Федеральное государственное бюджетное образовательное учреждение высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»

Экономический факультет

ОПОП по направлению подготовки
09.03.02 Информационные системы и технологии

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

Б1.О.22 Безопасность информационных технологий и систем

Направленность (профиль) «Информационные системы и технологии в бизнесе»

Обеспечивающая преподавание дисциплины кафедра	Кафедра экономики, бухгалтерского учета и финансового контроля
Разработчик, канд. экон. наук, доцент	В.В. Кузнецова

ВВЕДЕНИЕ

1. Фонд оценочных средств по дисциплине является обязательным обособленным приложением к Рабочей программе дисциплины.

2. Фонд оценочных средств является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися указанной дисциплины.

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

4. Фонд оценочных средств по дисциплине включает в себя: оценочные средства, применяемые для входного контроля; оценочные средства, применяемые в рамках индивидуализации выполнения, контроля фиксированных видов ВАРС; оценочные средства, применяемые для текущего контроля и оценочные средства, применяемые при промежуточной аттестации по итогам изучения дисциплины.

5. Разработчиками фонда оценочных средств по дисциплине являются преподаватели кафедры экономики, бухгалтерского учета и финансового контроля, обеспечивающей изучение обучающимися дисциплины в университете. Содержательной основой для разработки ФОС послужила Рабочая программа дисциплины.

.

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

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)
Общепрофессиональные 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$_{ОПК-3}$ Выбирает 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	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	Умеет использовать методы и средства для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности	Владеет методами и средствами для 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$_{ОПК-3}$ Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знает как применять информационно-коммуникационные технологий и с учетом основных требований информационной безопасности решает задачи профессиональной деятельности	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 методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
		ИД-3$_{ОПК-3}$ Участвует в подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Знает принципы, методы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Умеет составлять обзор, писать аннотации, рефераты, научные доклады, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности

ЧАСТЬ 2. ОБЩАЯ СХЕМА ОЦЕНИВАНИЯ ХОДА И РЕЗУЛЬТАТОВ ИЗУЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общие критерии оценки и реестр применяемых оценочных средств

2.1. Обзорная ведомость-матрица оценивания хода и результатов изучения учебной дисциплины в рамках педагогического контроля

Категория контроля и оценки		Режим контрольно-оценочных мероприятий				
		само-оценка	взаимо-оценка	Оценка со стороны		Комис-сионная оценка
				препода-вателя	представителя производства	
		1	2	3	4	5
Входной контроль	**1**					
Индивидуализация выполнения*, **контроль фиксированных видов ВАРС:**	**2**					
реферат	2.1			Проверка выполненной работы (реферата)		
Текущий контроль:	**3**					
Самостоятельное изучение тем		Вопросы изучаемой темы	Обсуждение изученных тем	Тест		
в рамках практических (семинарских) занятий и подготовки к ним	3.1	Вопросы темы занятия		Проверка выполненных лабораторных работ на занятиях		
в рамках обще-университетской системы контроля успеваемости	3.2					
Промежуточная аттестация* обучающихся по итогам изучения дисциплины	**4**			Итоговый тест, дифференцированный зачет		

* данным знаком помечены индивидуализируемые виды учебной работы

2.2. Общие критерии оценки хода и результатов изучения учебной дисциплины

1. Формальный критерий получения обучающимися положительной оценки по итогам изучения дисциплины:	
1.1. Предусмотренная программа изучения дисциплины обучающимся выполнена полностью до начала процесса промежуточной аттестации	1.2. По каждой из предусмотренных программой видов работ по дисциплине обучающийся успешно отчитался перед преподавателем, демонстрируя при этом должный (не ниже минимально приемлемого) уровень сформированности элементов компетенций
2. Группы неформальных критериев качественной оценки работы обучающегося в рамках изучения дисциплины:	
2.1 Критерии оценки качества хода процесса изучения обучающимся программы дисциплины (текущей успеваемости)	**2.2.** Критерии оценки качества выполнения конкретных видов ВАРС
2.3 Критерии оценки качественного уровня итоговых результатов изучения дисциплины	**2.4**. Критерии аттестационной оценки качественного уровня результатов изучения дисциплины

2.3 РЕЕСТР элементов фонда оценочных средств по учебной дисциплине

Группа оценочных средств	Оценочное средство или его элемент
	Наименование
1. Средства для индивидуализации выполнения, контроля фиксированных видов ВАРС	Перечень тем для написания реферата. Процедура выбора темы обучающимся
	Шкала и критерии оценки реферата
2. Средства для текущего контроля	Вопросы для самоподготовки по темам лабораторных занятий
	Критерии оценки самоподготовки по темам лабораторных занятий
	Примерные задания для лабораторных работ
3. Средства для промежуточной аттестации по итогам изучения дисциплины	Тестовые вопросы для проведения итогового тестирования
	Шкала и критерии оценки ответов на тестовые вопросы тестирования по итогам освоения дисциплины
	Плановая процедура проведения зачета

2.4. Описание показателей, критериев и шкал оценивания и этапов формирования компетенций в рамках дисциплины

