. Специалист по взлому защиты программ ,с целью незаконного доступа к хранящейся в ней информации
13. Видоизменение вируса
14. Вид интернет - мошенничества, цель которого - получить идентификационные данные пользователя
16. Вредоносная программа, заражающая документы, шаблоны документов
17. Антивирус, чей принцип работы основан на подсчете контрольных сумм для присутству ющих на диске файлов
18. Процесс установки простой и похож на установку AVG, но не проще, чем Касперского или Trend

Micro. Стандартное сканирование проходит за 19 минут, а полное сканирование за 45 минут, используя около 15 Мб RAM. При этом на системные ресурсы оказывается очень незначительное влияние. Для осуществления минимального воздействия на компьютер, запускаются специальные сценарии, обеспечивающие к тому же минимальное воздействие на процедуру завершения работы Windows.

20. Вредоносная программа, осуществляющая несанкционированную пользователем передачу управления компьютером удаленному пользователю



По вертикали

1. Аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети интернета
3. Российский программист, специалист по антивирусной защите, один из основателей собственной лаборатории
5. Программы, способные обнаружить и остановить вирус на самой ранней стадии его развития
6. Навязчивая электронная рассылка, почтовый мусор
7. Резидентные программы, которые постоянно сохраняются в памяти компьютера и в определенное пользователем время проверяют оперативную память
9. Набор программ для скрытого взятия под контроль взломанной системы
10. Вредоносные программы, распространяющие свои копии по локальным или глобальным сетям
15. Компьютерная программа, блок данных или фрагмент программного кода, которые вызывают некорректную работу программного обеспечения
19. Тип вредоносной программы

Критерии оценивания самостоятельной работы:

– правильность выполнения задания на лабораторную работу в соответствии с вариантом;
– степень усвоения теоретического материала по теме лабораторной работы;
– способность продемонстрировать преподавателю навыки работы в инструментальной программной среде, а также применить их к решению типовых задач, отличных от варианта задания;
– качество подготовки отчета по лабораторной работе;
– правильность и полнота ответов на вопросы преподавателя при защите работы.

Шкала оценивания

Баллы для учета в рейтинге (оценка)	Степень удовлетворения критериям
86-100 баллов «отлично»	Выполнены все задания лабораторной работы, обучающийся четко и без ошибок ответил на все контрольные вопросы
71-85 баллов «хорошо»	Выполнены все задания лабораторной работы; обучающийся ответил на все контрольные вопросы с замечаниями
56-70 баллов «удовлетворительно»	Выполнены все задания лабораторной работы с замечаниями; обучающийся ответил на все контрольные вопросы с замечаниями
менее 56 баллов «неудовлетворительно»	Обучающийся не выполнил или выполнил неправильно задания лабораторной работы; обучающийся ответил на контрольные вопросы с ошибками или не ответил на контрольные вопросы

Кейс задания

Задача 1

«Шифры замены». Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения закодированы с помощью этой таблицы?

Вариант1

16	55	54	10	69	09	61	89	29	90	49	44	10	08	02	73	21	32	83	54	74
41	55	77	10	23	68	08	20	66	90	76	44	21	61	90	55	21	61	83	54	42
57	30	27	10	91	68	32	20	80	02	49	45	40	32	46	55	40	08	83	27	17

Вариант 2

19	55	54	10	69	09	61	89	29	90	49	44	10	08	02	73	21	32	83	54	74
58	55	77	10	23	68	08	20	66	90	76	44	21	61	90	55	21	61	83	54	42
87	30	27	10	91	68	32	20	80	02	49	45	40	32	46	55	40	08	83	27	17

Вариант 3

08	55	54	10	69	09	61	89	29	90	49	44	10	08	02	73	21	32	83	54	74
32	55	77	10	23	68	08	20	66	90	76	44	21	61	90	55	21	61	83	54	42
61	30	27	10	91	68	32	20	80	02	49	45	40	32	46	55	40	08	83	27	17

Задача 2

«Шифры замены». Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Задача 3

Задачи на определение наличия или отсутствия каких-либо нарушений прав личности, связанных с нарушением информационной безопасности Задачи по основным положениям закона «О правовой охране программ для ЭВМ и баз данных».

