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

Тарский филиал
Факультет высшего образования

ОПОП по направлению 38.03.01 Экономика

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

Б1.О.33 Информационная безопасность

Направленность (профиль) «Бухгалтерский учет, анализ и аудит»

ВВЕДЕНИЕ

1. Фонд оценочных средств по дисциплине является обязательным обособленным приложением к Рабочей программе учебной 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 учебной 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; оценочные средства, применяемые для рубежного контроля и оценочные средства, применяемые при промежуточной аттестации по итогам изучения дисциплины.

5. Разработчиками фонда оценочных средств по дисциплине являются преподаватели кафедры гуманитарных, социально-экономических и фундаментальных дисциплин, обеспечивающей изучение обучающимися дисциплины в университете. Содержательной основой для разработки ФОС послужила Рабочая программа учебной 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)
1			2	3	4
Профессиональные компетенции					
ОПК-5	Способность применять знания (на промежуточном уровне) экономической теории при решении прикладных задач;	ИД-1$_{опк-5}$ применяет современные информационные технологии и программные средства для поиска и обработки экономической информации	современные технические средства и информационные технологии	использовать современные технические средства и информационные технологии для поиска и обработки экономической информации	владеть навыками применения современных технических средств и информационных технологий для поиска и обработки экономической информации

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	взаимооценка	препода-вателя	Комиссионная оценка
Входной контроль	**1**			-	
Индивидуализация выполнения*, **контроль фиксированных видов ВАРС:**	**2**				
- контрольная для заочной формы обучения	2.1			Проверка выполненной контрольной работы	
- презентация для очной и очно-заочнойформы	2.2			Проверка презентаций	
Текущий контроль:	**3**				
- самостоятельное изучение тем	3.1			Презентация для очной и очно-заочной форм обучения; опрос для заочной формы обучения	
- в рамках лабораторных занятий и подготовки к ним	3.2	Вопросы для самоподготовки		Провести анализ безопасности информации в социальной сети	

- в рамках обще-университетской системы контроля успеваемости	3.2				
- по итогам изучения 1 -3 разделов	3.4			Тестирование	
Итоговый контроль	**4**			Тестирование	

2.2 Общие критерии оценки хода и результатов изучения учебной дисциплины

1. Формальный критерий получения студентом 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 студента в рамках изучения дисциплины:	
2.1 Критерии оценки качества хода процесса изучения обучающимся программы дисциплины (текущей успеваемости)	**2.2.** Шкала и критерии оценивания качества выполнения конкретных видов ВАРС
2.3 Критерии оценки качественного уровня рубежных результатов изучения дисциплины	**2.4**. Шкала и критерии аттестационной оценки* качественного уровня результатов изучения дисциплины
* дифференцированного зачета	

2.3 РЕЕСТР элементов фонда оценочных средств по учебной дисциплине

Группа оценочных средств	Оценочное средство или его элемент
	Наименование
1. Средства для входного контроля	
2. Средства для индивидуализации выполнения, контроля фиксированных видов ВАРС	Перечень тем для выполнения презентации для очной и очно-заочной формы обучения
	Общий алгоритм подготовки презентации для очной и очно-заочной форм обучения
	Критерии оценки индивидуальных результатов выполнения презентации для очной и очно-заочной форм обучения
	Перечень вопросов для контрольной работы для заочной формы обучения
	Критерии оценки индивидуальных результатов выполнения контрольной работы для заочной формы обучения
3. Средства для текущего контроля	Перечень вопросов для самостоятельного изучения тем
	Общий алгоритм самостоятельного изучения темы
	Критерии оценки самостоятельного изучения темы
	Задания к лабораторным занятиям
	Общий алгоритм подготовки к лабораторной работе
	Критерии оценки самоподготовки по темам лабораторных занятий
	Шкала и критерии оценивания самоподготовки по темам лабораторных занятий
	Тестовые вопросы для проведения текущего контроля
	Шкала и критерии оценки ответов на тестовые вопросы текущего контроля
4. Средства для промежуточной аттестации по итогам изучения дисциплины	Тестовые вопросы для проведения итогового контроля
	Критерии оценки ответов на тестовые вопросы итогового контроля

