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

ОПОП по направлению 38.03.01 Экономика

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

Б1.О.33 Информационная безопасность

Направленность (профиль) «Прикладная экономика и финансы»

Обеспечивающая преподавание дисциплины 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)
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 информационные технологии и программные средства для анализа информационной безопасности социальных сетей и платежных систем	использовать современные информационные технологии и программные средства для поиска и обработки экономической информации	владеть навыками применения современных информационных технологий и программными средствами 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 география
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

Номер раздела дисциплины	Тема в составе раздела/ вопрос в составе темы раздела, вынесенные на самостоятельное изучение	Расчетная трудоемкость, час.	Форма текущего контроля по теме
1	2	3	4
Очная/ очно-заочная форма обучения			
3	Эффективные меры антивирусной защиты	-/20	презентация
3	Новейшие аппаратные средства защиты информации	-/20	презентация
Заочная форма обучения			
3	Эффективные меры антивирусной защиты	28	опрос
3	Новейшие аппаратные средства защиты информации	26	опрос
3	Новейшие программные средства защиты информации	26	опрос

Примечание: Учебная, учебно-методическая литература и иные библиотечно-информационные ресурсы и средства обеспечения самостоятельного изучения тем – см. Приложения 1, 2, 3, 4.

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 аудиторно 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.

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

6. Что такое процедура?
A. Правила использования программного и аппаратного обеспечения в компании
B. Пошаговая инструкция по выполнению задачи
C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
A. Поддержка высшего руководства
B. Эффективные защитные меры и методы их внедрения
C. Актуальные и адекватные политики и процедуры безопасности
D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
B. Когда риски не могут быть приняты во внимание по политическим соображениям
C. Когда необходимые защитные меры слишком сложны
D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?
A. Пошаговые инструкции по выполнению задач безопасности
B. Общие руководящие требования по достижению определенного уровня безопасности
C. Широкие, высокоуровневые заявления руководства
D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
A. Анализ рисков
B. Анализ затрат / выгоды
C. Результаты ALE
D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?
A. Количественно оценить уровень безопасности среды
B. Оценить возможные потери для каждой контрмеры
C. Количественно оценить затраты / выгоды
D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:
A. Среднесрочное планирование
B. Долгосрочное планирование
C. Ежедневное планирование
D. Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?
A. Нечто, приводящее к ущербу от угрозы
B. Любая потенциальная опасность для информации или систем
C. Любой недостаток или отсутствие информационной безопасности
D. Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:
A. Технических и нетехнических методов
B. Контрмер и защитных механизмов
C. Физической безопасности и технических средств защиты
D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
A. Внедрение управления механизмами безопасности
B. Классификацию данных после внедрения механизмов безопасности
C. Уровень доверия, обеспечиваемый механизмом безопасности
D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
A. Только военные имеют настоящую безопасность
B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?
A. Угрозы x Риски x Ценность актива
B. (Угрозы x Ценность актива x Уязвимости) x Риски
C. SLE x Частоту = ALE
D. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?
A. Делегирование полномочий
B. Количественная оценка воздействия потенциальных угроз
C. Выявление рисков
D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
A. Поддержка
B. Выполнение анализа рисков
C. Определение цели и границ
D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
A. Чтобы убедиться, что проводится справедливая оценка
B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Что является наилучшим описанием количественного анализа рисков?
A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
D. Метод, основанный на суждениях и интуиции

22. Почему количественный анализ рисков в чистом виде не достижим?
A. Он достижим и используется
B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
C. Это связано с точностью количественных элементов
D. Количественные измерения должны применяться к качественным элементам

23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
A. Много информации нужно собрать и ввести в программу
B. Руководство должно одобрить создание группы
C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
D. Множество людей должно одобрить данные

РАЗДЕЛ 2. Ведение в криптографию. Правовое и организационное обеспечение информационной безопасности.

1. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?
A. Стандарты
B. Должный процесс (Due process)
C. Должная забота (Due care)
D. Снижение обязательств

2. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
A. Список стандартов, процедур и политик для разработки программы безопасности
B. Текущая версия ISO 17799
C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
D. Открытый стандарт, определяющий цели контроля

3. Из каких четырех доменов состоит CobiT?
A. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
B. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
C. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
D. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

4. Что представляет собой стандарт ISO/IEC 27799?
A. Стандарт по защите персональных данных о здоровье
B. Новая версия BS 17799
C. Определения для новой серии ISO 27000
D. Новая версия NIST 800-60

5. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
A. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
B. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
C. COSO учитывает корпоративную культуру и разработку политик
D. COSO – это система отказоустойчивости

6. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
A. NIST и OCTAVE являются корпоративными
B. NIST и OCTAVE ориентирован на ИТ
C. AS/NZS ориентирован на ИТ
D. NIST и AS/NZS являются корпоративными

7. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
A. Анализ связующего дерева
B. AS/NZS
C. NIST
D. Анализ сбоев и дефектов

8. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
A. Безопасная OECD
B. ISO\IEC
C. OECD
D. CPTED

9. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

10. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

11. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

12. Защита информации от утечки это деятельность по предотвращению:
1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или

правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

13. Защита информации это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

14. Естественные угрозы безопасности информации вызваны:
1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

15. Икусственные угрозы безопасности информации вызваны:
1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

16. К основным непреднамеренным искусственным угрозам АСОИ относится:
1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

РАЗДЕЛ 3. Меры защиты информации

1. К посторонним лицам нарушителям информационной безопасности относится:
1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.
7. лица, нарушившие пропускной режим;

2. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
1. черный пиар;

2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

3. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

4. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

5. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:
1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

6. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:
1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

7. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

8. Активный перехват информации это перехват, который:
1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

9. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

10. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5.просмотр мусора.

11. Перехват, который осуществляется путем использования оптической техники называется:
1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. К внутренним нарушителям информационной безопасности относится:
1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание

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.

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

Под непреднамеренным воздействием на защищаемую информацию понимают?

Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
Процесс ее преобразования, при котором содержание информации изменяется на ложную
Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Основные предметные направления Защиты Информации?

охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
Охрана золотого фонда страны
Определение ценности информации
Усовершенствование скорости передачи информации

Государственная тайна это

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
Ограничения доступа в отдельные отрасли экономики или на конкретные производства
Защищаемые банками и иными кредитными организациями сведения о банковских операциях
Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Коммерческая тайна это….

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
Ограничения доступа в отдельные отрасли экономики или на конкретные производства
Защищаемые банками и иными кредитными организациями сведения о банковских операциях
Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Банковская тайна это….

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
Ограничения доступа в отдельные отрасли экономики или на конкретные производства
Защищаемые банками и иными кредитными организациями сведения о банковских операциях
Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Профессиональная тайна

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
Ограничения доступа в отдельные отрасли экономики или на конкретные производства
Защищаемые банками и иными кредитными организациями сведения о банковских операциях
Защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

К основным объектам банковской тайны относятся следующие:

Все ответы верны
Тайна банковского счета
Тайна операций по банковскому счету
Тайна банковского вклада

Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право
управление доступом
конфиденциальность
аутентичность
целостность
доступность
К открытым источникам информация относятся.
Газеты, Радио, Новости
Информация украденная у спецслужб
Из вскрытого сейфа
Украденная из правительственной организации
По сведениям Media и Pricewaterhouse Coopers, на чью долю приходится 60% всех инцидентов IT-безопасности?
Хакерские атаки
Различные незаконные проникновения
Инсайдеры
Технические компании
Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?
Индивидуальный подход к защите
Комплексный подход к защите
Смешанный подход к защите
Рациональный подход к защите
Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе
Информационная безопасность
Защитные технологии
Заземление
Конфиденциальность
Можно выделить следующие направления мер информационной безопасности
Правовые
Организационные
Все ответы верны
Технические
Что можно отнести к правовым мерам ИБ?
Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра итд
Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
Охрану вычислительного центра, установку сигнализации и многое другое
Что можно отнести к организационным мерам ИБ?
Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку

резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Что можно отнести к техническим мерам ИБ?

Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства

Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое

Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов

В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Потенциальные угрозы, против которых направлены технические меры защиты информации

Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей

Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения

Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.

Потери информации из-за не достаточной установки сигнализации в помещении.

Процессы преобразования, при котором информация удаляется

Шифрование информации это

Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов

Процесс преобразования, при котором информация удаляется

Процесс ее преобразования, при котором содержание информации изменяется на ложную

Процесс преобразования информации в машинный код

Какие сбои оборудования, при которых теряется информация, бывают?

