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

Факультет зоотехнии, товароведения и стандартизации

ОПОП по направлению 36.03.02 Зоотехния

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

Б1.В.ДВ.01.01 Информационная безопасность

Направленность (профиль) «IT-технологии в животноводстве»

Обеспечивающая преподавание дисциплины кафедра -	математических и естественнонаучных дисциплин
Разработчики	Харитонова Н.Д.

Омск 2021

ВВЕДЕНИЕ

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

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

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

5. 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.

6. Разработчиками фонда оценочных средств по дисциплине являются преподаватели кафедры математических и естественнонаучных дисциплин, 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					
ПК-1	Способен использовать информационно-коммуникативные и цифровые технологии при планировании и реализации профессиональных задач	ИД-1$_{ПК-1}$ Знает информационно-коммуникативные и цифровые технологии, позволяющие повысить эффективность животноводства	Знает информационно-коммуникативные и цифровые технологии, основные понятия информационной безопасности, основные виды угроз, пути и каналы утечки информации	Умеет использовать информационно-коммуникативные и цифровые технологии, соблюдает основные требования информационной безопасности	Владеет навыками применения информационно-коммуникативных и цифровых технологий, методами защиты информации, в том числе, правилами защиты от «компьютерных вирусов»
		ИД-2$_{ПК-1}$ Умеет координировать автоматизированные технологические процессы, отслеживать и контролировать производственные показатели	Знает автоматизированные технологические процессы, контролируемые производственные показатели	Умеет координировать автоматизированные технологические процессы, отслеживать и контролировать производственные показатели	Владеет навыками координирования автоматизированных технологических процессов, отслеживает и контролирует производственные показатели
		ИД-3$_{ПК-1}$ Владеет навыками своевременного принятия решений на основе цифровых данных и осуществления долгосрочного планирования	Знает как принимать решения на основе цифровых данных и осуществления долгосрочного планирования	Умеет принимать решения на основе цифровых данных и осуществления долгосрочного планирования	Владеет навыками своевременного принятия решений на основе цифровых данных и осуществления долгосрочного планирования

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

Общие критерии оценки и реестр применяемых оценочных средств

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

Категория контроля и оценки		Режим контрольно-оценочных мероприятий				
		само-оценка	взаимо-оценка	Оценка со стороны		Комис-сионная оценка
				препода-вателя	представителя производства	
		1	2	3	4	5
Индивидуализация выполнения*, **контроль фиксированных видов ВАРС:**	**1**					
- эссе	1.1			Рецензирование		
- электронная презентация	1.2			Рецензирование		
Текущий контроль:	**2**					
- Самостоятельное изучение тем		Перечень тем для самостоятельного изучения		Проверка конспекта		
- в рамках практических (семинарских) занятий и подготовки к ним	2.1	Вопросы для самоподготовки		Проверка выполненных работ		
-тестирование		Тестовые вопросы		тестирование		
- в рамках обще-университетской системы контроля успеваемости	2.2			Фронтальный контроль текущей успеваемости по контрольным неделям, установленным в университете		
Промежуточная аттестация* обучающихся по итогам изучения дисциплины	**3**			зачет		
* данным знаком помечены индивидуализируемые виды учебной работы						

2.2 Общие критерии оценки хода и результатов изучения учебной дисциплины

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

2.3 Критерии оценки качественного уровня итоговых результатов изучения дисциплины	**2.4**. Критерии аттестационной оценки качественного уровня результатов изучения дисциплины

2.3 РЕЕСТР
элементов фонда оценочных средств по учебной дисциплине

Группа оценочных средств	Оценочное средство или его элемент
	Наименование
1	2
1. Средства для индивидуализации выполнения, контроля фиксированных видов ВАРС	Перечень тем для выполнения эссе
	Критерии оценки эссе
	Перечень тем для выполнения электронной презентации. Процедура выбора темы обучающимся. Этапы работы над электронной презентацией
	Критерии оценки электронной презентации
2. Средства для текущего контроля	Вопросы для самостоятельного изучения темы
	Общий алгоритм самостоятельного изучения темы
	Критерии оценки самостоятельного изучения темы
	Вопросы для самоподготовки по темам семинарских занятий
	Критерии оценки самоподготовки по темам семинарских занятий
3. Средства для промежуточной аттестации по итогам изучения дисциплины	Типовые тестовые вопросы для проведения итогового заключительного тестирования
	Критерии оценки ответов на тестовые вопросы итогового заключительного тестирования
	Промежуточная (семестровая) аттестация по курсу