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

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				
				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	
Критерии оценивания								
ОПК -5	ИД-1$_{опк-5}$	Полнота **знаний**	современные информационные технологии и программные средства для поиска и обработки экономической информации	Не знает современные информационные технологии и программные средства для поиска и обработки экономической информации	Знаком с современными информационными технологиями и программными средствами для поиска и обработки экономической информации	Знает современные информационные технологии и программные средства	Знает современные информационные технологии и программные средства и применяет для поиска и обработки экономической информации	Тестирование; опрос; индивидуальное задание, контрольная работа для заочной формы, презентация для очной и очно-заочной формы
		Наличие **умений**	использовать современные информационные технологии и программные средства для поиска и обработки экономической информации	Не умеет использовать современные информационные технологии и программные средства для поиска и обработки экономической информации	Умеет использовать информационные технологии	Умеет использовать современные информационные технологии и программные средства	В совершенстве использует современные информационные технологии и программные средства для поиска и обработки экономической информации	
		Наличие **навыков** (владение опытом)	навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации	Не владеет навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации	Владеет навыками применения информационных технологий и программными средствами	Владеет навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации	В совершенстве владеет навыками применения современных информационных технологий и программными средствами для поиска и обработки экономической информации	

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

Средства
для индивидуализации выполнения, контроля фиксированных видов ВАРС
Темы для оформления презентации для очной и очно-заочной форм обучения

1. Информационная безопасность в социальных сетях;
2. Безопасность применения платежных систем – законодательство и практика.
3. Принципы работы с электронной почтой. Создание почтовых ящиков на общедоступных сайтах и на серверах учреждений. Адресная книга.
4. Угрозы паролям.
5. Сравнительная характеристика антивирусных программ.
6. Законодательство о персональных данных.
7. Безопасность применения пластиковых карт – законодательство и практика.
8. Идентификация по голосу. Скрытые возможности.
9. Бухгалтерская отчетность как источник рассекречивания информации.
10. Информационная безопасность: экономические аспекты.
11. Безопасность розничной торговли.
12. Биопаспорт.
13. Сравнительная характеристика симметричных и ассиметричных методов шифрования.
14. Особенности и проблемы применения биометрических средств защиты информации.
15. Ответственность за нарушения в сфере информационного права.

Рекомендации по оформлению презентации

Презентация начинается с титульного листа, содержащего ее название и, возможно, имена авторов. Эти элементы обычно выделяются более крупным шрифтом, чем основной текст работы. Также на первый слайд целесообразно поместить логотип ВУЗа, от лица которой делается презентация. В качестве фона первого листа можно использовать рисунок или фотографию, имеющую непосредственное отношение к теме работы, однако текст поверх такого изображения должен читаться очень легко. Подобное правило соблюдается и для фона остальных листов (см. ниже). Тем не менее, монотонный фон или фон в виде мягкого градиента будет смотреться на первом листе тоже вполне эффектно.

Для оформления работы следует использовать стандартные, широко распространенные пропорциональные шрифты, такие как Arial, Tahoma, Verdana, Times New Roman, Georgia и др.

Для работы изначально необходимо подобрать цветовую гамму: обычно это три—пять цветов, среди которых есть как теплые, так и холодные. Очевидно, любой из этих цветов должен отлично читаться на выбранном ранее фоне; малейшее подозрение на то, что цвет шрифта хотя бы немного сливается с фоном — и что-то одно из этого подлежит немедленной замене: не вынуждайте тех, для кого делается презентация, портить зрение.

Ни в коем случае не стоит стараться разместить на одном листе как можно больше текста. Для того, чтобы прочесть мелкий текст, многим необходимо существенно напрягать зрение, и, скорее всего, по своей воле никто это- го делать не будет. Поэтому, чем больше текста на одном листе вы предложите аудитории, тем с меньшей вероятностью она его прочитает.

Хорошо известно, что любая речь воспринимается намного лучше, если она произносится докладчиком, обратившим свой взор к слушателям, фактически, находящимся с аудиторией в прямом зрительном контакте. Если же докладчик начинает читать с листа, то эффективность передачи информации значительно снижается. И уж совсем нелепо выглядит человек, делающий презентацию, когда ему приходится читать текст непосредственно со слайда. В этом случае слушатели, как правило, перестают и слушать, и читать то, что изображено на экране. Докладчику, потерявшему в такой момент внимание аудитории, очень сложно вернуть его в дальнейшем. Старайтесь не использовать текст на слайде как часть вашей речи; лучше поместите туда важные тезисы и лишь один—два раза обернитесь к ним, посвятив остальное время непосредственной коммуникации с вашими слушателями. Обязательно иллюстрируйте презентацию рисунками, фотографиями, наглядными схемами, графиками и диаграммами. Яркие картинки привлекают внимание куда эффективнее, чем сухой текст или, порой, даже очень неплохая речь. Изображению всегда следует придавать как можно больший размер; если это