случайное уничтожение или изменение данных

перебои электропитания

некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных;

несанкционированное копирование, уничтожение или подделка информации

Какие потери информации бывают из-за некорректной работы программ?

потери при заражении системы компьютерными вирусами

сбои дисковых систем

перебои электропитания

сбои работы серверов, рабочих станций, сетевых карт и тд

Какие потери информации, связанные с несанкционированным доступом, бывают?

несанкционированное копирование, уничтожение или подделка информации

потери при заражении системы компьютерными вирусами

случайное уничтожение или изменение данных

сбои дисковых систем

Потери из-за ошибки персонала и пользователей бывают?

несанкционированное копирование, уничтожение или подделка информации

потери при заражении системы компьютерными вирусами

случайное уничтожение или изменение данных

сбои дисковых систем

О**т сбоев устройств для хранения информации?**

установка источников бесперебойного питания (UPS)

симметричное мультипроцессирование

Каждую минуту сохранять данные

Организация надежной и эффективной системы резервного копирования и дублирования данных

Средства защиты данных, функционирующие в составе программного обеспечения.

Программные средства защиты информации

Технические средства защиты информации

Источники бесперебойного питания (UPS)

Смешанные средства защиты информации

Программные средства защиты информации.

средства архивации данных, антивирусные программы
Технические средства защиты информации
Источники бесперебойного питания (UPS)
Смешанные средства защиты информации
Программное средство защиты информации.
криптография
источник бесперебойного питания
резервное копирование
дублирование данных
Обеспечение достоверности и полноты информации и методов ее обработки.
Конфиденциальность
Целостность
Доступность
Целесообразность
Обеспечение доступа к информации только авторизованным пользователям?
Конфиденциальность
Целостность
Доступность
Целесообразность
Виды защиты БД
защита паролем, защита пользователем,
учётная запись группы администратора
приложение, которое используется для управления базой данных
группа Users
Наибольшую угрозу для безопасности сети представляют.
несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение;
вскрытие стандартной учётной записи пользователя
вскрытие стандартной учётной группы администратора
копирование файлов, которые были изменены в течение дня, без отметки о резервном копировании
Защита через права доступа заключается.
присвоении каждому пользователю определенного набора прав
запереть серверы в специальном помещении с ограниченным доступом
присвоить пароль каждому общедоступному ресурсу
в наличии преобразователя микрофона
Дифференцированное резервное копирование это
Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании;
Копирование всех выбранных файлов без отметки о резервном копировании
Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования;
Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании
Полное копирование данных это
Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования
Копирование всех выбранных файлов без отметки о резервном копировании
Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании
Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования
Наиболее распространенный криптографический код
Код Хэмминга
код Рида-Соломона
код Морзе
итеративный код
Наиболее простой и недорогой метод предотвратить катастрофическую потерю данных
Резервное копирование на магнитную ленту
Шифрование данных
Бездисковые компьютеры
Все ответы верны
Право Execute дает вам возможность
Запуск (выполнение) программ из каталога

Создание новых файлов в каталоге
Запрещение на доступ к каталогу, файлу, ресурсу
Чтение и копирование файлов из совместно используемого каталога
Право No Access дает вам возможность
Удаление файлов в каталоге
Запрещение на доступ к каталогу, файлу, ресурсу
Запуск (выполнение) программ из каталога
Создание новых файлов в каталоге
Право Read дает вам возможность
Удаление файлов в каталоге
Запуск (выполнение) программ из каталога
Запрещение на доступ к каталогу, файлу, ресурсу
Чтение и копирование файлов из совместно используемого каталога
Право Write дает вам возможност
Удаление файлов в каталоге
Запрещение на доступ к каталогу, файлу, ресурсу
Создание новых файлов в каталоге
Чтение и копирование файлов из совместно используемого каталога
Методы сохранение данных при чрезвычайных ситуаций
резервное копирование на магнитную ленту;
источники бесперебойного питания (UPS);
отказоустойчивые системы
Все ответы верны
Какой способ данные, дублируя и размещая их на различных физических носителях (например, на разных дисках).
Журнал резервного копирования
Отказоустойчивые системы
Метод резервного копирования
Шифрование данных
Пароль доступа к ресурсам
Доступ только для чтения
такой пароль не существует
Отказоустойчивые системы
Метод резервного копирования
Шифрование данных
Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?
установка источников бесперебойного питания (UPS)
Такого средства не существует
Каждую минуту сохранять данные
Перекидывать информацию на носитель, который не зависит от энергии
Ежедневное копирование данных это
Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании
Копирование всех выбранных файлов без отметки о резервном копировании
Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования
Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании
Способ защиты от сбоев процессора?
установка источников бесперебойного питания (UPS)
симметричное мультипроцессирование
Каждую минуту сохранять данные
Перекидывать информацию на носитель, который не зависит от энергии
Способ защиты от сбоев устройств для хранения информации?
установка источников бесперебойного питания (UPS)
симметричное мультипроцессирование
Каждую минуту сохранять данные
Организация надежной и эффективной системы резервного копирования и дублирования данных
Средства защиты данных, функционирующие в составе программного обеспечения.
Программные средства защиты информации
Технические средства защиты информации
Источники бесперебойного питания (UPS)