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				
				Не зачтено	Зачтено			
				Характеристика сформированности компетенции				
				Компетенция в полной мере не сформирована. Имеющихся знаний, умений и навыков недостаточно для решения практических (профессиональных) задач	1. Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач. 2. Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач. 3. Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.		
Критерии оценивания								
ПК-1	ИД-1$_{ПК-1}$	Полнота знаний	Знает информационно-коммуникативные и цифровые технологии, основные понятия информационной безопасности, основные виды угроз, пути и каналы утечки информации	Не знает информационно-коммуникативные и цифровые технологии, основные понятия информационной безопасности, основные виды угроз, пути и каналы утечки информации	1. Знает фрагментарно информационно-коммуникативные и цифровые технологии, основные понятия информационной безопасности, основные виды угроз, пути и каналы утечки информации 2. Знает достаточно хорошо информационно-коммуникативные и цифровые технологии, основные понятия информационной безопасности, основные виды угроз, пути и каналы утечки информации 3. Знает в полной мере информационно-коммуникативные и цифровые технологии, основные понятия информационной безопасности, основные виды угроз, пути и каналы утечки информации		Тестирование, эссе, электронная презентация, опрос
		Наличие умений	Умеет использовать информационно-коммуникативные и цифровые технологии, соблюдает основные требования информационной безопасности	Не умеет использовать информационно-коммуникативные и цифровые технологии, соблюдает основные требования информационной безопасности	1. Частично умеет использовать информационно-коммуникативные и цифровые технологии, соблюдает основные требования информационной безопасности 2. Умеет достаточно хорошо использовать информационно-коммуникативные и цифровые технологии, соблюдает основные требования информационной безопасности 3. Уверенно и в полной мере умеет использовать информационно-коммуникативные и цифровые технологии, соблюдает основные требования информационной безопасности		
		Наличие навыков (владение опытом)	Владеет навыками применения информационно-коммуникативных и цифровых технологий, методами защиты информации, в том числе, правилами защиты от «компьютерных вирусов»	Не владеет навыками применения информационно-коммуникативных и цифровых технологий, методами защиты информации, в том числе, правилами защиты от «компьютерных вирусов»	1. Частично владеет некоторыми навыками применения информационно-коммуникативных и цифровых технологий, методами защиты информации, в том числе, правилами защиты от «компьютерных вирусов» 2. Владеет практически всеми из основных навыков применения информационно-коммуникативных и цифровых технологий, методами защиты информации, в том числе, правилами защиты от «компьютерных вирусов» 3. Уверенно владеет всеми основными навыками применения информационно-коммуникативных и цифровых технологий, методами защиты информации, в том числе, правилами защиты от «компьютерных вирусов»		