При решении приведенных ниже ситуационных задач студенты должны ответить на вопрос: «Имеет ли место в данной ситуации нарушение авторского права гражданина (граждан)?», а также обосновать свой ответ, указав наименование соответствующего нормативного документа, его статьи и пункта статьи.

Вариант 1

Гражданин Иванов предложил гражданам Шаталову и Моисееву идею создания информационно-справочной системы «Альбомы рок-музыкантов» в среде программирования Delphi 6.0, лицензионная версия которой была приобретена Моисеевым. Граждане Шаталов и Моисеев создали такую систему и зарегистрировали свое авторство на нее без участия гражданина Иванова.

Имеет ли место в данной ситуации нарушение авторского права гражданина Иванова?

Вариант 2

Гражданин Алексеев создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Alex 3D» и зарегистрировал на него свои права. 20.09. 06 этот гражданин заключил договор с компанией « Moscow Technology» и передал свои имущественные права на распространение своего программного продукта сроком на один год (т. е. до 19.09. 07). После заключения договора компания «Moscow Technology» распространила версию программы «Alex 3D» с предварительной модификацией данного программного продукта без ведома автора.

Имеет ли место в данной ситуации нарушение авторского права гражданина Алексеева?

Вариант 3

Гражданин Серебренников разработал в соавторстве с гражданином Семеновым информационно-справочную систему «Энциклопедия. Животные Крайнего севера». Финансовую поддержку программных разработок вышеупомянутым гражданам оказал гражданин Андреев. Граждане Серебренников и Семенов 13.05.06 оформили свое авторство на данную информационную систему. В марте 2006 г. данный программный продукт был выпущен под авторством гражданина Андреева.

Имеет ли место в данной ситуации нарушение авторского права граждан Серебренникова и Семенова?

Критерии оценивания

- соответствие решения с формулированным в кейсе вопросам (адекватность проблеме и рынку);
- оригинальность подхода (новаторство, креативность);
- применимость решения на практике;
- глубина проработки проблемы (обоснованность решения, наличие альтернативных вариантов, прогнозирование возможных проблем, комплексность решения).

Шкала оценивания

Баллы для учета в рейтинге (оценка)	Степень удовлетворения критериям
100-85 баллов «отлично»	Предложенное решение соответствует поставленной в кейс-задании проблеме. Обучающийся применяет оригинальный подход к решению поставленной проблемы, демонстрирует высокий уровень теоретических знаний, анализ соответствующих источников. Формулировки кратки, ясны и точны. Ожидаемые результаты применения предложенного решения конкретны, измеримы и обоснованы.
84-70 балла «хорошо»	Предложенное решение соответствует поставленной в кейс-задае проблеме. Обучающийся применяет в основном традиционный подход с элементами новаторства, частично подкрепленный анализом соответствующих источников, демонстрирует хороший уровень теоретических знаний. Формулировки недостаточно кратки, ясны и точны. Ожидаемые результаты применения предложенного решения требуют исправления незначительных ошибок.
69-55 балла «удовлетворительно»	Предложенное решение требует дополнительной конкретизации и обоснования, в целом соответствует поставленной в задаче проблеме. При решении поставленной проблемы обучающийся применяет традиционный подход, демонстрирует твердые знания по поставленной проблеме. Предложенное решение содержит ошибки, уверенно исправленные после наводящих вопросов.
Менее55 баллов «неудовлетворительно»	Наличие грубых ошибок в решении ситуации, непонимание сущности рассматриваемой проблемы, неуверенность и неточность ответов после наводящих вопросов. Предложенное решение не обосновано и не применимо на практике

Комплект тестовых заданий

Вариант 1

1. На сегодняшний день под защитой компьютерной информации понимается:
    1. Совокупность методов криптографического преобразования исходных данных с целью получения зашифрованных данных.
    2. Совокупность мероприятий, методов и средств, обеспечивающих решение задач проверки целостности информации, исключения несанкционированного доступа к ресурсам ЭВМ и хранящимся в ней программам и данным, а также исключения несанкционированного использования программных продуктов.

3. Защита от умышленных попыток человека получить доступ к этой информации либо модифицировать еѐ.
4. Совокупность методов, программ и алгоритмов, позволяющих обеспечить надежное хранение информации в условиях ее эксплуатации.

