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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по освоению учебной дисциплины

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

Содержание

ВВЕДЕНИЕ

1. Настоящее издание является основным организационно-методическим документом учебно-методического комплекса по дисциплине в составе основной профессиональной образовательной программы высшего образования (ОПОП ВО). Оно предназначено стать для них методической основой по освоению данной дисциплины.

2. Содержательной основой для разработки настоящих методических указаний послужила Рабочая программа дисциплины, утвержденная в установленном порядке.

3. Методические аспекты развиты в учебно-методической литературе и других разработках, входящих в состав УМК по данной дисциплине.

4. Доступ обучающихся к электронной версии Методических указаний по изучению дисциплины, обеспечен в информационно-образовательной среде университета.

При этом в электронную версию могут быть внесены текущие изменения и дополнения, направленные на повышение качества настоящих методических указаний.

Уважаемые обучающиеся!

Приступая к изучению новой для Вас учебной дисциплины, начните с вдумчивого прочтения разработанных для Вас кафедрой специальных методических указаний. Это поможет Вам вовремя понять и правильно оценить ее роль в Вашем образовании.

Ознакомившись с организационными требованиями кафедры по этой дисциплине и соизмерив с ними свои силы, Вы сможете сделать осознанный выбор собственной тактики и стратегии учебной деятельности, уберечь самих себя от неразумных решений по отношению к ней в начале семестра, а не тогда, когда уже станет поздно. Используя эти указания, Вы без дополнительных осложнений подойдете к промежуточной аттестации по этой дисциплине. Успешность аттестации зависит, прежде всего, от Вас. Ее залог – ритмичная, целенаправленная, вдумчивая учебная работа, в целях обеспечения которой и разработаны эти методические указания.

1. Место учебной дисциплины в подготовке выпускника

Учебная дисциплина относится к дисциплинам ОПОП университета, состав которых определяется вузом и требованиями ФГОС.

Цель дисциплины – ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами, научить использовать современные методы защиты информации на уровне квалифицированного пользователя, как на локальных компьютерах, так и в компьютерных сетях.

В ходе освоения дисциплины обучающийся должен:

иметь целостное представление о сущности информации, информационных процессов и информационной безопасности и методах ее защиты; о проблемах защиты информации в персональных компьютерах и сетях;

владеть навыками применения методов и средств защиты информации, включая криптографические;

знать:

- основные понятия и определения ИБ;
- виды объектов, подлежащих защите;
- уровни ИБ объектов;
- виды и назначение различных мер обеспечения ИБ;
- особенности использования технических и программных мер по обеспечению ИБ;
- основные принципы построения систем защиты информации;
- классификацию вирусов;
- средства защиты от воздействия вирусов;
- классификацию антивирусных программ;
- методы профилактики заражения вирусами;
- основные международные правовые акты по защите информации;
- Российские общегосударственные правовые документы по защите информации;
- Российские отраслевые нормативные документы по защите информации;

уметь:

- применять организационные, технические и программные средства защиты информации;
- распознавать воздействия вируса на информацию;
- использовать антивирусные программы.

1.1. Перечень компетенций с указанием этапов их формирования в результате освоения учебной дисциплины:

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

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

<table>
<tr><td rowspan="7">Индекс и название компетенции</td><td rowspan="7">Код индикатора достижений компетенции</td><td rowspan="7">Индикаторы компетенции</td><td rowspan="7">Показатель оценивания – знания, умения, навыки (владения)</td><td colspan="4">Уровни сформированности компетенций</td><td rowspan="7">Формы и средства контроля формирования компетенций</td></tr>
<tr><td>компетенция не сформирована</td><td>минимальный</td><td>средний</td><td>высокий</td></tr>
<tr><td colspan="4">Оценки сформированности компетенций</td></tr>
<tr><td>Не зачтено</td><td colspan="3">Зачтено</td></tr>
<tr><td colspan="4">Характеристика сформированности компетенции</td></tr>
<tr><td>Компетенция в полной мере не сформирована. Имеющихся знаний, умений и навыков недостаточно для решения практических (профессиональных) задач</td><td colspan="3">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.</td></tr>
<tr><td colspan="9">Критерии оценивания</td></tr>
<tr><td rowspan="2">ПК-1</td><td rowspan="2">ИД-1$_{ПК-1}$</td><td>Полнота знаний</td><td>Знает информационно-коммуникативные и цифровые технологии, основные понятия информационной безопасности, основные виды угроз, пути и каналы утечки информации</td><td>Не знает информационно-коммуникативные и цифровые технологии, основные понятия информационной безопасности, основные виды угроз, пути и каналы утечки информации</td><td colspan="3">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</td><td rowspan="2">Тестирование, эссе, электронная презентация, опрос</td></tr>
<tr><td>Наличие умений</td><td>Умеет использовать информационно-коммуникативные и цифровые технологии, соблюдает основные требования информационной безопасности</td><td>Не умеет использовать информационно-коммуникативные и цифровые технологии, соблюдает основные требования информационной безопасности</td><td colspan="3">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</td></tr>
</table>

		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	

2. Структура учебной работы, содержание и трудоёмкость основных элементов дисциплины

2.1. Организационная структура, трудоемкость и план изучения дисциплины

Вид учебной работы		Трудоемкость, час			
		семестр, курс*			
		очная / очно-заочная форма		заочная форма	
		3 сем.	№ сем.	2 курс	№ курса
1. Аудиторные занятия, всего		**56**		**10**	
- лекции		24		4	
- практические занятия (включая семинары)		32		6	
- лабораторные работы					
2. Внеаудиторная академическая работа		**52**		**94**	
2.1 Фиксированные виды внеаудиторных самостоятельных работ:					
Выполнение и сдача/защита индивидуального/группового задания в виде**					
- Выполнение электронной презентации		6		8	
- Выполнение эссе		6		8	
2.2 Самостоятельное изучение тем/вопросов программы		24		64	
2.3 Самоподготовка к аудиторным занятиям		10		4	
2.4 Самоподготовка к участию и участие в контрольно-оценочных мероприятиях, проводимых в рамках текущего контроля освоения дисциплины (*за исключением учтённых в пп. 2.1 – 2.2):*		6		10	
3. Получение зачёта по итогам освоения дисциплины		+		**4**	
ОБЩАЯ трудоемкость дисциплины:	**Часы**	**108**		**108**	
	Зачетные единицы	**3**		**3**	

Примечание:
* – ***семестр*** – для очной и очно-заочной формы обучения, ***курс*** – для заочной формы обучения;
** – КР/КП, реферата/эссе/презентации, контрольной работы (для обучающихся заочной формы обучения), расчетно-графической (расчетно-аналитической) работы и др.;

2.2. Укрупнённая содержательная структура учебной дисциплины и общая схема её реализации в учебном процессе

	Номер и наименование раздела дисциплины. Укрупненные темы раздела	Трудоемкость раздела и ее распределение по видам учебной работы, час.							Формы текущего контроля успеваемости и промежуточной аттестации	№№ компетенций, на формирование которых ориентирован раздел
		общая	Аудиторная работа				ВАРС			
			всего	лекции	занятия		всего	фиксированные виды		
					практические (всех форм)	лабораторные				
		2	3	4	5	6	7	8	9	10
Очная/очно-заочная форма обучения										
1	**Актуальность информационной безопасности. Угрозы информации** 1.1 Актуальность информационной безопасности. Классификация компьютерных преступлений. 1.2 Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Интернете. 1.3 Виды угроз информационной безопасности РФ 1.4 Источники угроз информационной безопасности РФ. Удаленные атаки на интрасети.	30	14	6	8	0	16	4	Электронная презентация, эссе, опрос, тестовые вопросы	ПК-1
2	**Вредоносные программы. Защита от компьютерных вирусов**	38	20	8	12	0	18	4	Электронная	ПК-1