	ИД-2$_{ПК-1}$	Полнота знаний	Знает автоматизированные технологические процессы, контролируемые производственные показатели	Не знает автоматизированные технологические процессы, контролируемые производственные показатели	1. Знает частично автоматизированные технологические процессы, контролируемые производственные показатели 2. Знает хорошо некоторые из основных автоматизированных технологических процессов, контролируемые производственные показатели 3. Знает все основные автоматизированные технологические процессы, контролируемые производственные показатели	
		Наличие умений	Умеет координировать автоматизированные технологические процессы, отслеживать и контролировать производственные показатели	Не умеет координировать автоматизированные технологические процессы, отслеживать и контролировать производственные показатели	1. Умеет на уровне ниже среднего, координировать автоматизированные технологические процессы, отслеживать и контролировать производственные показатели 2. Умеет на хорошем уровне координировать автоматизированные технологические процессы, отслеживать и контролировать производственные показатели 3. Умеет на высоком уровне координировать автоматизированные технологические процессы, отслеживать и контролировать производственные показатели	
		Наличие навыков (владение опытом)	Владеет навыками координирования автоматизированных технологических процессов, отслеживает и контролирует производственные показатели	Не владеет навыками координирования автоматизированных технологических процессов, отслеживает и контролирует производственные показатели	1. Владеет некоторыми навыками координирования автоматизированных технологических процессов, отслеживает и контролирует производственные показатели 2. Владеет достаточно хорошо основными навыками координирования автоматизированных технологических процессов, отслеживает и контролирует производственные показатели 3. Владеет уверенно и в полной мере всеми основными навыками координирования автоматизированных технологических процессов, отслеживает и контролирует производственные показатели	
	ИД-3$_{ПК-1}$	Полнота знаний	Знает как принимать решения на основе цифровых данных и осуществления долгосрочного планирования	Не знает как принимать решения на основе цифровых данных и осуществления долгосрочного планирования	1. Частично знает, как принимать решения на основе цифровых данных и осуществления долгосрочного планирования 2. Знает в некоторых основных случаях, как принимать решения на основе цифровых данных и осуществления долгосрочного планирования 3. Знает уверенно и в полной мере, как принимать решения на основе цифровых данных и осуществления долгосрочного планирования	
		Наличие умений	Умеет принимать решения на основе цифровых данных и осуществления долгосрочного планирования	Не умеет принимать решения на основе цифровых данных и осуществления долгосрочного планирования	1. Умеет на уровне ниже среднего принимать решения на основе цифровых данных и осуществления долгосрочного планирования 2. Умеет на хорошем уровне принимать решения на основе цифровых данных и осуществления долгосрочного планирования 3. Умеет на высоком уровне принимать решения на основе цифровых данных и осуществления долгосрочного планирования	
		Наличие навыков (владение опытом)	Владеет навыками своевременного принятия решений на основе цифровых данных и осуществления долгосрочного планирования	Не владеет навыками своевременного принятия решений на основе цифровых данных и осуществления долгосрочного планирования	1. Владеет некоторыми навыками своевременного принятия решений на основе цифровых данных и осуществления долгосрочного планирования 2. Владеет достаточно хорошо основными навыками своевременного принятия решений на основе цифровых данных и осуществления долгосрочного планирования 3. Владеет уверенно и в полной мере всеми основными навыками своевременного принятия решений на основе цифровых данных и осуществления долгосрочного планирования	

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

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

3.1.1 . Средства
для индивидуализации выполнения, контроля фиксированных видов ВАРС

***Перечень примерных тем* эссе**

1. Кто и почему создает вредоносные программы?
2. Правовая защита моей персональной информации.
3. Информация как объект правового регулирования
4. Актуальность защиты компьютерной информации.
5. Безопасная среда для работы в интернете
6. Почтовый ящик, проблема выбора.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ

- «зачтено» выставляется, если обучающийся на основе самостоятельного изученного материала, смог всесторонне раскрыть теоретическое содержание темы;
- «не зачтено» если обучающийся не смог раскрыть теоретическое содержание темы или выполнил работу несамостоятельно**.**

***Перечень примерных тем* электронной презентации**

1. Анализ способов нарушений информационной безопасности.
2. Международные стандарты информационного обмена.
3. Классификация угроз информационной безопасности.
4. Место информационной безопасности экономических систем в национальной безопасности страны.
5. Компьютерная преступность и безопасность
6. Троянские программы. Назначение и классификация.
7. Стеганография
8. Электронная цифровая подпись
9. Криптография с открытым ключом
10. Фишеры и фишинг.
11. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации».
12. Федеральный закон РФ «О персональных данных».
13. Классификация алгоритмов шифрования.
14. Актуальность информационной безопасности.
15. Протоколы обмена ключами.
16. Программирование систем защиты. Сравнительный анализ способов реализации.
17. Спамы и зашита от спамов.
18. Алгоритм Диффи Хеллмана.
19. Способы совершения компьютерных преступлений.
20. Классические компьютерные вирусы.
21. Условия существования вредоносных программ..
22. Идентификация и установление подлинности объекта (субъекта).
23. Безопасность программно-технических средств и информационных ресурсов
24. Виды, способы защиты информации в каналах связи.
25. Жизненный цикл информационных продуктов и услуг

Выбор темы электронной презентации

- Очень важно правильно выбрать тему. Выбор темы не должен носить формальный характер, а иметь практическое и теоретическое обоснование с учетом его познавательных интересов. В этом случае обучающемуся предоставляется право самостоятельного (с согласия преподавателя) выбора тему презентации из списка тем, рекомендованных кафедрой по данной дисциплине (см. выше). При этом весьма полезными могут оказаться советы и обсуждение темы с преподавателем, который может оказать помощь в правильном выборе темы и постановке задач.
- Если интересующая тема отсутствует в рекомендательном списке, то по согласованию с преподавателем обучающемуся предоставляется право самостоятельно предложить тему реферата, раскрывающую содержание изучаемой дисциплины.