Смешанные средства защиты информации
Средством предотвращения потерь информации при кратковременном отключении электроэнергии является?
источник бесперебойного питания (UPS)
источник питания
электро-переключатель
все перечисленное
Что такое Информационная безопасность?
меры по защите информации от неавторизованного доступа
меры по защите ПК
безопасность личной информации
все перечисленное
Целью информационной безопасности является?
все перечисленное
обезопасить ценности системы
защитить и гарантировать точность и целостность информации
минимизировать разрушения
Укажите направления мер информационной безопасности.
правовые, организационные, технические
правовые, аппаратные, программные
личные, организационные
технические
Технические меры защиты можно разделить на:
средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и тд;
правовые, организационные, технические
правовые, аппаратные, программные
личные, организационные
Программные средства защиты можно разделить на:
криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и тд
административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и тд
правовые, организационные, технические
правовые, аппаратные, программные
К наиболее важному элементу аппаратной защиты можно отнести?
защита от сбоев серверов, рабочих станций и локальных компьютеров
защиту от вирусов
защиту от хакеров
все перечисленное
Как связаны ключи шифрования между собой?
математической функцией
связкой
шифром
специальным паролем
В чем заключается уникальность гибких дисков?
в форматировании
в быстродействии
их защищенность
в простоте обработки данных
Что такое пароль?
механизм управления доступом
средство защиты
безопасность личной информации
Безопасность людей
Меры по защите информации от неавторизованного доступа называется
Информационной безопасностью
Безопасностью ПК
Личной безопасностью
Безопасностью группы администратора
Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания относится к?
техническим мерам защиты

не правовым мерам защиты
организационным мерам защиты
программным средствам защиты
Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?
аппаратным средствам защиты
программным средствам защиты
техническим средствам защиты
правовым средствам защиты
Как еще называют радиомикрофон с дистанционным (кодовым) включением через любой телефон?
«электронное ухо»
«электронный микрофон»
«громкоговоритель»
«электронный приемник»
К программным средствам защиты можно отнести?
средства идентификации и аутентификации пользователей
средства защиты авторских прав программистов
неиспользованные дорожки на дискете
дорожки дискеты
К правовым мерам следует отнести?
разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов
охрану вычислительного центра и аппаратуры связи
проектирование ЛВС и ГБС
средства идентификации и аутентификации пользователей
Сбои дисковых систем относится к?
техническим и организационным мерам защиты
правовым мерам защиты
мерам защиты от НДС и кражи
к средствам идентификации и аутентификации
Потеря или изменение данных при ошибках ПО относится к
техническим и правовым мерам защиты
организационным мерам защиты
правовым мерам защиты
мерам защиты от НДС и кражи
к средствам идентификации и аутентификации
Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?
Аппаратным и техническим средствам защиты
Программным средствам защиты
Средствам защиты идентификации и аутентификации
Организационным и общим средствам защиты
Криптографические средства относится к?
Программным средствам
Аппаратным средствам
Организационным средствам защиты
Захвату данных
Служат обеспечению сохранения целостности программного обеспечения в составе вычислительной системы
пароль
корпус вычислительной системы
шифры
сигналы
В каких случаях криптография неэффективна?
когда элементы текста известны в зашифрованном и исходном виде
когда элементы текста известны в открытом и активном виде
если есть пароль и логин
когда элементы текста представлены в открытом и не полном виде
В каком случае надежнее шифр?
короткий зашифрованный текст
длинный зашифрованный текст
зашифрованный текст среднего размера
зашифрованный текст не влияет на надежность шифра
В каких случаях возможно вычисление одного ключа с помощью другого

Использованием только ЭВМ
Ни в каких случаях невозможна
Использованием математической функцией
Использованием только ЛВС

Назначение пароля в ИС?