	2.1 Условия существования вредоносных программ.								презентация, эссе, опрос, тестовые вопросы	
	2.2 Классические компьютерные вирусы.									
	2.3 Защита от компьютерных вирусов: признаки и источники заражения									
	2.4 Основные правила защиты. Антивирусные программы.									
3	**Методы и средства защиты компьютерной информации. Правовые документы**	40	22	10	12	0	18	4	Электронная презентация, эссе, опрос, тестовые вопросы	ПК-1
	3.1 Методы обеспечения информационной безопасности РФ.									
	3.2 Ограничение доступа. Идентификация и установление подлинности объекта (субъекта).									
	3.3 Методы и средства защиты информации, включая криптографические									
	3.4 Лицензирование и сертификация в области защиты информации									
	3.5 Правовые документы по информационной безопасности									
	Промежуточная аттестация		×	×	×	×	×	×	зачет	
	Итого по дисциплине	108	56	24	32	0	52	12		
Заочная форма обучения										
1	**Актуальность информационной безопасности. Угрозы информации**	33	3	1	2	0	30	4	Электронная презентация, эссе, опрос, тестовые вопросы	ПК-1
	1.1 Актуальность информационной безопасности. Классификация компьютерных преступлений.									
	1.2 Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Интернете.									
	1.3 Виды угроз информационной безопасности РФ									
	1.4 Источники угроз информационной безопасности РФ. Удаленные атаки на интрасети.									
2	**Вредоносные программы. Защита от компьютерных вирусов**	35	3	1	2	0	32	6	Электронная презентация, эссе, опрос, тестовые вопросы	ПК-1
	2.1 Условия существования вредоносных программ.									
	2.2 Классические компьютерные вирусы.									
	2.3 Защита от компьютерных вирусов: признаки и источники заражения									
	2.4 Основные правила защиты. Антивирусные программы.									
3	**Методы и средства защиты компьютерной информации. Правовые документы**	36	4	2	2	0	32	6	Электронная презентация, эссе, опрос, тестовые вопросы	ПК-1
	3.1 Методы обеспечения информационной безопасности РФ.									
	3.2 Ограничение доступа. Идентификация и установление подлинности объекта (субъекта).									
	3.3 Методы и средства защиты информации, включая криптографические									
	3.4 Лицензирование и сертификация в области защиты информации									
	3.5 Правовые документы по информационной безопасности									
	Промежуточная аттестация	4	×	×	×	×	×	×	зачет	
	Итого по дисциплине	108	10	4	6	0	94	16		

3. Общие организационные требования к учебной работе обучающегося

3.1. Организация занятий и требования к учебной работе обучающегося

Организация занятий по дисциплине носит циклический характер. По всем разделам предусмотрена взаимоувязанная цепочка учебных работ: лекция – самостоятельная работа обучающихся (аудиторная и внеаудиторная). На занятиях студенческая группа получает задания и рекомендации.

Для своевременной помощи обучающимся при изучении дисциплины кафедрой организуются индивидуальные и групповые консультации, устанавливается время приема выполненных работ.

Учитывая статус дисциплины к её изучению предъявляются следующие организационные требования;:

- обязательное посещение обучающимся всех видов аудиторных занятий;
- ведение конспекта в ходе лекционных занятий;
- качественная самостоятельная подготовка к практическим занятиям, активная работа на них;
- активная, ритмичная самостоятельная аудиторная и внеаудиторная работа обучающегося в соответствии с планом-графиком; своевременная сдача преподавателю отчетных документов по аудиторным и внеаудиторным видам работ;
- в случае наличия пропущенных обучающимся занятиям, необходимо получить консультацию по подготовке и оформлению отдельных видов заданий.