Этапы работы над электронной презентацией

- Знакомство с любой научной проблематикой следует начинать с освоения имеющейся основной научной литературы. При этом следует сразу же составлять библиографические выходные данные (автор, название, место и год издания, издательство, страницы) используемых источников. Названия работ иностранных авторов приводятся только на языке оригинала.
- Начинать знакомство с избранной темой лучше всего с чтения обобщающих работ по данной проблеме, постепенно переходя к узкоспециальной литературе.
- На основе анализа прочитанного и просмотренного материала по данной теме следует составить тезисы по основным смысловым блокам, с пометками, собственными суждениями и оценками. Составление плана. Автор по предварительному согласованию с преподавателем может самостоятельно составить план электронной презентации, с учетом замысла работы по соответствующей теме. Правильно построенный план помогает систематизировать материал и обеспечить последовательность его изложения.
- *Оглавление* (план, содержание) включает названия всех разделов (пунктов плана) электронной презентации и номера слайдов, указывающие начало этих разделов в тексте презентации.
- *Основная часть* презентации может быть представлена одной или несколькими главами, которые могут включать 3-4 слайда (подпункта, раздела).
- Здесь достаточно полно и логично излагаются главные положения в используемых источниках, раскрываются все пункты плана с сохранением связи между ними и последовательности перехода от одного к другому.
- *Заключение* (выводы). В этой части обобщается изложенный в основной части материал, формулируются общие выводы, указывается, что нового лично для себя вынес автор презентации из работы над данной темой. Выводы делаются с учетом опубликованных в источниках различных точек зрения по проблеме, рассматриваемой в презентации, сопоставления их и личного мнения автора презентации. Заключение по объему не должно превышать 1-2 слайда.
- *Приложения* могут включать графики, таблицы.
- *Библиография* (список литературы) здесь указывается реально использованная для написания презентации электронные источники информации.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ

- «зачтено» выставляется, если обучающийся на основе самостоятельного изученного материала, смог всесторонне раскрыть теоретическое содержание темы;
- «не зачтено» если обучающийся не смог раскрыть теоретическое содержание темы или выполнил работу несамостоятельно**.**

3.1.2. Средства для текущего контроля

ВОПРОСЫ
для самостоятельного изучения темы

- Национальные интересы РФ в информационной безопасности
- Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации.
- Предоставление привилегий на доступ. (субъекта).
- Защита информации от утечки за счет побочного электромагнитного излучения и наводок
- Методы защиты информации от аварийных ситуаций.
- Организационные мероприятия по защите информации.
- Организация информационной безопасности компании.
- Выбор средств информационной безопасности.
- Информационное страхование

Общий алгоритм самостоятельного изучения темы

1) Ознакомиться с рекомендованной учебной литературой и электронными ресурсами по теме.

2) На этой основе составить развёрнутый план изложения темы

3) Выбрать форму отчетности конспектов (план – конспект, текстуальный конспект, свободный конспект, конспект – схема)

2) Оформить отчётный материал в установленной форме в соответствии методическими рекомендациями

3) Предоставить отчётный материал преподавателю

4) Подготовиться к предусмотренному контрольно-оценочному мероприятию по результатам самостоятельного изучения темы

6) Принять участие в указанном мероприятии, пройти тестирование по разделу на аудиторном занятии и итоговое тестирование в установленное для внеаудиторной работы время

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ
самостоятельного изучения темы

– оценка «зачтено» выставляется, если студент на основе самостоятельного изученного материала, смог раскрыть основное теоретическое содержание темы и выполнил предложенные тестовые задания (не менее 60%)

– оценка «не зачтено» выставляется, если студент не смог всесторонне раскрыть основное теоретическое содержание темы и выполнил предложенные тестовые задания (менее 60%).

ВОПРОСЫ
для самоподготовки к практическим (семинарским) занятиям

Тема 1. Актуальность информационной безопасности. Угрозы информации

- Актуальность информационной безопасности.
- Национальные интересы РФ в информационной сфере и их обеспечение.
- Классификация компьютерных преступлений.
- Способы совершения компьютерных преступлений.
- Пользователи и злоумышленники в Интернете.
- Причины уязвимости сети Интернет.
- Виды угроз информационной безопасности РФ.
- Источники угроз информационной безопасности РФ.
- Угрозы информационной безопасности для АСОИ.
- Классификация удаленных атак на интрасети.