возможно, иллюстрации стоит распределить по нескольким слайдам, нежели размещать их на одном но в уменьшенном виде. Подписи вполне допустимо располагать не над и не под изображением, а сбоку, если оно, например, имеет вертикальную ориентацию. Нет ничего забавнее, чем маленькая картинка и подпись к ней, выполненная крупным шрифтом.

И, наконец, завершать работу следует кратким резюме, содержащим ее основные положения, важные данные.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ ПРЕЗЕНТАЦИИ
для очной и очно-заочной форм обучения

Оценка «зачтено» выставляется обучающемуся при соблюдении следующих условий:

- содержание задания полностью соответствует ее теме;
-высокая/достаточная/приемлемая полнота и глубина раскрытия темы презентации;
- степень самостоятельности обучающегося при подготовке презентации не вызывает сомнения;
- общие требования к оформлению презентации соблюдены полностью/ соблюдены на приемлемом уровне;
- уровень понимания обучающимся материала, отражённого в презентации, соответствует требуемому полностью/находится на приемлемом уровне.

Оценка «не зачтено» выставляется обучающемуся при соблюдении следующих условий:

- содержание презентации не соответствует ее теме;
- не приемлемая полнота и глубина раскрытия темы презентации;
- степень самостоятельности обучающимся при подготовке презентации вызывает сомнения;
- уровень понимания обучающимся материала, не соответствует минимально требуемому.

Перечень заданий для контрольных работ
обучающихся заочной формы обучения

1. Настройка безопасности ОС Windows при работе в сети
2. Организация мер по защите
3. Разработка методики противодействия социальному инжинирингу
4. Организация антивирусной защиты частного предприятия с 25-ю рабочими станциями
5. Отправка сообщения в будущее
6. Криптографические системы защиты данных
7. Преступления в сфере компьютерной информации
8. Компьютерная преступность и компьютерная безопасность
9. Ответственность за нарушения в сфере информационного права
10. Комплекс технических решений по защите информации, записанной на отчуждаемых электронных носителях.
11. Проектирование системы информационной безопасности
12. Современные угрозы и каналы утечки информации в компьютерных сетях
13. Правовая охрана программ для ЭВМ и баз данных
14. Рекреационная геграфия
15. Настройка параметров безопасности операционной системы Windows
16. Оптимизация ОС Windows Vista с целью обеспечения информационной безопасности
17. Администрирование ОС Windows
18. Безопасность файловых ресурсов сети Windows
19. Разработка программы приема и передачи сообщений в локальной сети Microsoft
20. Оценка и анализ структуры системы защиты информации
21. Методы защиты информации в телекоммуникационных сетях
22. Защита информации от несанкционированного доступа методом криптопреобразования
23. Преступления в сфере компьютерной информации : криминологический анализ
24. Общая характеристика преступлений в сфере компьютерной информации
25. Понятие и характеристика преступлений в сфере компьютерной информации
26. Расследование преступлений в сфере компьютерной информации
27. Практика привлечения к административной ответственности лиц, совершивших правонарушения в области избирательного права
28. Правовые основы обеспечения информационной безопасности Российской Федерации
29. Проблемы защиты информации
30. Информационное право и правовая защита информации
31. Правовое регулирование в сфере защиты информации
32. Проектирование системы информационной безопасности