<table>
<tr><td rowspan="9">Индекс и название компетенции</td><td rowspan="9">Код индикатора достижений компетенции</td><td rowspan="9">Индикаторы компетенции</td><td rowspan="9">Показатель оценивания – знания, умения, навыки (владения)</td><td colspan="4">Уровни сформированности компетенций</td><td rowspan="9">Формы и средства контроля формирования компетенций</td></tr>
<tr><td>компетенция не сформирована</td><td>минимальный</td><td>средний</td><td>высокий</td></tr>
<tr><td colspan="4">Оценки сформированности компетенций</td></tr>
<tr><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>Оценка «неудовлетворительно»</td><td>Оценка «удовлетворительно»</td><td>Оценка «хорошо»</td><td>Оценка «отлично»</td></tr>
<tr><td colspan="4">Характеристика сформированности компетенции</td></tr>
<tr><td>Компетенция в полной мере не сформирована. Имеющихся знаний, умений и навыков недостаточно для решения практических (профессиональных) задач</td><td>Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач</td><td>Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач</td><td>Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач</td></tr>
<tr><td colspan="9">Критерии оценивания</td></tr>
</table>

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$_{ОПК-3}$	Полнота знаний	Знает основные 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	Не знает 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	Поверхностно ориентируется в методах и средствах решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Твёрдо знает основные 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	Глубоко и прочно освоил применяемые 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	Тестирование, реферат, проверка выполненных лабораторных работ, опрос

Индекс 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				
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 информационной безопасности	ИД-1$_{ОПК-3}$	Наличие умений	Умеет использовать основные 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	Не умеет использовать основные 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	Умеет самостоятельно применять 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	Умеет правильно использует полученные знания при решении стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Имеет навыки применения методы и приемы информационной безопасности, использует информационно-коммуникационные технологии	Тестирование, реферат, проверка выполненных лабораторных работ, опрос
		Наличие навыков (владение опытом)	Владения основными принципами, методами и средствами 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 основными принципами, методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Имеет поверхностные навыки применения основных 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	Имеет навыки применения 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	Уверенно владеет навыками применения методами и приемами информационной безопасности, использует информационно-коммуникационные технологии	

Индекс 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				
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 информационной безопасности	ИД-2$_{ОПК-3}$	Полнота знаний	Знает методики 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 методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Поверхностно ориентируется в методиках решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Твердо знает методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	В совершенстве знает методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Тестирование, реферат, проверка выполненных лабораторных работ, опрос
		Наличие умений	Умеет применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Не умеет применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Умеет применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Умеет самостоятельно применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Умеет грамотно и самостоятельно применять методики решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	

Индекс 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				
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 информационной безопасности	ИД-2$_{ОПК-3}$	Наличие навыков (владение опытом)	Владение методикой 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 методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Имеет поверхностные навыки владения методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Имеет навыки владения методикой решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	В совершенстве владеет навыками применения методик решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Тестирование, реферат, проверка выполненных лабораторных работ, опрос
	ИД-3$_{ОПК-3}$	Полнота знаний	Знает принципы, методы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Не знает принципы, методы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Знает особенности принципов, методов подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Знает особенности принципов, методов подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности, но допускает небольшие ошибки.	В совершенстве знает особенности принципов, методов подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	

Индекс 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				
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 информационной безопасности	ИД-3$_{ОПК-3}$	Наличие умений	Умеет проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Не умеет проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Не умеет участвовать в подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Умеет проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Умеет грамотно проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Тестирование, реферат, проверка выполненных лабораторных работ, опрос
		Наличие навыков (владение опытом)	Владение методами и методиками проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Не владеет методами и методиками проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Имеет поверхностные навыки работы в проведении подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Имеет основные навыки в проведении подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	В совершенстве владеет методиками работы в подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	

ЧАСТЬ 3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Часть 3.1. Типовые контрольные задания, необходимые для оценки знаний, умений, навыков

3.1.1 . Средства
для индивидуализации выполнения, контроля фиксированных видов ВАРС

Выполнение и сдача рефератов

ПРИМЕРНАЯ ТЕМАТИКА
реферата

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
4. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
5. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
6. Информационная безопасность (по материалам зарубежных источников и литературы).
7. Правовые основы защиты конфиденциальной информации.
8. Экономические основы защиты конфиденциальной информации.
9. Организационные основы защиты конфиденциальной информации.
10. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
11. Составление инструкции по обработке и хранению конфиденциальных документов.
12. Направления и методы защиты документов на бумажных носителях.
13. Направления и методы защиты машиночитаемых документов.
14. Архивное хранение конфиденциальных документов.
15. Направления и методы защиты аудио- и визуальных документов.
16. Порядок подбора персонала для работы с конфиденциальной информацией.
17. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами организации.
18. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам организации.
19. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
20. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
21. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы. 22. Порядок защиты информации в рекламной и выставочной деятельности.
23. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
24. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной организации).
25. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
26. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
27. Назначение, виды, структура и технология функционирования системы защиты информации.
28. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
29. Аналитическая работа по выявлению каналов утечки информации организации.
30. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
31. Направления и методы защиты профессиональной тайны.
32. Направления и методы защиты служебной тайны.
33. Направления и методы защиты персональных данных о гражданах.
34. Методы защиты личной и семейной тайны.
35. Построение и функционирование защищенного документооборота.
36. Защита секретов в дореволюционной России.
37. Методика инструктирования и обучения персонала правилами защиты секретов организации.