Тема 2. Вредоносные программы. Защита от компьютерных вирусов

- Условия существования вредоносных программ.
- Классические компьютерные вирусы.
- Сетевые черви.
- Троянские программы.
- Спам.
- Признаки заражения компьютера.
- Источники компьютерных вирусов.
- Основные правила защиты.
- . Антивирусные программы.

Тема 3. Методы и средства защиты
компьютерной информации. Правовые документы

- Методы обеспечения информационной безопасности РФ.
- Ограничение доступа.
- Контроль доступа к аппаратуре.
- Разграничение и контроль доступа к информации.
- Предоставление привилегий на доступ.
- Идентификация и установление подлинности объекта (субъекта).
- Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
- Методы и средства защиты информации от случайных воздействий.
- Методы защиты информации от аварийных ситуаций.
- Организационные мероприятия по защите информации.
- Выбор средств информационной безопасности.
- Информационное страхование.
- Классификация методов криптографического закрытия информации.
- Шифрование.
- Кодирование.
- Стеганография.
- Электронная цифровая подпись
- Законодательство в области лицензирования и сертификации.
- Правила функционирования системы лицензирования

- Критерии безопасности компьютерных систем «Оранжевая книга».
- Правовые документы Российской Федерации в области информации

Шкала и критерии оценивания
самоподготовки по темам практических и лабораторных занятий

- оценка «зачтено» выставляется, если обучающийся на основе самостоятельного изученного материала, смог всесторонне раскрыть теоретическое содержание вопросов, владеет методиками при решении практических задач.

- оценка «не зачтено» выставляется, если обучающийся не смог раскрыть теоретическое содержание вопросов, не владеет методиками при решении практических задач или выполнил несамостоятельно.

3.1.4. Средства для промежуточной аттестации по итогам изучения дисциплины

Типовые тестовые вопросы итогового тестирования

1) Основными источниками угроз информационной безопасности являются...
Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
Хищение данных, подкуп системных администраторов, нарушение регламента работы

2) К видам информационной безопасности относятся…
+ Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
Локальная, глобальная, смешанная

3) Цели информационной безопасности – своевременное обнаружение, предупреждение…
+ несанкционированного доступа
инсайдерства в организации
чрезвычайных ситуаций

4) Основными объектами информационной безопасности являются…
+ Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

5) Основными рисками информационной безопасности являются…
Искажение, уменьшение объема, перекодировка информации
Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

6) К основным принципам обеспечения информационной безопасности относится…
+ Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются…
руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести…
+ Установление регламента, аудит системы, выявление рисков
Установка новых офисных приложений, смена хостинг-компании
Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения…
+ Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности

11) Принципом политики информационной безопасности является принцип…
+ Невозможности миновать защитные средства сети (системы)

Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип…
+ Усиления защищенности самого незащищенного звена сети (системы)
Перехода в безопасное состояние работы сети, системы
Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип…
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Одноуровневой защиты сети, системы
Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится…
Компьютерный сбой
+ Логические закладки («мины»)
Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует…
Прочитать приложение, если оно не содержит ничего ценного – удалить
Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа…
Секретность ключа определена секретностью открытого сообщения
Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП расшифровывается как…
Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
Электронно-цифровой процессор

18) Наиболее распространенной угрозой информационной безопасности корпоративной системы является…
Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
Сознательного внедрения сетевых вирусов

19) Наиболее распространенными угрозами информационной безопасности сети являются…
Распределенный доступ клиент, отказ оборудования
Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространенными средствами воздействия на сеть офиса являются…
Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая…
+ Потерей данных в системе
Изменением формы информации
Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности является…
+ Целостность
Доступность
Актуальность

23) Угроза информационной системе (компьютерной сети) – это…
+ Вероятное событие
Детерминированное (всегда определенное) событие

Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется…
Регламентированной
Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются…
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет…
+ Владелец сети
Администратор сети
Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс…
+ Руководств, требований обеспечения необходимого уровня безопасности
Инструкций, алгоритмов поведения пользователя в сети
Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является…
Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

29) Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется…
достоверной
конфиденциальной
+ документированной
коммерческой тайной