механизм управления доступом, средство защиты и безопасность личной информации
скрытие копирования участков магнитной ленты из ОЗУ в ПЗУ
технические меры защиты и средство защиты данных
участки магнитной ленты скрытые шифром
механизм управления средствами защиты и безопасность доступа к ОЗУ в ПЗУ

Меры по защите информации от неавторизованного доступа называется

Информационной безопасностью
Безопасностью ПК
Личной безопасностью
Средства защиты
Меры скрытия копирования

Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?

аппаратным средствам защиты
программным средствам защиты
техническим средствам защиты
правовым средствам защиты

Какие атакующие средства включены в современные способы несанкционированного доступа?

активные и пассивные
положительные и отрицательные
большие и маленькие
объединенные и разъединенные
односторонние и разносторонние

Что относится к пассивным средствам защиты информации?

Фильтры
Детекторы поля
Сканирующие приемники
Комплекс радио контроля
Нелинейные локаторы

Самый известный в России производитель систем защиты от вирусов, спама и хакерских атак.

лаборатория Касперского
Российский центр по защите от вредоносных программ
компания McAfee Security
лаборатория доктора Веб
компания Тумар

Метод резервного копирования когда, копирование всех выбранных файлов производится без отметки о резервном копировании

Полное копирование
Копирование
Ежедневное копирование
Дифференцированное резервное копирование
Резервное копирование с приращением

Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

Полное копирование
Копирование
Ежедневное копирование
Дифференцированное резервное копирование
Резервное копирование с приращением

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).
Процедура получения зачёта -	Представлены в Фонде оценочных средств по данной учебной дисциплине (см. – Приложение 9)
Методические материалы, определяющие процедуры оценивания знаний, умений, навыков:	

4. ОЦЕНОЧНЫЕ СРЕДСТВА
сформированности компетенции

4.1. ОПК 5 - Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.

ИД-1 - Применяет современные информационные технологии и программные средства для поиска и обработки экономической информации

Тип заданий: выбор одного варианта правильного ответа из нескольких предложенных / выбор нескольких правильных вариантов из предложенных вариантов ответов

1.Определите методы повышения достоверности входных данных, с учетом применения современных информационных технологий
ВЫБЕРИТЕ НЕ МЕНЕЕ ТРЕХ ВАРИАНТОВ ОВЕТОВ
+ замена процесса ввода значения процессом выбора значения из предлагаемого множества
отказ от использования данных
проведение комплекса регламентных работ
+ использование вместо ввода значения его считывание с машиночитаемого носителя
+ введение избыточности в документ первоисточник
многократный ввод данных и сличение введенных значений

2. Выбирая средства решения стандартных задач в профессиональной деятельности с применением современных информационных технологий и с учетом основных требований информационной безопасности, определите сервисы безопасности
ВЫБЕРИТЕ НЕ МЕНЕЕ ПЯТИ ВАРИАНТОВ ОВЕТОВ
+ идентификация и аутентификация
+ шифрование
инверсия паролей
+ контроль целостности
регулирование конфликтов
+ экранирование
+ обеспечение безопасного восстановления
кэширование записей

3.Выбирая методы решения стандартных задач в профессиональной деятельности с применением современных информационных технологий и с учетом основных требований информационной безопасности, определите причины возникновения ошибки в данных
ВЫБЕРИТЕ НЕ МЕНЕЕ ШЕСТИ ВАРИАНТОВ ОВЕТОВ
+ погрешность измерений
+ ошибка при записи результатов измерений в промежуточный документ
+ неверная интерпретация данных
+ ошибки при переносе данных с промежуточного документа в компьютер
использование недопустимых методов анализа данных
неустранимые причины природного характера
+преднамеренное искажение данных
+ ошибки при идентификации объекта или субъекта хозяйственной деятельности