Для успешного освоения дисциплины, обучающемуся предлагаются учебно-информационные источники в виде учебной, учебно-методической литературы по всем разделам.

4. Лекционные занятия

Для изучающих дисциплину читаются лекции в соответствии с планом, представленным в таблице 3.

Таблица 3 - Лекционный курс.

№ раздела	№ лекции	Тема лекции. Основные вопросы темы	Трудоемкость по разделу, час. очная форма	Трудоемкость по разделу, час. заочная форма	Применяемые интерактивные формы обучения
1	2	3	4	5	6
1	1, 2	Тема: Актуальность информационной безопасности		1	
		1. Актуальность информационной безопасности. Классификация компьютерных преступлений.	2		
		2 Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Интернете.	2		Лекция визуализация
	3	Тема: Угрозы информации			
		1.Виды угроз информационной безопасности РФ	2		
		2.Источники угроз информационной безопасности РФ. Удаленные атаки на интрасети.			
2	4, 5	Тема: Вредоносные программы.		1	
		1. Условия существования вредоносных программ.	2		
		2.Классические компьютерные вирусы.	2		Лекция визуализация
	6, 7	Тема: Защита от компьютерных вирусов			
		1.Защита от компьютерных вирусов: признаки и источники заражения	2		
		2. Основные правила защиты. Антивирусные программы.	2		Лекция с разбором конкретных ситуаций
3	8, 9	Тема: Методы и средства защиты компьютерной информации		2	
		1. Методы обеспечения информационной безопасности РФ.	2		
		2. Ограничение доступа. Идентификация и установление подлинности объекта (субъекта).	2		
	10, 11	Тема: Криптографические методы информационной безопасности			
		1. Классификация методов криптографического закрытия информации.	4		Лекция визуализация
		2. Шифрование, кодирование и стенография			
		3. Электронная цифровая подпись			
	12	Тема: Правовые документы и лицензии в области информационной безоавсности			
		1. Лицензирование и сертификация в области защиты информации	1		
		2. Правовые документы по информационной безопасности	1		
Общая трудоемкость лекционного курса			24	4	x

Всего лекций по дисциплине:	час.	Из них в интерактивной форме:	час.
- очная/очно-заочная форма обучения	24	- очная/очно-заочная форма обучения	10
- заочная форма обучения	4	- заочная форма обучения	2

5. Практические занятия по дисциплине и подготовка к ним

Практические занятия по курсу проводятся в соответствии с планом, представленным в таблице 4.

Таблица 4 - Примерный тематический план практических занятий по разделам учебной дисциплины

№ раздела (модуля)	№ занятия	Тема занятия / Примерные вопросы на обсуждение (для семинарских занятий)	Трудоемкость по разделу, час. очная форма	Трудоемкость по разделу, час. заочная форма	Используемые интерактивные формы**	Связь занятия с ВАРС*
1	2	3	4	5	6	7
1	1, 2	Тема: Актуальность информационной безопасности		2		**ОСП УЗ СРС**
		1. Актуальность информационной безопасности. Классификация компьютерных преступлений.	2			
		2 Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Интернете.	2			
	3, 4	Тема: Угрозы информации				
		1.Виды угроз информационной безопасности РФ	2		Работа в малых группах	
		2.Источники угроз информационной безопасности РФ. Удаленные атаки на интрасети.	2			
2	5, 6	Тема: Вредоносные программы.		2		**ОСП УЗ СРС**
		1. Условия существования вредоносных программ.	2			
		2.Классические компьютерные вирусы.	2		Работа в малых группах	
	7-10	Тема: Защита от компьютерных вирусов				
		1.Защита от компьютерных вирусов: признаки и источники заражения	4			
		2. Основные правила защиты. Антивирусные программы.	4			
3	11, 12	Тема: Методы и средства защиты компьютерной информации		2		**ОСП УЗ СРС**
		1. Методы обеспечения информационной безопасности РФ.	2			
		2. Ограничение доступа. Идентификация и установление подлинности объекта (субъекта).	2		Работа в малых группах	
	13, 14	Тема: Криптографические методы информационной безопасности				
		1. Классификация методов криптографического закрытия информации.	4		Работа в малых группах	
		2. Шифрование, кодирование и стенография				
		3. Электронная цифровая подпись				
	15, 16	Тема: Правовые документы и лицензии в области информационной безоавсности				
		1. Лицензирование и сертификация в области защиты информации	2			
		2. Правовые документы по информационной безопасности	2			