33. Современные угрозы и каналы утечки информации в компьютерных сетях
34. Антивирусная защита ПО для серверов
35. Принципы работы с электронной почтой. Создание почтовых ящиков на общедоступных сайтах и на серверах учреждений. Адресная книга. Настройка Outlook Express
36. Организация и функционирование электронной почты
37. Защита электронной почты в Internet
38. Электронная почта как сервис глобальной сети. Протоколы передачи почты
39. Защита информации в Интернет
40. Системы обнаружения атак. (Анализаторы сетевых протоколов и сетевые мониторы)
41. Спам и нормы пользования сетью
42. Российский рынок информационной безопасности
43. Информация и личная безопасность
44. Компьютерная преступность в России.
45. Пользователи и злоумышленники сети Internet.
46. Защита от сбоев в электропитании. Источники бесперебойного питания: назначение, характеристики, принципы работы.
47. Защита от формирования электромагнитных полей (излучений). Средства защиты кабельной системы.
48. Средства защиты от сбоев в работе устройств хранения информации.
49. Биометрические средства и технологии установления подлинности.
50. Особенности и проблемы применения биометрических средств защиты информации.
51. Угрозы паролям.
52. Модели разграничения прав доступа.
53. Использование цифровой подписи и хэш-функций.
54. Понятие цифровых сертификатов.
55. Стандарт шифрования AES.
56. Стандарт шифрования RIJNDAEL.
57. Сравнительная характеристика симметричных и ассиметричных методов шифрования.
58. Структура современных компьютерных вирусов.
59. Подробное описание основных классов вирусов.
60. Троянские вирусы.
61. Вирусы - черви.
62. Полиморфные и стелс - вирусы.
63. Политика безопасности антивирусных программ.
64. Сравнительная характеристика антивирусных программ.
65. Политика безопасности брандмауэра.
66. Фильтрация пакетов: достоинства и недостатки.
67. Прокси - серверы.
68. Особенности защиты баз данных.
69. Стандарты защищенности.
70. Методы борьбы с фишинговыми атаками.
71. Законодательство о персональных данных.
72. Защита авторских прав.
73. Назначение, функции и типы систем видеозащиты.
74. Как подписывать с помощью ЭЦП электронные документы различных форматов.
75. Обзор угроз и технологий защиты Wi-Fi-сетей.
76. Проблемы внедрения дискового шифрования.
77. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
78. Особенности процессов аутентификации в корпоративной среде.
79. Квантовая криптография.
80. Утечки информации: как избежать. Безопасность смартфонов.
81. Безопасность применения пластиковых карт - законодательство и практика.
82. Защита CD- и DVD-дисковот копирования.
83. Современные угрозы и защита электронной почты.
84. Программные средства анализа локальных сетей на предмет уязвимостей.
85. Безопасность применения платежных систем - законодательство и практика.
86. Аудит программного кода по требованиям безопасности.
87. Антишпионское ПО (antispyware).
88. Обеспечение безопасности Web-сервисов.
89. Защита от внутренних угроз.
90. Технологии RFID.
91. Уничтожение информации на магнитных носителях.
92. Ботнеты - плацдарм современных кибератак.

93. Цифровые водяные знаки в изображениях.
94. Электронный документооборот. Модели нарушителя.
95. Идентификация по голосу. Скрытые возможности.
96. Безопасность океанских портов.
97. Безопасность связи.
98. Безопасность розничной торговли.
99. Банковская безопасность.
100. Информатизация управления транспортной безопасностью.
101. Биопаспорт.
102. Обзор современных платформ архивации данных.
103. Что такое консалтинг в области ИБ.
104. Бухгалтерская отчетность как источник рассекречивания информации.
105. Управление рисками: обзор употребительных подходов.
106. Категорирование информации и информационных систем.
107. Обеспечение базового уровня информационной безопасности.
108. Распределенные атаки на распределенные системы.
109. Оценка безопасности автоматизированных систем.
110. Функциональная безопасность программных средств.
111. Технологические процессы и стандарты обеспечения функциональной безопасности в
112. жизненном цикле программных средств.
113. Информационная безопасность: экономические аспекты.

Тема контрольной работы выбирается по последней цифре номера зачетной книжки.

Шкала и критерии оценивания контрольной работы для заочной формы обучения

Оценка «зачтено» выставляется обучающемуся при соблюдении следующих условий:
- содержание задания полностью соответствует ее теме;
- высокая/достаточная/приемлемая полнота и глубина раскрытия темы контрольной работы;
- степень самостоятельности обучающегося при подготовке контрольной работы не вызывает сомнения;
- общие требования к оформлению контрольной работы соблюдены полностью/ соблюдены на приемлемом уровне;
- уровень понимания обучающимся материала, отражённого в контрольной работе, соответствует требуемому полностью/находится на приемлемом уровне.

Оценка «не зачтено» выставляется обучающемуся при соблюдении следующих условий:
- содержание контрольной работы не соответствует ее теме;
- не приемлемая полнота и глубина раскрытия темы контрольной работы;
- степень самостоятельности обучающимся при подготовке контрольной работы вызывает сомнения;
- уровень понимания обучающимся материала, не соответствует минимально требуемому.