Процедура выбора темы обучающимся

Очень важно правильно выбрать тему. Выбор темы не должен носить формальный характер, а иметь практическое и теоретическое обоснование.

Автор реферата должен осознанно выбрать тему с учетом его познавательных интересов. Если интересующая тема отсутствует в рекомендательном списке, то по согласованию с преподавателем обучающемуся предоставляется право самостоятельно предложить тему реферата, раскрывающую содержание изучаемой дисциплины. Тема не должна быть слишком общей и глобальной, так как небольшой объем работы (до 20 страниц) не позволит раскрыть ее.

При выборе темы необходимо учитывать полноту ее освещения в имеющейся научной литературе. Для этого можно воспользоваться тематическими каталогами библиотек и библиографическими указателями литературы, периодическими изданиями, либо справочно-библиографическими ссылками изданий посвященных данной теме.

После выбора темы составляется список изданной по теме (проблеме) литературы, опубликованных статей, необходимых справочных источников.

Знакомство с любой научной проблематикой следует начинать с освоения имеющейся основной научной литературы. При этом следует сразу же составлять библиографические выходные данные (автор, название, место и год издания, издательство, страницы) используемых источников. Названия работ иностранных авторов приводятся только на языке оригинала.

Начинать знакомство с избранной темой лучше всего с чтения обобщающих работ по данной проблеме, постепенно переходя к узкоспециальной литературе.

На основе анализа прочитанного и просмотренного материала по данной теме следует составить тезисы по основным смысловым блокам, с пометками, собственными суждениями и оценками. Предварительно подобранный в литературных источниках материал может превышать необходимый объем реферата, но его можно использовать для составления плана реферата.

ШКАЛА И КРИТЕРИИ ОЦЕНКИ
реферата

– «зачтено» Тема раскрыта. Продемонстрировано владение материалом. Использованы надлежащие источники в нужном количестве. Структура работы соответствует поставленным задачам. Степень самостоятельности работы высокая.
– «не зачтено» Тема не раскрыта. Продемонстрировано неудовлетворительное владение материалом. Использованные источники недостаточны. Структура работы не соответствует поставленным задачам. Работа несамостоятельна.

3.1.2. ВОПРОСЫ
для проведения входного контроля

не предусмотрено

3.1.3 Средства для текущего контроля

ВОПРОСЫ
для самостоятельного изучения темы
«Основные понятия теории информационной безопасности»

1. История становления информационной безопасности.
2. Основные термины и определения правовых понятий в области информационных отношений и защиты информации.
3. Предметная область теории информационной безопасности.

ВОПРОСЫ
для самостоятельного изучения темы
«Информация как объект защиты»

1. Понятие об информации как объекте защиты.
2. Уровни предоставления информации.
3. Виды и формы представления информации. Информационные ресурсы.

ВОПРОСЫ
для самостоятельного изучения темы
«Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности»

1. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.
2. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.

ВОПРОСЫ
для самостоятельного изучения темы
«Угрозы информационной безопасности»

1. Анализ уязвимостей системы.
2. Классификация угроз информационной безопасности.
3. Основные направления и методы реализации угроз.

ВОПРОСЫ
для самостоятельного изучения темы
«Построение систем защиты от угрозы нарушения конфиденциальности»

1. Определение и основные способы несанкционированного доступа.
2. Методы защиты от НСД.
3. Основные направления и цели использования криптографических методов.

ВОПРОСЫ
для самостоятельного изучения темы
«Построение системы защиты от угрозы нарушения целостности информации и отказа доступа»

1. Защита целостности информации при хранении.
2. Защита целостности информации при обработке.
3. Защита целостности информации при транспортировке.

ВОПРОСЫ
для самостоятельного изучения темы
«Политика и модели безопасности»

1. Политика безопасности.
2. Субъективно-объектные модели разграничения доступа.
3. Аксиомы политики безопасности.

ВОПРОСЫ
для самостоятельного изучения темы
«Обзор международных стандартов информационной безопасности»

1. Роль стандартов информационной безопасности.
2. Единые критерии безопасности информационных технологий.
3. Группа международных стандартов.

ВОПРОСЫ
для самостоятельного изучения темы
«Информационные войны и информационное противоборство»

1. Определение и основные виды информационных войн.
2. Информационно-техническая война.
3. Информационно-психологическая война.

Общий алгоритм самостоятельного изучения темы

1. Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме (ориентируясь на вопросы для самоконтроля)
2. На этой основе составить развёрнутый план изложения темы
3. Провести самоконтроль освоения темы по вопросам, выданным преподавателем
4. Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы – тестирование
5. Принять участие в указанном мероприятии, пройти тестирование по разделу на аудиторном занятии и заключительное тестирование в установленное для внеаудиторной работы время

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ
самостоятельного изучения темы

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

ВОПРОСЫ
для самоподготовки к лабораторным занятиям

В процессе подготовки к семинарскому занятию обучающийся изучает представленные ниже вопросы по темам. На занятии обучающийся демонстрирует свои знания по изученным вопросам в форме устного ответа. Для усвоения материала по теме занятия обучающийся выполняет лабораторные задания.