2. Укажите традиционные направления защиты компьютерной информации
   1. Криптография
   2. Антивирусология
   3. Линейное программирование
   4. Защита от несанкционированного копирования
   5. Сетевая защита
3. Основным документом, на основе которого проводится политика информационной безопасности предприятия, является:
   1. закон РФ «Об информации, информатизации и защите информации»
   2. перечень критериев оценки надежных компьютерных систем («Оранжевая книга»)
   3. программа информационной безопасности предприятия
4. Что является объектом защиты информации?
   1. Компьютерная система или автоматизированная система обработки данных (АСОД)
   2. Вычислительные сети
   3. Системы управления базами данных (СУБД)
   4. Память ЭВМ
5. Что является предметом защиты в компьютерных системах?
   1. электронные и электромеханические устройства, а также машинные носители
   2. информация
   3. системы передачи данных (СПД)
6. Дайте определение понятия «Надежная система»
   1. Надежной называется система, эффективно использующая аппаратные и программные средства для обнаружения и предотвращения возможных атак на информацию
   2. Надежной называется система, использующая достаточные программные и аппаратные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа
   3. Надежной называется система, гарантированность безопасного хранения информации в которой близка к 100%
7. Согласно «Оранжевой книге» надежность системы оценивается по следующим критериям:
   1. Криптостойкость
   2. Гарантированность
   3. Надежность
   4. Конфиденциальность
   5. Политика безопасности
8. Европейские критерии безопасности компьютерных систем рассматривают следующие составляющие информационной безопасности:
   1. Конфиденциальность
   2. Целостность
   3. Гарантированность
   4. Доступность
   5. Надежность
9. Расположите в порядке убывания основные причины повреждений электронной информации
   1. Ошибочные действия пользователя
   2. Стихийные бедствия (затопления, пожары и т.п.)
   3. Умышленные действия человека или отказ техники
   4. Прочие непредвиденные обстоятельства
10. Под угрозой безопасности информации понимается:
    1. Атака на информацию со стороны злоумышленника
    2. Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации
    3. Несанкционированный доступ к информации, который может привести к нарушению целостности системы компьютерной безопасности
11. Все множество потенциальных угроз безопасности информации в КС может быть разделено на следующие классы:
    1. Случайные угрозы
    2. Потенциальные угрозы
    3. Преднамеренные угрозы
12. Что понимается под возможным каналом утечки информации?
    1. Способ, позволяющий нарушителю получить доступ к хранящейся или обрабатываемой

информации
2.Техническое средство, с помощью которого нарушитель может получить доступ к хранящейся или обрабатываемой информации
3. Комплекс программных и/или аппаратных средств, позволяющих осуществлять передачу данных от источника информации к нарушителю

13. . С помощью каких типов средств может происходить утечка информации по возможному каналу?
1. Данные
2. Человек
3. Компьютерная сеть
4. Программа
5. Аппаратура

14. Перечислите основные виды случайных угроз:
1. Стихийные бедствия и аварии
2. Сбои и отказы технических средств
3. Ошибки при разработке компьютерных систем
4. Электромагнитные излучения и наводки

15. Установите соответствие между методом преобразования и классом секретных систем, к которому он относится.

1	Использование «невидимых» чернил для записи сообщений	А	Системы маскировки
2	Инвертирование речи	Б	Тайные системы
3	Шифр Цезаря	В	Криптографические системы

16. Закон «Об информации, информатизации и защите информации» в Российской Федерации был принят в_____ году?

17. Дайте определение понятия криптография:
1. Криптография - это наука о защите информации от несанкционированного доступа посторонними лицами
2. Криптография - наука о защите информации от прочтения еѐ посторонними лицами, достигаемая путем шифрования, которое делает защищенные данные труднораскрываемыми без знания специальной (ключевой) информации
3. Криптография - это наука о защите информации с помощью математических преобразований, которые являются симметричными

18. Дайте определение понятия шифр:
1. Шифр - это совокупность преобразований, с помощью которых осуществляется кодирование информации
2. Шифр - это алгоритм преобразования, в котором используется ключ
3. Шифр - это совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования

19. Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности возможных для данного алгоритма называется…

20. Соотношение, описывающее процесс образования зашифрованных данных из открытых называется:
1. Алгоритмом шифрования
2. Методом шифрования
3. Функцией шифрования
4. Уравнением шифрования

21. Согласно классификации секретных систем по К. Шеннону существует три общих типа таких систем. Укажите какие.
1. Системы сокрытия информации
2. Системы маскировки
3. Системы защиты данных
4. Криптографические системы

22. Назовите фамилию автора известной статьи «Теория связи в секретных системах», одного из основоположников теории современной криптографии…

23. Секретная система - это:
1. совокупность методов и алгоритмов шифрования, которые обеспечивают возможность криптографической защиты данных
2. некоторое множество отображений одного пространства (множества возможных сообщений) в

другое пространство (множество возможных криптограмм), где каждое конкретное отображение из этого множества соответствует способу шифрования при помощи конкретного ключа
3. некоторое множество отображений одного пространства (множества возможных сообщений) в другое пространство (множество возможных криптограмм), где каждое конкретное отображение из этого множества соответствует способу шифрования при помощи нескольких ключей
24. Замена смысловых конструкций исходной информации (слов, предложений) кодами называется:
1. Шифрованием
2. Кодированием
3. Сжатием
4. Дешифрованием

25. Расположите указанные системы шифрования в хронологическом порядке их появления
1: Шифр Скитала
2: Квадрат Полибия
3: Шифр Цезаря
4: Книжный шифр
26. Синонимом термина «стеганография» является понятие:
1. Системы сокрытия информации
2. Системы маскировки
3. Системы защиты данных
4. Криптографические системы
27. Замена смысловых конструкций исходной информации (слов, предложений) кодами называется:
1. Шифрованием
2. Кодированием
3. Сжатием
4.Дешифрованием
28. Электронная цифровая подпись (ЭЦП) позволяет избежать следующих потенциальных угроз:
1. Отказ (ренегатство)
2. Модификация (переделка)
3. Утечка информации (перехват сообщений в канале связи)
4. Активный перехват (перехват сообщений в канале связи и их скрытая модификация)
29. Первые идеи по созданию электронной цифровой подписи (ЭЦП) принадлежат следующим авторам:
1. Ш.Адельману
2. Р.Рависту
3. М. Хеллману
4. Шнайеру
30. Процесс получения электронной цифровой подписи (ЭЦП) также называют:
1. Коротким шифрованием
2. Хешированием
3. Кадрированием
4. Кодированием

Вариант 2

1. Составляющие национальной безопасности:
   1. соблюдение … Российской Федерации.
   2. Правовое … всех участников процесса информационного взаимодействия.
   3. Соблюдение ... прав и свобод человека и гражданина в области получения информации и пользования ею.
   4. Приоритетное … отечественных современных информационных технологий
2. Для информационной войны обычно четко определена … … .

3. Какой метод обеспечения информационной без опасности отсутствует в перечне:

1 Организационный	3 Правовой	5 Технический
2 Экономический	4 Идеологический	

4. Информация воздействия - … знания, … модели окружающего мира.

5. Совокупность информации, информационной инфраструктуры, субъектов и системы регулирования общественных отношений являются составляющими частями … … .

6. Автономная информация - информация , существующая … от какого-либо субъекта.

7. Информационная сфера - являясь системообразующим фактором жизни общества, активно влияет на сосояние … , … , … и др. составляющих безопасности Российской Федерации.

8. Информация взаимодействия - … одного субъекта на другого, имеющее целью …, моделей внешней среды двух субъектов или коллектива.
9. Информационная безопасность - … защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью … интересов личности, общес тва и государства.
10. Общая схема национальной безопасности:
1. Формулировка …
2. Формирование перечня …
3. Оценка … и …
4. Разработка …
5. Принятие …
11. Вторая классификация национальных интересов:

1. по принадлежности интересов
2. по национальным признакам
3. по важности интересов
4. по экономическим признакам

12. Классификация информации как объекта исследования:

13. Дайте определение понятия криптография:
1. Криптография - это наука о защите информации от несанкционированного доступа посторонними лицами
2. Криптография - наука о защите информации от прочтения еѐ посторонними лицами, достигаемая путем шифрования, которое делает защищенные данные труднораскрываемыми без знания специальной (ключевой) информации
3. Криптография - это наука о защите информации с помощью математических преобразований, которые являются симметричными

14. Дайте определение понятия шифр:
1. Шифр - это совокупность преобразований, с помощью которых осуществляется кодирование информации
2. Шифр - это алгоритм преобразования, в котором используется ключ
3. Шифр - это совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования

15. Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности возможных для данного алгоритма называется…

16. Соотношение, описывающее процесс образования зашифрованных данных из открытых называется:
1. Алгоритмом шифрования
2. Методом шифрования
3. Функцией шифрования
4. Уравнением шифрования

17. Согласно классификации секретных систем по К. Шеннону существует три общих типа таких систем. Укажите какие.
1. Системы сокрытия информации
2. Системы маскировки
3. Системы защиты данных
4. Криптографические системы

18. Назовите фамилию автора известной статьи «Теория связи в секретных системах», одного из основоположников теории современной криптографии…

19. Секретная система - это:
1. совокупность методов и алгоритмов шифрования, которые о беспечивают возможность криптографической защиты данных
2. некоторое множество отображений одного пространства (множества возможных сообщений) в другое пространство (множество возможных криптограмм), где каждое конкретное отображение из этого множества соответствует способу шифрования при помощи конкретного ключа

3. некоторое множество отображений одного пространства (множества возможных сообщений) в другое пространство (множество возможных криптограмм), где каждое конкретное отображение из этого множества соответствует способу шифрования при помощи нескольких ключей

20. Замена смысловых конструкций исходной информации (слов, предложений) кодами называется:
1. Шифрованием
2. Кодированием
3. Сжатием
4. Дешифрованием

21. Расположите указанные системы шифрования в хронологическом порядке их появления
1: Шифр Скитала
2: Квадрат Полибия
3: Шифр Цезаря
4: Книжный шифр

22. Синонимом термина «стеганография» является понятие:
1. Системы сокрытия информации
2. Системы маскировки
3. Системы защиты данных
4. Криптографические системы

23. Замена смысловых конструкций исходной информации (слов, предложений) кодами называется:
1. Шифрованием
2. Кодированием
3. Сжатием
4.Дешифрованием

24. Электронная цифровая подпись (ЭЦП) позволяет избежать следующих потенциа льных угроз:
1. Отказ (ренегатство)
2. Модификация (переделка)
3. Утечка информации (перехват сообщений в канале связи)
4. Активный перехват (перехват сообщений в канале связи и их скрытая модификация)

25. Первые идеи по созданию электронной цифровой подписи (ЭЦП) принадлежат следующим авторам:
1. Ш.Адельману
2. Р.Рависту
3. М. Хеллману
4. Шнайеру

26. Процесс получения электронной цифровой подписи (ЭЦП) также называют:
1. Коротким шифрованием
2. Хешированием
3. Кадрированием
4. Кодированием

27. Укажите традиционные направления защиты компьютерной информации
1. Криптография
2. Антивирусология
3. Линейное программирование
4. Защита от несанкционированного копирования
5. Сетевая защита

28. Основным документом, на основе которого проводится политика информационной безопасности предприятия, является:
1. закон РФ «Об информации, информатизации и защите информации»
2. перечень критериев оценки надежных компьютерных систем («Оранжевая книга»)
3. программа информационной безопасности предприятия

29. Что является объектом защиты информации?
1. Вычислительные сети
2. Системы управления базами данных (СУБД)
3. Память ЭВМ

30.Что является предметом защиты в компьютерных системах?
1. электронные и электромеханические устройства, а также машинные носители
2. информация
3. системы передачи данных (СПД)

Критерии оценивания:
- отношение правильно выполненных заданий к общему их количеству

Шкала оценивания

Баллы для учета в рейтинге (оценка)	Степень удовлетворения критериям
86-100 баллов «отлично»	Выполнено 86-100% заданий
85-71 балла «хорошо»	Выполнено 71-85% заданий
70-56 балла «удов лет во р ительно»	Выполнено 56-70% заданий
Менее 56 баллов «неу дов лет в ор иительно»	Выполнено 0-56% заданий