3.2 ВОПРОСЫ
для самостоятельного изучения тем

Очная/ очно-заочная форма обучения
Эффективные меры антивирусной защиты
Новейшие аппаратные средства защиты информации

Заочная форма обучения
Эффективные меры антивирусной защиты
Новейшие аппаратные средства защиты информации
Новейшие программные средства защиты информации

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) Выбрать форму отчетности конспектов – презентация (для обучающихся очной и очно-заочной форм обчения)
2) Оформить отчётный материал в установленной форме в соответствии методическими рекомендаци
3) Провести самоконтроль освоения темы по вопросам, выданным преподавателем
4) Предоставить отчётный материал преподавателю по согласованию с ведущим преподавателем
5) Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы
6) Принять участие в указанном мероприятии, пройти рубежное тестирование по разделу на аудиторн занятии и заключительное тестирование в установленное для внеаудиторной работы время

ВОПРОСЫ
для самостоятельного изучения темы
«Эффективные меры антивирусной защиты»

1. Как называется этап, в ходе которого вирусный код может воспроизводить себя в теле других программ?
2. Как, одним словом можно назвать вредоносную программу?
3. Как называются вирусы, использующие для распространения сетевые ресурсы?
4. От какого типа вирусов заражение компьютера происходит при открытии файла?
5. Как называется класс вирусов, которые при воздействии не мешают работе компьютера?
6. Как называется программа, предназначенная для устранения вирусов?
7. К какому виду антивирусных программ относится Avast?

Общий алгоритм самостоятельного изучения темы

1) Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме (ориентируясь на вопросы, выданные преподавателем для подготовки к лабораторному занятию)
2) Провести самоконтроль освоения темы по вопросам, выданным преподавателем
3) Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы (опросу)

ВОПРОСЫ
для самостоятельного изучения темы
«Новейшие аппаратные средства защиты информации»

1. Понятие вредоносной программы.
2. Механизмы статического скрытия вредоносного программного кода.
3. Механизмы скрытности вредоносных программ на этапе выполнения.
4. Классификация и основные особенности различных видов вредоносных про- грамм.
5. Вредоносные действия компьютерных программ, приводящие к несанкционированной модификации компьютерной информации.
6. Вредоносные действия компьютерных программ, приводящие к несанкционированному удалению и блокированию компьютерной информации.
7. Виды программно-управляемого копирования компьютерной информации.
8. Программные нарушения работы ЭВМ и их виды.
9. Способы подготовки вредоносных программ к безусловному запуску.
10. Возможности программных закладок. Виды и способы программного пере- хвата компьютерной информации.
11. Компьютерные вирусы: их виды, особенности вирусного инфицирования, используемые деструктивные действия.

12. Особенности распространения и функционирования вредоносных программ сетевого типа.

13. Понятие о «троянских» программах и их функциях. Программы-«джойнеры».

14. Способы скрытого внедрения и запуска вредоносных программ в интерактивном режиме.

15. Виды автоматического запуска вредоносных программ

16. Традиционные способы антивирусной защиты и сравнительная оценка их эффективности.

Общий алгоритм самостоятельного изучения темы

1) Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме (ориентируясь на вопросы, выданные преподавателем для подготовки к лабораторному занятию)
2) Провести самоконтроль освоения темы по вопросам, выданным преподавателем
3) Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы (опросу)

ВОПРОСЫ
для самостоятельного изучения темы
«Новейшие программные средства защиты информации»

1. Пакеты прикладных программ автоматизированных рабочих мест (АРМ).
2. Базы данных вычислительных сетей.
3. Программные средства автоматизированных систем управления (АСУ).
4. Программные средства идентификации изготовителя программного (информационного) продукта, включая средства идентификации авторского права.

Общий алгоритм самостоятельного изучения темы

1) Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме (ориентируясь на вопросы, выданные преподавателем для подготовки к лабораторному занятию)
2) Провести самоконтроль освоения темы по вопросам, выданным преподавателем
3) Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы (опросу)

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ ОПРОСА
для заочной формы обучения

- оценка «зачтено» по самостоятельно изученной теме выставляется обучающемуся, если он, принимал активное участие в обсуждении темы на лабораторной занятии, а именно: выступил на лабораторном занятии по одному или нескольким вопросам темы, дал обоснованные ответы на вопросы, задавал вопросы по теме другим обучающимися.