Тема. Построение системы защиты и угрозы нарушения

1. В чем отличие идентификации от аутентификации..
2. Основные направления и цели использования криптографических методов?
3. Посторение систем защиты от угрозы утечки по техническим каналам.

Тема. Построение системы защиты от угрозы нарушения целостности информации и отказа доступа

1. Основные понятия программно-технического уровня информационной безопасности.
2. Архитектурная безопасность – три принципа, содержащихся в приведенном утверждении.
3. Международные стандарты информационного обмена.
4. Безопасность в сетях Internet и Intranet.

Тема. Политика и модели безопасности

1. Модели анализа безопасности программного обеспечения.
2. Элементы политики безопасности.
3. Политка верхнего уровня, среднего уровня.
4. Мероприятия по управлению рисками.

Тема. Международные стандарты информационной безопасности

1 .«Оранжевая книга» как оценочный стандарт.
2. Шесть классов безопасности и их основные характеристики.
3. Сетевые механизмы безопасности.
4. Администрирование средств безопасности.
5. Руководящие документы Гостехкомиссии России.

Шкала и критерии оценивания
самоподготовки по темам лабораторных занятий

- оценка «зачтено» выставляется обучающемуся, если все вопросы темы раскрыты, во время дискуссии высказывается собственная точка зрения на обсуждаемую проблему, демонстрируется способность аргументировать доказываемые положения и выводы.

- оценка «не зачтено» выставляется, если обучающийся не способен доказать и аргументировать собственную точку зрения по изученной теме, не способен ссылаться на мнения ведущих специалистов по обсуждаемой проблеме.

Примерные задания для лабораторных работ

Лабораторная работа №1
Исследование информационной модели системы

Цель работы: Научиться основам исследования информационных систем, информационных потоков.

Задание для самостоятельного выполнения:
Получить у преподавателя описание информационной системы. Построить IDEF модель системы с информационными потоками.

Вопросы для контрольного опроса:
1. Что такое модель IDEF?
2. Каковы особенности взаимосвязи элементов системы?
3. Особенности композиции и декомпозиции системы.

Лабораторная работа №2
Выделение типов информации и формирование требований защиты информации

Цель работы: Научиться основам исследования информационных систем, информационных потоков.

Задание для самостоятельного выполнения:
По результатам лабораторной работы №1 оценить требования к информационным потокам системы. Определить требования к защите информации.

Вопросы для контрольного опроса:
1. Какие существуют угрозы для информации?
2. Как можно исключить эти угрозы?
3. Какие мероприятия применяются для устранения возможности возникновения угроз?
4. Какие мероприятия применяются для устранения последствий угроз?

Лабораторная работа №3
Разработка политик безопасности

Цель работы: Научиться основам работы с политиками безопасности.

Задание для самостоятельного выполнения:
Создать ограничивающие политики на уровне локальных политик, политик домена, политик компьютеров, политик пользователей, политик учетных записей.

Вопросы для контрольного опроса:
1. Что такое политики безопасности?
2. Что такое локальные политики безопасности?
3. Что такое политики безопасности домена?
4. Что такое политики безопасности контроллера домена?

Лабораторная работа №4
Изучение средств защиты информации в Windows XP

Цель работы: Научиться использованию средств защиты информации.

Задание для самостоятельного выполнения:
Для выбранных объектов установить права доступа и организовать аудит использования этих объектов

Вопросы для контрольного опроса:
1. Какие права имеются на использование файлов в Windows XP?
2. Какие права имеются на использование директорий в Windows XP?
3. Какие права имеются на использование исполняемых объектов в Windows XP?
4. Что такое аудит?

5. Какие действия с объектами можно контролировать?
6. Как организовать аудит?

Лабораторная работа №5
Изучение криптографических методов подстановки

Цель работы: Изучить особенности построения шифров простой замены.

Программное обеспечение: Среда программирования Delphi 7, Visual C или Borland CBuilder

Теоретический материал:

Системы подстановок

Определение Подстановкой на алфавите Z_m называется автоморфизм Z_m, при котором буквы исходного текста t замещены буквами шифрованного текста (t):

Z_m Z_m; : t (t).

Набор всех подстановок называется симметрической группой Z_m è будет в дальнейшем обозначаться как SYM(Z_m).

Утверждение SYM(Z_m) с операцией произведения является группой, т.е. операцией, обладающей следующими свойствами:

Замкнутость: произведение подстановок $_{12}$ является подстановкой:

: $t_1(_2(t))$.

Ассоциативность: результат произведения $_{123}$ не зависит от порядка расстановки скобок:

$(_{12})_3=_1(_{23})$

Существование нейтрального элемента: постановка i, определяемая как i(t)=t, 0t<m, является нейтральным элементом SYM(Z_m) по операции умножения: i=i для SYM(Z_m).