4. Применяя программные средства для поиска и обработки экономической информации, определите разделы современной криптографии:
ВЫБЕРИТЕ НЕ МЕНЕЕ ЧЕТЫРЕХ ВАРИАНТОВ ОВЕТОВ
+ симметричные криптосистемы
+ криптосистемы с открытым ключом
криптосистемы с дублированием защиты
+ системы электронной подписи
управление паролями
управление передачей данных
+ управление ключами

5. Применяя современные информационные технологии и программные средства для поиска и обработки экономической информации, определите элементы знака охраны авторского права:
ВЫБЕРИТЕ НЕ МЕНЕЕ ТРЕХ ВАРИАНТОВ ОВЕТОВ
+ буквы С в окружности или круглых скобках
буквы Р в окружности или круглых скобках
+ наименования (имени) правообладателя
наименование охраняемого объекта
+ года первого выпуска программы

6. Применяя современные программные средства, какое Вы выберите свойство информации, наиболее актуальное при обеспечении информационной безопасности:
+ целостность
доступность
актуальность

7.С учетом основных требований информационной безопасности, что является наилучшим описанием количественного анализа рисков?
анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности.
метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков.
+метод, сопоставляющий денежное значение с каждым компонентом оценки рисков.
метод, основанный на суждениях и интуиции.

8.Какие составляющие относятся к информационно-технологическому ресурсу современного предприятия, с учетом основных требований информационной безопасности?
ВЫБЕРИТЕ НЕ МЕНЕЕ ТРЕХ ВАРИАНТОВ ОВЕТОВ
+ внешняя и внутренняя информация
+ обслуживающие системы и технологии
весь персонал
+ ИТ-специалисты и персонал ИТ-подразделений
финансовый капитал

9.Чем регулируется ответственность за причинение вреда и ответственность за реализацию мероприятий по разработке, внедрению и использованию систем информационной безопасности во внутренней среде?
ВЫБЕРИТЕ НЕ МЕНЕЕ ДВУХ ВАРИАНТОВ ОВЕТОВ
+ внутренними корпоративными документами
+ действующим законодательством РФ и стран, с которыми осуществляется бизнес
международными стандартами в области информационной безопасности
Доктриной информационной безопасности

10. Кто в конечном счете несет ответственность, в рамках профессиональной деятельности, за гарантии того, что данные классифицированы и защищены, с учетом современных информационных технологий и программных средств?
владельцы данных
пользователи
администраторы
+ руководство

11. При использовании современных программных средств и с учетом требований информационной безопасности, какие компоненты присутствуют в модели системы защиты с полным перекрытием?
ВЫБЕРИТЕ НЕ МЕНЕЕ ТРЕХ ВАРИАНТОВ ОВЕТОВ
+ область угроз
область рисков
+защищаемая область
+система защиты
область безопасности

12. При поиске и обработке экономической информации выделите охраняемую информацию, оборот которой контролируется:
ВЫБЕРИТЕ НЕ МЕНЕЕ ТРЕХ ВАРИАНТОВ ОВЕТОВ

персональные данные
+ объекты промышленной собственности
государственная тайна
коммерческая тайна
+ объекты авторского права
+ несекретные информационные ресурсы, имеющие государственное значение

13. При поиске и обработке экономической информации, назовите наиболее распространенные угрозы информационной безопасности сети:
распределенный доступ клиент, отказ оборудования
моральный износ сети, инсайдерство
+ сбой (отказ) оборудования, нелегальное копирование данных

14. Участвуя в поиске и обработке экономической информации, выберите, невыполнение какого из следующих требований политики безопасности, на Ваш взгляд, может наибольшим образом повысить существующие в системе информационные риски:
+регулярное обновление антивирусных баз
создание и поддержание форума по информационной безопасности для всех специалистов, вовлеченных в процесс обеспечения ИБ
классификация ресурсов по степени важности с точки зрения ИБ
завершение активной сессии пользователя по окончании работы

15. При применении современных информационных технологий и программных средств для поиска и обработки экономической информации, необходимо помнить, что обеспечение информационной безопасности есть обеспечение ...
независимости информации
изменения информации
копирования информации
+сохранности информации
преобразования информации

Тип заданий: установление правильной последовательности в предложенных вариантах ответов / установление соответствия между элементами в предложенных вариантах ответов

16.Выбирая методы и средства решения стандартных задач в профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, укажите на порядок формирования требований к системе защиты информации
УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА
1.Принятие решения о необходимости защиты обрабатываемой информации.
2.Классификация объекта по требованиям защиты информации (установление уровня защищенности обрабатываемой информации).
3.Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации.
4.Определение требований к системе защиты информации.