- оценка «не зачтено» по самостоятельно изученной теме выставляется обучающемуся, если он, не принимал активное участие в обсуждении темы на лабораторном занятии, а именно: не выступил на лабораторном занятии по одному или нескольким вопросам темы, не дал обоснованные ответы на вопросы, не задавал вопросы по теме другим обучающимися.

Часть 3.3 Средства для текущего контроля

ЗАДАНИЕ
к лабораторным занятиям

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ

Социальная сеть — платформа, онлайн-сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений, визуализацией которых являются социальные графы.

Характерными особенностями социальной сети являются:

– создание личных профилей (публичных или полупубличных), в которых зачастую требуется указать реальные персональные данные и другую информацию о себе (место учёбы и работы, хобби, жизненные принципы и др.);
– предоставление практически полного спектра возможностей для обмена информацией (размещение фотографий, видео-записей, размещение текстовых записей (в режиме блогов или микроблогов), организация тематических сообществ, обмен личными сообщениями и т. п.);
– возможность задавать и поддерживать список других пользователей, с которыми у него имеются некоторые отношения (например, дружбы, родства, деловых и рабочих связей и т. п.)

Популярность в Интернете социальные сети начали завоёвывать в 1995 году, с появлением американского портала Classmates.com («Одноклассники» являются его русским аналогом). Проект оказался весьма успешным, что в следующие несколько лет спровоцировало появление не одного десятка аналогичных сервисов. Но официальным началом бума социальных сетей принято считать 2003—2004 гг., когда были запущены LinkedIn, MySpace и Facebook.

Цель лабораторной работы: исследовать защищенность информации пользователя в различных типах социальных сетей и провести сравнительный анализ, выявив наиболее безопасную из них.

В рамках лабораторной работы следует познакомится с такими социальными сетями, как: **Facebook,** Instagram, **Google+, LinkedIn,** MySpace, **ВКонтакте, Одноклассники.**

Изучите материалы касающиеся информационной безопасности в социальных сетях, как представленные Вам в рамках лабораторной работы, так и размещенные в сети Интернет.

На основании полученной информации, выберите 7 критериев, так или иначе характеризующих информационную безопасность по которым Вы будете сравнивать социальные сети между собой.

Лабораторная работа выполняется индивидуально. *Примечание: обучающийся может выбрать свои критерии.*

Расставьте значимость критериев (весомость) в системе оценки, так чтобы общая сумма составляла 100. Это позволит Вам ранжировать важность критерия в общей системе оценки. ***Весомость проставляется по согласованию мнения всех участников группы!!!!*** Заполните таблицу 1.

Таблица 1

Выбор критериев информационной безопасности социальной сети и оценка их значимости

Критерии	***Весомость***
1.	
2.	
3.	
4.	
5.	
6.	
7.	
И	

Проведите анализ безопасности информации в социальной сети по всем выбранным Вами критериям, информацию по каждой программе занесите в таблицы 2-6. ***Каждый студент сам заполняет свои таблицы, излагая там свои аргументы!!!!*** Затем оцените представленные результаты по пятибалльной шкале и занесите результаты в таблицу 7.

Рассчитайте среднюю оценку исходя из мнения четырех экспертов, которыми выступаете Вы. Рассчитайте комплексный критерий ИБ. Заполните таблицу 8.

Задание можно выполнять как в тетради, так и в файле. Электронный отчет сдается преподавателю путем отправки на электронную почту каждым студентом, так как таблицы 2-6 у Вас разные. Электронный адрес: tv.monastyreva@omgau.org

Таблица 2

Информационная безопасность Facbook

Критерии	Оценка качества критерия

Таблица 3

Информационная безопасность сети вВКонтакте

Критерии	Оценка качества критерия

Таблица 4

Информационная безопасность социально сети Googl+

Критерии	Оценка качества критерия

Таблица 5

Информационная безопасность социально сети LinkedIn

Критерии	Оценка качества критерия

Таблица 6

Информационная безопасность социально сети Одноклассники

Критерии	Оценка качества критерия

Таблица 7

Бальная оценка качеств социальных сетей по заданным критериям

Критерии	Facebook					ВКонтакте					Google+					LinkedIn					Одноклассники				
	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Средняя оценка	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Средняя оценка	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Средняя оценка	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Средняя оценка	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Средняя оценка
1																									
2																									
3																									
4																									
5																									
6																									
7																									