Существование обратного: для любой подстановки существует единственная обратная подстановка $^{-1}$, удовлетворяющая условию

$^1=\ ^1$=i.

Число возможных подстановок в симметрической группе Z_m называется *порядком* SYM(Z_m) и равно *m*!

.

Определение. Ключом подстановки *k* для Z_m называется последовательность элементов симметрической группы Z_m:

k=(p_0,p_1,...,p_{n-1},...), p_nSYM(Z_m), 0n<

Подстановка, определяемая ключом *k*, является криптографическим преобразованием T_k, при помощи которого осуществляется преобразование *n*-граммы исходного текста (x_0 ,x_1,..,x_{n-1}) в *n*-грамму шифрованного текста (y_0 ,y_1 ,...,y_{n-1}):

$y_i=p(x_i)$, 0i

где *n* – произвольное (n=1,2,..). T_k называется моноалфавитной подстановкой, если *p*неизменно при любом i, i=0,1,..., в противном случае T_k называется многоалфавитной подстановкой.

Примечание. К наиболее существенным особенностям подстановки T_k относятся следующие:

1. Исходный текст шифруется посимвольно. Шифрования *n*-граммы (x_0 ,x_1 ,..,x_{n-1}) и ее префикса (x_0 ,x_1 ,..,x_{s-1}) связаны соотношениями

$T_k(x_0$,x_1 ,..,$x_{n-1})=(y_0$,y_1 ,...,$y_{n-1})$

$T_k(x_0$,x_1 ,..,$x_{s-1})=(y_0$,y_1 ,...,$y_{s-1})$

2. *Буква шифрованного текста y_i является функцией только i-й компоненты ключа p_i и i-й буквы исходного текста* x_i.

Подстановка Цезаря

Подстановка Цезаря является самым простым вариантом подстановки. Она относится к группе *моноалфавитных подстановок*.

Определение. Подмножество C_m={C_k: 0*k*m), содержащее *m* подстановок

C_k: j(j+*k*) (mod *m*), 0*k* < *m*,

называется подстановкой Цезаря.

Умножение коммутативно, $C_kC_j=C_jC_k=C_{j+k}$, C_0 – идентичная подстановка, а обратной к C_kявляется $C_k^{-1}=C_{m-k}$, где 0<*k*3.

Подстановка определяется по таблице замещения, содержащей пары соответствующих букв “исходный текст – шифрованный текст”. Для C_3 подстановки приведены в Табл. 1. Стрелка () означает, что буква исходного текста (слева) шифруется при помощи C_3 в букву шифрованного текста (справа).

*Определение***.** *Системой Цезаря* называется моноалфавитная подстановка, преобразующая*n*-грамму исходного текста (x_0, x_1 ,..,x_{n-1}) в *n* грамму шифрованного текста (y_0 ,y_1 ,...,y_{n-1}) в соответствии с правилом

$y_i=C_k(x_i)$, 0i

Например, ВЫШЛИТЕ_НОВЫЕ_УКАЗАНИЯ посредством подстановки C_3 преобразуется в еюыолхиврсеюивцнгкгрлб.

При своей несложности система легко уязвима. Если злоумышленник имеет
1) шифрованный и соответствующий исходный текст или
2) шифрованный текст выбранного злоумышленником исходного текста,
то определение ключа и дешифрование исходного текста тривиальны.
Более эффективны обобщения подстановки Цезаря - *шифр Хилла* и *шифр Плэйфера*. Они основаны на подстановке не отдельных символов, а 2-грамм (шифр Плэйфера) или *n*-грамм[1] (шифр Хилла).
При более высокой криптостойкости они значительно сложнее для реализации и требуют достаточно большого количества ключевой информации.
Многоалфавитные системы. Системы одноразового использования.
Слабая криптостойкость моноалфавитных подстановок преодолевается с применением подстановок многоалфавитных.
Многоалфавитная подстановка определяется ключом =($_1$,
$_2$, ...), содержащим не менее двух различных подстановок. В начале рассмотрим многоалфавитные системы подстановок с нулевым начальным смещением.
Пусть {K_i: 0im
*P*кл{(K_0, K_1, ..., K_{n-1})=(k_0, k_1, ..., k_{n-1})}=(1/m)^n
Система одноразового использования преобразует исходный текст X=(X_0, x_1, ..., x_{n-1}) в шифрованный текст Y=(Y_0, y_1, ..., y_{n-1}) при помощи подстановки Цезаря

$$Y_i=C_{Ki}(x_i)=(K_i+X_i) \pmod m \quad i=0...n-1 \quad (1)$$

Для такой системы подстановки используют также термин “одноразовая лента” и “одноразовый блокнот”. Пространство ключей К системы одноразовой подстановки является вектором рангов (K_0, K_1, ..., K_{n-1}) и содержит m^n точек.
Рассмотрим небольшой пример шифрования с бесконечным ключом. В качестве ключа примем текст “БЕСКОНЕЧНЫЙ_КЛЮЧ....”.
Зашифруем с его помощью текст “ШИФР_НЕРАСКРЫВАЕМ”. Шифрование оформим в таблицу:

Исходный текст невозможно восстановить без ключа.
Наложение белого шума в виде бесконечного ключа на исходный текст меняет статистические характеристики языка источника. Системы одноразового использования*теоретически не расшифруемы*[2], так как не содержат достаточной информации для восстановления текста.
Почему же эти системы неприменимы для обеспечения секретности при обработке информации? Ответ простой - они непрактичны, так как требуют независимого выбора значения ключа для каждой буквы исходного текста. Хотя такое требование может быть и не слишком трудным при передаче по прямому кабелю Москва - Нью-Йорк, но для информационных оно непосильно, поскольку там придется шифровать многие миллионы знаков.
Посмотрим, что получится, если ослабить требование шифровать каждую букву исходного текста отдельным значением ключа.
Системы шифрования Вижинера
Начнем с конечной последовательности ключа
$k = (k_0 ,k_1 ,...,k_n)$,
которая называется *ключом пользователя*, и продлим ее до бесконечной последовательности, повторяя цепочку. Таким образом, получим *рабочий ключ*
$k = (k_0 ,k_1 ,...,k_n)$, $k_j = k_{(j \bmod r)}$, 0 j < .
Например, при r = и ключе пользователя 15 8 2 10 11 4 18 рабочий ключ будет периодической последовательностью:
15 8 2 10 11 4 18 15 8 2 10 11 4 18 15 8 2 10 11 4 18 ...
Определение. Подстановка Вижинера VIG_k определяется как
VIG_k : (x_0, x_1, ..., x_{n-1}) (y_0, y_1, ..., y_{n-1}) = (x_0+k, x_1+k,. .., x_{n-1}+k).
Таким образом:
1) исходный текст x делится на r *фрагментов* x_i = (x_i , x_{i+r} , ..., $x_{i+r(n-1)}$), 0 i < r;
2) i-й фрагмент исходного текста x_i шифруется при помощи подстановки Цезаря C_k :
(x_i , x_{i+r} , ..., $x_{i+r(n-1)}$) (y_i , y_{i+r} , ..., $y_{i+r(n-1)}$),
Вариант системы подстановок Вижинера при m=2 называется *системой Вернама (1917 г)*.
В то время ключ k=(k_0 ,k_1 ,...,$k_{к-1}$) записывался на бумажной ленте. Каждая буква исходного текста в алфавите, расширенном некоторыми дополнительными знаками, сначала переводилась с использованием *кода Бодо* в пятибитовый символ. К исходному тексту Бодо добавлялся ключ (по модулю 2). Старинный телетайп фирмы AT&T со считывающим устройством Вернама и оборудованием для шифрования, использовался корпусом связи армии США.
Очень распространена плохая с точки зрения секретности *практика использовать слово или фразу в качестве ключа* для того, чтобы k=(k_0 ,k_1 ,...,$k_{к-1}$) было легко запомнить. В ИС для обеспечения безопасности информации это недопустимо. Для получения ключей должны использоваться программные или аппаратные средства случайной генерации ключей.

Пример. Преобразование текста с помощью подстановки Вижинера (r=4)
Исходный текст (ИТ1):
НЕ_СЛЕДУЕТ_ВЫБИРАТЬ_НЕСЛУЧАЙНЫЙ_КЛЮЧ
Ключ: КЛЮЧ
Разобьем исходный текст на блоки по 4 символа:
НЕ_С ЛЕДУ ЕТ_В ЫБИР АТЬ_ НЕСЛ УЧАЙ НЫЙ_ КЛЮЧ
и наложим на них ключ (используя таблицу Вижинера):
Н+К=Ч, Е+Л=Р и т.д.
Получаем зашифрованный (ЗТ1) текст:
ЧРЭЗ ХРБЙ ПЭЭЩ ДМЕЖ КЭЩЦ ЧРОБ ЭБЮ_ ЧЕЖЦ ФЦЫН
Можно выдвинуть и обобщенную систему Вижинера. ЕЕ можно сформулировать не только при помощи подстановки Цезаря.
Пусть x - подмножество симметрической группы $SYM(Z_m)$.
Определение. *r-многоалфавитный ключ* шифрования есть r-набор = $(_0, _1, ..., _{r-1})$ с элементами в x.
Обобщенная система Вижинера преобразует исходный текст $(x_0, x_1, ..., x_{n-1})$ в шифрованный текст $(y_0, y_1, ..., y_{n-1})$ при помощи ключа = $(_0, _1, ..., _{r-1})$ по правилу
$VIG_k : (x_0, x_1, ..., x_{n-1})\ (y_0, y_1, ..., y_{n-1}) = (_0(x_0), _1(x_1), ..., _{n-1}(x_{n-1}))$,
где используется условие $_i = _{i \bmod r}$.
Следует признать, что и многоалфавитные подстановки в принципе доступны криптоаналитическому исследованию. Криптостойкость многоалфавитных систем резко убывает с уменьшением длины ключа.
Тем не менее такая система как шифр Вижинера допускает несложную аппаратную или программную реализацию и при достаточно большой длине ключа может быть использован в современных ИС.