30) Формы защиты интеллектуальной собственности - …
+ авторское, патентное право и коммерческая тайна
интеллектуальное право и смежные права
коммерческая и государственная тайна
гражданское и административное право

31) По принадлежности информационные ресурсы подразделяются на…
+ государственные, коммерческие и личные
государственные, не государственные и информацию о гражданах
информацию юридических и физических лиц
официальные, гражданские и коммерческие

32) По доступности информация классифицируется на…
открытую информацию и государственную тайну
конфиденциальную информацию и информацию свободного доступа
+ информацию с ограниченным доступом и общедоступную информацию
виды информации, указанные в остальных пунктах

33) К конфиденциальной информации относятся документы, содержащие…
+ государственную тайну
законодательные акты
"ноу-хау"
сведения о золотом запасе страны

34) Запрещено относить к информации ограниченного доступа…
информацию о чрезвычайных ситуациях
информацию о деятельности органов государственной власти
документы открытых архивов и библиотек
+ все, перечисленное в остальных пунктах

35) К конфиденциальной информации НЕ относится…
коммерческая тайна
персональные данные о гражданах
государственная тайна
+"ноу-хау"

36) Вопросы информационного обмена регулируются (...) правом.
+ гражданским
информационным
конституционным
уголовным

37) Система криптографической защиты информации называется…
BFox Pro
CAudit Pro
+ Крипто Про +

38) Вирусы, которые активизируются в самом начале работы с операционной системой называются…
+ загрузочные вирусы
троянцы
черви

39) Под информационной безопасностью понимается…
+ **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.**
- программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
- нет правильного ответа

40) Защита информации – это..
+ **комплекс мероприятий, направленных на обеспечение информационной безопасности.**
- процесс разработки структуры базы данных в соответствии с требованиями пользователей
- небольшая программа для выполнения определенной задачи

41) От чего зависит информационная безопасность?
А) **от компьютеров**
Б) от поддерживающей инфраструктуры
В) от информации

42) Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

Доступность – это…
А) **возможность за приемлемое время получить требуемую информационную услугу.**
Б) логическая независимость
В) нет правильного ответа

43) Целостность – это..
А) **целостность информации**
Б) непротиворечивость информации
В) защищенность от разрушения

44) Конфиденциальность – это..
А) **защита от несанкционированного доступа к информации**
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

45) Для чего создаются информационные системы?
А) **получения определенных информационных услуг**
Б) обработки информации
В) все ответы правильные

46) Целостность можно подразделить:
А) **статическую**
Б) динамичную
В) структурную

47) Где применяются средства контроля динамической целостности?
А) **анализе потока финансовых сообщений**
Б) обработке данных
В) **при выявлении кражи, дублирования отдельных сообщений**

48) Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) **все ответы правильные**

49) Угроза – это…
А) **потенциальная возможность определенным образом нарушить информационную безопасность**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

50) Атака – это…
А) **попытка реализации угрозы**
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

51) Источник угрозы – это..
А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа

52) Окно опасности – это…
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.**
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

53) Какие события должны произойти за время существования окна опасности?
А) **должно стать известно о средствах использования пробелов в защите.**
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

54) Угрозы можно классифицировать по нескольким критериям:
А) **по спектру И.Б.**
Б) по способу осуществления
В) по компонентам И.С.

55) По каким компонентам классифицируется угрозы доступности:
А) **отказ пользователей**
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

56) Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) **все ответы правильные**

57) Основными источниками внутренних отказов являются:
А) **ошибки при конфигурировании системы**
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

58) По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

59) Какие существуют грани вредоносного П.О.?
А) **вредоносная функция**
Б) внешнее представление
В) способ распространения

60) По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) **все ответы правильные**

61) Вирус – это…
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

62) Черви – это…
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

63) Конфиденциальную информацию можно разделить:
А**) предметную**
Б) служебную
В) глобальную

64) Природа происхождения угроз:
А) **случайные**
Б) преднамеренные
В) природные

65) Предпосылки появления угроз:
А) **объективные**
Б) субъективные
В) преднамеренные

66) К какому виду угроз относится присвоение чужого права?
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда

67) Отказ, ошибки, сбой – это:
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы

68) Отказ - это…
А) **нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций**
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

69) Ошибка – это…
А) **неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния**
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