Таблица 8

Оценка уровня информационной безопасности социальной сети

Критерии	Facebook		ВКонтакте		Google+		LinkedIn		Одноклас-сники	
	Средняя оценка	Средняя оценка * Весомость	Средняя оценка	Средняя оценка * Весомость	Средняя оценка	Средняя оценка * Весомость	Средняя оценка	Средняя оценка * Весомость	Средняя оценка	Средняя оценка * Весомость
1										
2										
3										
4										
5										
6										
7										
Комплексный критерий (итого)	x		x		x		x		x	

БЕЗОПАСНОСТЬ ПЛАТЕЖЕЙ В СЕТИ ИНТЕРНЕТ

Изучите информацию в сети Интернет:

1) http://bankir.ru/tehnologii/s/bezopasnost-i-zaschita-internet-platejei-5899180/
2) http://trustorg.com/article/34
3) http://finbrok.ru/moshenniki/9-bezopasnost-internetplatezhej.html
4) http://samoucka.ru/document14559.html

Ответьте на следующие вопросы:

1. Что такое SSL (Secure Socked Layer)? Как он применяется при защите коммерческой информации в сети Интернет?
2. Охарактеризуйте такой способ идентификации держателя карты, как проверка CVV2/CVK2-кодов (CVV2-код для карт платежной системы Visa и CVK2 — для MasterCard).
3. Что подразумевает проверка адреса AVS (Address Verification Service)?
4. В чем сущность технологии применения протокола 3-D Secure?

Зарегистрируетесь на сайте https://qiwi.ru и проанализируйте безопасность использования платежной системы Киви.

Отчет можно составить в произвольной форме.

ВОПРОСЫ
для самоподготовки к лабораторным занятиям

Самостоятельное изучение тем рекомендуется проводить в следующем порядке:

1) Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме.
2) На этой основе составить развёрнутый план изложения темы
3) Оформить отчётный материал в форме расчетно-аналитической работы
4) Провести самоконтроль освоения темы по вопросам, выданным преподавателем
5) Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы
6) Принять участие в указанном мероприятии

Рекомендации по конкретным темам дисциплины

Основные положения теории информационной безопасности.

1. Основные понятия в сфере информационной безопасности.
2. Угрозы информационной безопасности.

3. Основные методы обеспечения информационной безопасности

Криптография как способ защиты информации.

1. Основные понятия криптографии и криптоанализа.
2. История криптографии.
3. Методы шифрования.
4. Электронная цифровая подпись.
5. Стенография.

Правовое и организационное обеспечение информационной безопасности.

1. Конституция РФ об информационной безопасности.
2. Стратегические и доктринальные документы в области информационной безопасности.
3. Законодательство РФ об информационной безопасности.
4. Подзаконные акты по вопросам информационной безопасности.
5. Организационное обеспечение информационной безопасности.

Физические и аппаратные меры защиты информации.

1. Технические каналы утечки информации.
2. Системы видеонаблюдения.
3. Тепловидение.
4. Системы контроля доступа.
5. Электронные ключи.
6. Программно-аппаратные комплексы.

Разрушающие программные воздействия.

1.Виды программного обеспечения.
2. Вирусы и программы антивирусной защиты
3. Технологии применения антивирусных средств.
4. Возможные действия злоумышленника для осуществления несанкционированного доступа.

КРИТЕРИИ ОЦЕНКИ
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.

Процедура оценивания

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.

Часть 3.4. Средства для текущего контроля

ВОПРОСЫ
для проведения рубежного контроля

Рубежный контроль осуществляется с целью определения качества проведения образовательных услуг по дисциплине, для оценки степени достижения обучающимися состояния, определяемого целевыми установками дисциплины, а также для формирования корректирующих мероприятий. Рубежный контроль осуществляется по разделам дисциплины в соответствии с планом. Рубежный контроль состоит из тестовых заданий по результатам изучения разделов дисциплины.

Образец

РАЗДЕЛ 1. Основы теории информационной безопасности

1. Кто является основным ответственным за определение уровня классификации информации?
A. Руководитель среднего звена
B. Высшее руководство
C. Владелец
D. Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
A. Сотрудники
B. Хакеры
C. Атакующие
D. Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
C. Улучшить контроль за безопасностью этой информации
D. Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?
A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
B. Необходимый уровень доступности, целостности и конфиденциальности
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
A. Владельцы данных
B. Пользователи
C. Администраторы
D. Руководство

Процедура оценивания

Шкала и критерии оценивания
ответов на тестовые вопросы тестирования по результатам освоения разделов 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.