Задание для самостоятельного выполнения:
Для шифра простой замены, используя генератор случайных чисел, построить таблицу замен. Написать программы шифрования и расшифровки, использующие таблицу замен.

Вопросы для контрольного опроса:
1. Что такое Система шифрования Цезаря?
2. Что такое Система шифрования Вижинера?
3. Что такое Шифр «двойной квадрат» Уитстона?
4. Чем отличаются моноалфавитные и многоалфавитные системы?
5. Что такое одноразовая система шифрования?
6. Как осуществляется шифрование методом Вернама?
7. Что такое Роторные машины.

Задание для самостоятельного выполнения:
Написать программы шифрования и расшифровки, использующие перестановку байт по ключу.

Вопросы для контрольного опроса:
Шифры перестановки.
Шифрующие таблицы.
Применение магических квадратов.
Шифры простой замены.
Полибианский квадрат.
Шифрование методом гаммирования.
Методы генерации псевдослучайных последовательностей чисел

Тестирование по темам 1-6

1) Что такое защита информации::
a) защита от несанкционированного доступа к информации
b) выпуск бронированных коробочек для дискет
c) комплекса мероприятий, направленных на обеспечение информационной безопасности

2) Что из перечисленного не относится к числу основных аспектов информационной безопасности:
a) доступность
b) целостность
c) защита от копирования
d) конфиденциальность

3) Компьютерная преступность в мире:
a) остается на одном уровне
b) снижается
c) растет

4) Что из перечисленного относится к числу основных аспектов информационной безопасности:
a) подлинность – аутентичность субъектов и объектов
b) целостность – актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения
c) стерильность – отсутствие недекларированных возможностей

5) Сложность обеспечения информационной безопасности является следствием:
a) невнимания широкой общественности к данной проблематике
b) все большей зависимости общества от информационных систем
c) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

6) Структурный подход опирается на:
a. семантическую декомпозицию
b. алгоритмическую декомпозицию
c. декомпозицию структур данных

7) Объектно-ориентированный подход использует:
a) семантическую декомпозицию
b) объектную декомпозицию
c) алгоритмическую декомпозицию

8) Метод объекта реализует волю:
a) вызвавшего его пользователя
b) владельца информационной системы
c) разработчика объекта

9)Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на просмотрщика файлов определенного формата могут быть наложены следующие ограничения:
a) запрет на чтение файлов, кроме просматриваемых и конфигурационных
b) запрет на изменение файлов, кроме просматриваемых и конфигурационных
c) запрет на изменение каких-либо файлов

10)Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что:
а)существует обширная литература по объектно-ориентированному подходу
б)объектно-ориентированный подход применим как на стадии проектирования информационных систем, так и при их реализации
в)объектно-ориентированный подход позволяет успешно справляться с модификацией сложных информационных систем

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ

ответов на тестовые вопросы тестирования

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

3.1.4. Средства для промежуточной аттестации по итогам изучения дисциплины

Промежуточная (семестровая) аттестация по курсу

Нормативная база проведения промежуточной аттестации обучающихся по результатам изучения дисциплины:	
Действующее «Положение о текущем контроле успеваемости, промежуточной аттестации обучающихся по программам высшего образования (бакалавриат, специалитет, магистратура) и среднего профессионального образования в ФГБОУ ВО Омский ГАУ»	
Основные характеристики промежуточной аттестации обучающихся по итогам изучения дисциплины	
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 зачёта в графике учебного процесса	1) участие обучающегося в процедуре получения зачёта осуществляется за счёт учебного времени (трудоёмкости), отведённого на изучение дисциплины
	2) процедура проводится в рамках ВАРО, на последней неделе семестра
Основные условия получения обучающимся зачёта:	1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине; 2) прошёл заключительное тестирование

ПРОЦЕДУРА ПРОВЕДЕНИЯ
зачета

1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине;

2) прошёл заключительное тестирование.

Заключительное тестирование по итогам изучения дисциплины

По итогам изучения дисциплины, обучающиеся проходят заключительное тестирование. Тестирование является формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин.

Подготовка к заключительному тестированию по итогам изучения дисциплины

Тестирование осуществляется по всем темам и разделам дисциплины, включая темы, выносимые на самостоятельное изучение.

Процедура тестирования ограничена во времени и предполагает максимальное сосредоточение обучающегося на выполнении теста, содержащего несколько тестовых заданий.

Тестирование проводится в письменной форме (на бумажном носителе). Тест включает в себя 30 вопросов. Время, отводимое на выполнение теста - 30 минут.

Бланк теста

Образец

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»

Тестирование по итогам освоения дисциплины
«Безопасность информационных технологий и систем»

Для обучающихся направления подготовки 09.03.02 Информационные системы и технологии

ФИО_____**группа**_____
Дата_____

Уважаемые обучающиеся!

Прежде чем приступить к выполнению заданий внимательно ознакомьтесь с инструкцией:

1. Отвечая на вопрос с выбором правильного ответа, правильный, на ваш взгляд, ответ (ответы) обведите в кружок.
2. В заданиях открытой формы впишите ответ в пропуск.
3. В заданиях на соответствие заполните таблицу.
4. В заданиях на правильную последовательность впишите порядковый номер в квадрат.
4. Время на выполнение теста – 30 минут
5. За каждый верный ответ Вы получаете 1 балл, за неверный – 0 баллов.