17. Выбирая принципы и средства решения стандартных задач в профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, укажите на порядок проведения качественного анализа риска
УКАЖИТЕ ПОРЯДКОВЫЙ НОМЕР ДЛЯ ВСЕХ ВАРИАНТОВ ОТВЕТА
1.Определение источников риска
2.Определение категории рисков
3.Определение факторов риска
4.Определение близости наступления риска
5.Определение степени угрозы риска

18. Выбирая средства решения стандартных задач в профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, установите соответствие

УСТАНОВИТЕ СООТВЕТСТВИЕ ДЛЯ КАЖДОГО ЭЛЕМЕНТА ЗАДАНИЯ

1. Защита информации от утечки по акустическому каналу	1. это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей
2. Защита информации от утечки по электромагнитным каналам	2. это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
	3. это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
	4. это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

19. Выбирая современные информационные технологии и программные средства для поиска и обработки экономической информации, с учетом информационной безопасности, установите соответствие между действием и документом

УСТАНОВИТЕ СООТВЕТСТВИЕ МЕЖДУ ДЕЙСТВИЕМ И ДОКУМЕНТОМ

1. Определение актуальных угроз безопасности информации	1. Частная модель угроз безопасности информации
2. Определение требований к системе защиты информации	2. ТЗ на создание системы защиты информации с указанием требований к мерам и средствам защиты информации
	3. Локальный нормативный правовой акт, определяющий необходимость создания системы защиты информации
	4. Акт классификации по требованиям безопасности информации

20. Выбирая современные информационные технологии и программные средства для поиска и обработки экономической информации и с учетом основных требований информационной безопасности, установите соответствие

УСТАНОВИТЕ СООТВЕТСТВИЕ ДЛЯ КАЖДОГО ЭЛЕМЕНТА ЗАДАНИЯ

1 Целостность	1. свойство информации; заключается в сохранности информации в неискаженном виде (отсутствие неправомочных и непредусмотренных владельцем информации искажений)
2 Доступность	2. свойство информации; наличие своевременного беспрепятственного доступа к информации для субъектов, обладающих соответствующими полномочиями
3 Аутентичность	3. возможность достоверно установить автора сообщения
	4. состояние информации, при котором субъект не может отказаться от того действия, которое имело место быть
	5. состояние информации, при котором доступ к ней осуществляют только те субъекты, которые имеют на это право

Тип заданий: открытого типа (самостоятельный ввод обучающимся правильного ответа в виде термина, краткого определения, цифрового значения) / Практико-ориентированные задания (кейсы)

21. На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника. Нарушены или не нарушены правила обеспечения информационной безопасности?

ОТВЕТ ЗАПИШИТЕ КАК "НАРУШЕНЫ" ИЛИ "НЕ НАРУШЕНЫ"

+ нарушены

22. Вправе ли должностное лицо, в производстве которого находится дело об административном правонарушении, запрашивать у руководства медицинской организации персональные данные их работников, с учетом основных требований информационной безопасности?

ОТВЕТ ЗАПИШИТЕ КАК "ВПРАВЕ" ИЛИ "НЕ ВПРАВЕ"

+ вправе

23.Какой термин определяет защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений — производителям, владельцам и пользователям информации и поддерживающей инфраструктуре?

ОТВЕТ ЗАПИШИТЕ СТРОЧНЫМИ БУКВАМИ В ФОРМЕ СЛОВОСОЧЕТАНИЯ В ИМЕНИТЕЛЬНОМ ПАДЕЖЕ

+ информационная безопасность

24.Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы

ОТВЕТ ЗАПИШИТЕ СТРОЧНЫМИ БУКВАМИ В ФОРМЕ СУЩЕСТВИТЕЛЬНОГО В РОДИТЕЛЬНОМ ПАДЕЖЕ

+ аутентификации

25.Продолжите фразу: «Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой – это …»

ОТВЕТ ЗАПИШИТЕ СТРОЧНЫМИ БУКВАМИ В ФОРМЕ СУЩЕСТВИТЕЛЬНОГО В ИМЕНИТЕЛЬНОМ ПАДЕЖЕ

+ пароль