Часть 3.5. Средства для итогового тестирования

ВОПРОСЫ
для проведения итогового тестирования

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

Образец
Как называется умышленно искаженная информация?
Дезинформация
Информативный поток

Достоверная информация
Перестает быть информацией
Как называется информация, к которой ограничен доступ?
Конфиденциальная
Противозаконная
Открытая
Недоступная
Какими путями может быть получена информация?
Проведением, покупкой и противоправным добыванием информации научных исследований
Захватом и взломом ПК информации научных исследований
Добыванием информации из внешних источников и скремблированием информации научных исследовании
Захватом и взломом защитной системы для информации научных исследований
Основной документ, на основе которого проводится политика информационной безопасности?
программа информационной безопасности
регламент информационной безопасности
политическая информационная безопасность
Протекторат
К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации
Информационным процессам
Мыслительным процессам
Машинным процессам
Микропроцессам

Дифференцированный зачет выставляется студенту по факту выполнения графика учебных работ, предусмотренных рабочей программой дисциплины. По итогам изучения дисциплины, студенты проходят итоговое тестирование. Тестирование является формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин.

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

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

Студенту рекомендуется:

1. при неуверенности в ответе на конкретное тестовое задание пропустить его и переходить к следующему, не затрачивая много времени на обдумывание тестовых заданий при первом проходе по списку теста;
2. при распределении общего времени тестирования учитывать (в случае компьютерного тестирования), что в автоматизированной системе могут возникать небольшие задержки при переключении тестовых заданий.

Необходимо помнить, что:

1. тест является индивидуальным. Общее время тестирования и количество тестовых заданий ограничены и определяются преподавателем в начале тестирования;
2. по истечении времени, отведённого на прохождение теста, сеанс тестирования завершается;
3. допускается во время тестирования только однократное тестирование;
4. вопросы студентов к преподавателю по содержанию тестовых заданий и не относящиеся к процедуре тестирования не допускаются;

Тестируемому во время тестирования запрещается:

1. нарушать дисциплину;
2. пользоваться учебно-методической и другой вспомогательной литературой, электронными средствами (мобильными телефонами, электронными записными книжками и пр.);
3. использование вспомогательных средств и средств связи на тестировании допускается при разрешении преподавателя-предметника.
4. копировать тестовые задания на съёмный носитель информации или передавать их по электронной почте;
5. фотографировать задания с экрана с помощью цифровой фотокамеры;
6. выносить из класса записи, сделанные во время тестирования.

На рабочее место тестируемому разрешается взять ручку, черновик, калькулятор.

За несоблюдение вышеперечисленных требований преподаватель имеет право удалить тестируемого, при этом результат тестирования удаленного лица аннулируется.

Тестируемый имеет право:

Вносить замечания о процедуре проведения тестирования и качестве тестовых заданий.

Перенести сроки тестирования (по уважительной причине) по согласованию с преподавателем.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ
ответов на вопросы итогового контроля

- 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.

Общие критерии оценки результатов изучения учебной дисциплины

Нормативная база проведения промежуточной аттестации обучающихся по результатам изучения дисциплины:	
1) 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 ВАРС, на последней неделе семестра
Основные условия получения студентом 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 итоговое тестирование; 3) подготовил презентацию (контрольную работу по заочной форме).

ЛИСТ РАССМОТРЕНИЙ И ОДОБРЕНИЙ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
в составе ОПОП 38.03.01 Экономика

1. Рассмотрена и одобрена:

а) На заседании обеспечивающей преподавание кафедры гуманитарных, социально-экономических и фундаментальных дисциплин

протокол № 7 от 17.03.2022 г.

Зав. кафедрой, канд.ист.наук, доцент _____ Е.В. Соколова

б) На заседании методического совета Тарского филиала;

протокол № 9А от 29.04.2022 г.

Председатель методического совета, канд. экон. наук, доцент. _____ Е.В.Юдина

2. Рассмотрение и одобрение представителями профессиональной сферы по профилю ОПОП:

Администрация Тарского муниципального района Омской области, гл. бухгалтер Комитета по сельскому хозяйству и продовольствию _____ О.П. Петрунишина

ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ
к фонду оценочных средств учебной дисциплины
Б1.О.33 Информационная безопасность
в составе ОПОП 38.03.01 Экономика

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