70) Сбой – это…
А) **такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент**
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

71) Побочное влияние – это…
А) **негативное воздействие на систему в целом или отдельные элементы**
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

72) СЗИ (система защиты информации) делится:
А) **ресурсы автоматизированных систем**
Б) организационно-правовое обеспечение
В) человеческий компонент

73) Что относится к человеческому компоненту СЗИ?
А) **системные порты**
Б) администрация
В) программное обеспечение

74) Что относится к ресурсам А.С. СЗИ?
А) лингвистическое обеспечение
Б) техническое обеспечение
В) **все ответы правильные**

75) По уровню обеспеченной защиты все системы делят:
А) **сильной защиты**
Б) особой защиты
В) слабой защиты

76) По активности реагирования СЗИ системы делят:
А) **пассивные**
Б) активные
В) полупассивные

77) Правовое обеспечение безопасности информации – это…
А) **совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

78) Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы
Б) национально-правовые нормы
В) **все ответы правильные**

79) Информацию с ограниченным доступом делят:
А) **государственную тайну**
Б) конфиденциальную информацию
В) достоверную информацию

80) Что относится к государственной тайне?
А) **сведения, защищаемые государством в области военной, экономической … деятельности**
Б) документированная информация
В) нет правильного ответа

81) Вредоносная программа - это…
А) **программа, специально разработанная для нарушения нормального функционирования систем**
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

82) Основополагающие документы для обеспечения безопасности внутри организации:
А) **трудовой договор сотрудников**
Б) должностные обязанности руководителей
В) коллективный договор

83) К организационно - административному обеспечению информации относится:
А) **взаимоотношения исполнителей**
Б) подбор персонала
В) регламентация производственной деятельности

84) Что относится к организационным мероприятиям:
А) **хранение документов**
Б) проведение тестирования средств защиты информации
В) **пропускной режим**

85) Какие средства используется на инженерных и технических мероприятиях в защите информации:
А) **аппаратные**
Б) криптографические
В) физические

86) Программные средства – это…
А) **специальные программы и системы защиты информации в информационных системах различного назначения**
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ

ответов на тестовые вопросы тестирования по итогам освоения дисциплины

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

4. Промежуточная (семестровая) аттестация по курсу

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 -	зачёт
Место процедуры получения зачёта в графике учебного процесса	1) участие обучающегося в процедуре получения зачёта осуществляется за счёт учебного времени (трудоёмкости), отведённого на изучение дисциплины
	2) процедура проводится в рамках ВАРО, на последней неделе семестра
Основные условия получения обучающимся зачёта:	1) обучающийся выполнил все виды учебной работы (включая самостоятельную) и отчитался об их выполнении в сроки, установленные графиком учебного процесса по дисциплине; 2) прошёл заключительное тестирование;
Процедура получения зачёта -	Представлены в Фонде оценочных средств по данной учебной дисциплине (см. – Приложение 9)
Методические материалы, определяющие процедуры оценивания знаний, умений, навыков:	

ЛИСТ РАССМОТРЕНИЙ И ОДОБРЕНИЙ
Фонда оценочных средств
рабочей программы дисциплины Б1.В.ДВ.01.01 Информационная безопасность
в составе ОПОП
36.03.02 Зоотехния

1) Рассмотрен и одобрен в качестве базового варианта:
а) На заседании обеспечивающей преподавание кафедры Математических и естественнонаучных дисциплин; протокол № 14 от 25 .05.2021 Зав. кафедрой, к.э.н., доцент _____Т.Ю. Степанова
б) На заседании методической комиссии по направлению – 36.03.02 Зоотехния; протокол № 10 от 10.06.2021 Председатель МКН – 36.03.02, канд. с.-х. наук, доцент _____ И.А. Коршева
2) Рассмотрен и одобрен внешним экспертом
а) Канд. пед. наук, доцент кафедры информатики и методики обучения информатике ФГБОУ ВО ОмГПУ _____Е.С. Гайдамак

«Омский государственный педагогический университет» (ФГБОУ ВО «ОмГПУ»)

ВЕРНО
Начальник отдела кадров ОмГПУ
Останина Е.А.
«29» 06 2021 г.

ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ
к фонду оценочных средств учебной дисциплины
Б1.В.ДВ.01.01 Информационная безопасность
в составе ОПОП 36.03.02 Зоотехния

Ведомость изменений

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