Желаем удачи!

Примерные тестовые задания

1) Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензируемых требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю называется:
a) дипломом
b) лицензией
c) патентом

2) Вредоносный код, который выглядит как функционально полезная программа, называется:
a) апплетом
b) троянской
c) математической

3) Целиком посвящена вопросам защиты информации. В статье Закона фигурируют все три основных аспекта информационной безопасности: доступность, целостность и конфиденциальность. Кроме того, обязательным является отслеживание нарушений безопасности и постоянный контроль за обеспечением уровня защищенности информации:
a) Статья 27
b) Статья 15
c) Статья 16
закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года номер 149-ФЗ (принят Государственной Думой 8 июля 2006 года). Редакция от 09.03.2021 (с изм. и доп., вступ. в силу с 20.03.2021).

4) Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и:
a) аппаратные средства
b) программы
c) сети.

5) Агрессивное потребление ресурсов является угрозой:
a) доступности
b) конфиденциальности
c) целостности

6) Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности :
a)просчеты при администрировании информационных систем
b)необходимость постоянной модификации информационных систем
c)сложность современных информационных систем

7) Самыми опасными источниками внутренних угроз являются:
a) некомпетентные руководители
b) обиженные сотрудники
c) любобытные администраторы

8) Melissa подвергает атаке на доступность:
a) системы электронной коммерции
b) геоинформационные системы
c) системы электронной почты

9) Спектр интересов, связанных с использованием информационных систем, можно разделить на следующие категории:
Обеспечение доступности, целостности, конфиденциальности информационных ресурсов и
_____
a) информационных услуг
b) поддерживающей инфраструктуры
c) сведения о технических каналах утечки информации

10) Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают:
а)средства выявления злоумышленной активности
б)средства обеспечения отказоустойчивости
в)средства контроля эффективности защиты информации

11) Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:
а)выработка и проведение в жизнь единой политики безопасности
б)унификация аппаратно-программных платформ
в)минимизация числа используемых приложений

12) Назначение принципа минимизации привилегий:
а)уменьшить ущерб от случайных или умышленных некорректных действий:
б)идентификация ресурсов, необходимых для выполнения критически важных функций
в)подготовиться к авариям

13) Меры физического управления доступом позволяют контролировать и при необходимости ограничивать:
а)конфигурационное управление персонала
б)вход и выход сотрудников и посетителей
в)выявление критически важных функций организации и установление приоритетов

14) На процедурном уровне можно выделить следующие классы мер:
а)управление персоналом
б)физическая защита
в)поддержание работоспособности
г)реагирование на нарушения режима безопасности
д)применение административных мер к персоналу
е)планирование восстановительных работ

15) Процесс планирования восстановительных работ можно разделить на следующие этапы:
а)выявление критически важных функций организации, установление приоритетов
б)идентификация ресурсов, необходимых для выполнения критически важных функций
в)определение перечня возможных аварий
г)разработка стратегии восстановительных работ
д)сертификация важных функций
е)подготовка к реализации выбранной стратегии
ж)проверка стратегии

Что не относится к этому процессу?

16) Уровень безопасности B, согласно «Оранжевой книге», характеризуется:
а)произвольным управлением доступом
б)принудительным управлением доступом
в)верифицируемой безопасностью

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ

ответов на тестовые вопросы тестирования по итогам освоения дисциплины

- оценка «отлично» выставляется обучающемуся, если получено более 81% правильных ответов.
- оценка «хорошо» - получено от 71 до 80% правильных ответов.
- оценка «удовлетворительно» - получено от 61 до 70% правильных ответов.
- оценка «неудовлетворительно» - получено менее 61% правильных ответов.

ЛИСТ РАССМОТРЕНИЙ И ОДОБРЕНИЙ

Фонд оценочных средств учебной дисциплины Б1.О.22 Безопасность информационных технологий и систем
в составе ОПОП 09.03.02 Информационные системы и технологии

1. Рассмотрен и одобрен в качестве базового варианта:

а) На заседании обеспечивающей кафедры экономики, бухгалтерского учета и финансового контроля

протокол № 11 от 19.05.2022.

Зав. кафедрой, канд. экон. наук, доцент _____ О.А. Блинов

б) На заседании методической комиссии по направлению 09.03.02 Информационные системы и технологии

протокол № 9 от 24.05.2022.

Председатель МКН – 09.03.02, канд. экон. наук _____ С.А. Нардина

2. Рассмотрен и одобрен внешним экспертом

Директор ООО «Сатори Партнер» _____ А.Б. Мальцев

М.П.

ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ
к фонду оценочных средств учебной дисциплины
Б1.О.22 Безопасность информационных технологий и систем
в составе ОПОП 09.03.02 Информационные системы и технологии

Ведомость изменений

Срок, с которого вводится изменение	Номер и основное содержание изменения и/или дополнения	Отметка об утверждении/ согласовании изменений	
		инициатор изменения	руководитель ОПОП или председатель МКН