Всего практических занятий по дисциплине:	час.	Из них в интерактивной форме:	час.
- очная/очно-заочная форма обучения	32	- очная/очно-заочная форма обучения	10
- заочная форма обучения	6	- заочная форма обучения	
В том числе в форме семинарских занятий			
- очная/очно-заочная форма обучения			
- заочная форма обучения			

** Условные обозначения:*
ОСП – предусмотрена обязательная самоподготовка к занятию; **УЗ СРС** – на занятии выдается задание на конкретную ВАРС; **ПР СРС** – занятие содержательно базируется на результатах выполнения обучающимся конкретной ВАРС.

** в т.ч. при использовании материалов МООК «Название», название ВУЗа-разработчика, название платформы и ссылка на курс (с указанием даты последнего обращения)

Подготовка обучающихся к практическим занятиям осуществляется с учетом общей структуры учебного процесса. На практических занятиях осуществляется текущий аудиторный контроль в виде опроса, по основным понятиям дисциплины.

Подготовка к практическим занятия подразумевает выполнение домашнего задания к очередному занятию по заданиям преподавателя, выдаваемым в конце предыдущего занятия.

6. Общие методические рекомендации по изучению отдельных разделов дисциплины

При изучении конкретного раздела дисциплины, из числа вынесенных на лекционные и практические занятия, обучающемуся следует учитывать изложенные ниже рекомендации. Обратите на них особое внимание при подготовке к аттестации.

Работа по теме прежде всего предполагает ее изучение по учебнику или пособию. Работа по теме кроме ее изучения по учебнику, пособию предполагает также поиск по теме научных статей в научных журналах.

Самостоятельная подготовка предполагает использование ряда методов.

1. Конспектирование. Конспектирование позволяет выделить главное в изучаемом материале и выразить свое отношение к рассматриваемой автором проблеме.

Техника записей в конспекте индивидуальна, но есть ряд правил, которые могут принести пользу его составителю: начиная конспект, следует записать автора изучаемого произведения, его название, источник, где оно опубликовано, год издания. Порядок конспектирования:

а) внимательное чтение текста;

б) поиск в тексте ответов на поставленные в изучаемой теме вопросы;

в) краткое, но четкое и понятное изложение текста;

г) выделение в записи наиболее значимых мест;

д) запись на полях возникающих вопросов, понятий, категорий и своих мыслей.

2. Записи в форме тезисов, планов, аннотаций, формулировок определений. Все перечисленные формы помогают быстрой ориентации в подготовленном материале, подборе аргументов в пользу или против какого- либо утверждения.

3. Словарь понятий и категорий. Составление словаря помогает быстрее осваивать новые понятия и категории, увереннее ими оперировать

Раздел 1. Актуальность информационной безопасности. Угрозы информации

Краткое содержание

1. Актуальность информационной безопасности.
2. Классификация компьютерных преступлений.
3 Способы совершения компьютерных преступлений.
4. Пользователи и злоумышленники в Интернете.
5.Виды угроз информационной безопасности РФ
6.Источники угроз информационной безопасности РФ.
7. Удаленные атаки на интрасети.

Вопросы для самоконтроля по разделу:

1) Дайте определение информации?
2) Перечислите основные свойства информации?
3) Что понимается под информационной безопасностью?
4) Какие классификации компьютерных преступлений существуют?
5) Как следует понимать слово «угроза»?
6) Кто такие злоумышленники?
7) Назовите источники угроз информационной безопасности
8) Какие способы совершения компьютерных преступлений существуют?

Раздел 2. Вредоносные программы. Защита от компьютерных вирусов

Краткое содержание

1. Условия существования вредоносных программ.
2. Классические компьютерные вирусы.
3. Защита от компьютерных вирусов: признаки и источники заражения
4. Основные правила защиты.
5. Антивирусные программы.

Вопросы для самоконтроля по разделу:

1) Назовите основные типы вредоносных программ.
2) При каких условиях могут существовать вредоносные программы.
3) Что такое классические компьютерные вирусы?

4) Как защититься от компьютерных вирусов?
5) Опишите основные правила защиты от компьютерных вирусов
6) Какие антивирусные программы вы знаете?

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

Краткое содержание

1. Методы обеспечения информационной безопасности РФ.
2. Ограничение доступа.
3. Идентификация и установление подлинности объекта (субъекта).
4. Методы и средства защиты информации, включая криптографические
5. Лицензирование и сертификация в области защиты информации
6. Правовые документы по информационной безопасности

Вопросы для самоконтроля по разделу:

1) Какие методы обеспечения информационной безопасности вы знаете?
2) Какие методы обеспечения информационной безопасности используют в РФ?
3) Расскажите об ограничении доступа к информации.
4) Как идентифицировать личность и установить ее подлинность?
5) Охарактеризуйте экспертные системы и области их применения.
6) Перечислите методы защиты информации.
7) Какие средства можно использовать для защиты информации?
8) Что такое криптография?
9) Перечислите криптографические методы защиты информации
10) Работает ли в области защиты информации юридические правила?
11) Какие правовые документы существуют в области защиты информации в РФ?

7. Общие методические рекомендации по оформлению и выполнению отдельных видов ВАРС

7.1. Рекомендации по выполнению и сдачи индивидуального задания в виде эссе

Учебные цели, на достижение которых ориентировано выполнение эссе: получить целостное представление о понятии информационная безопасность.

Учебные задачи, которые должны быть решены обучающимся в рамках выполнения эссе: формирование и отработка навыков работы над защитой информации.

***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 не самостоятельно**.**

7.2. Рекомендации по выполнению электронной презентации

Учебные цели, на достижение которых ориентировано выполнение электронной презентации: получить целостное представление о понятии информационная безопасность.

Учебные задачи, которые должны быть решены обучающимся в рамках выполнения электронной презентации: формирование и отработка навыков работы над защитой информации

***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 защита 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**.**

7.3. Рекомендации по самостоятельному изучению тем

Темы для самостоятельного изучения:

- 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%).

8. Текущий (внутрисеместровый) контроль хода и результатов учебной работы

8.1 Текущий контроль успеваемости

В течение семестра, проводится текущий контроль успеваемости по дисциплине, к которому обучающийся должен быть подготовлен.

Отсутствие пропусков аудиторных занятий, активная работа на практических занятиях, общее выполнение графика учебной работы являются основанием для получения положительной оценки по текущему контролю.

В качестве текущего контроля может быть использовано экспресс-тестирование. Тест состоит из небольшого количества элементарных вопросов по основным разделам дисциплины: неправильные решения разбираются на следующем занятии; частота тестирования определяется преподавателем.

ВОПРОСЫ и ЗАДАЧИ
для самоподготовки к практическим и лабораторным занятиям

Общий алгоритм самоподготовки

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

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 занятий

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

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

.

9. Промежуточная (семестровая) аттестация по курсу

6.1 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»	
6.2 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:	

9.2. Итоговое тестирование по итогам изучения дисциплины

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

9.2.1 Подготовка к итоговому тестированию

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

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

Подготовка к заключительному тестированию по итогам изучения дисциплины

Тестирование осуществляется по всем темам и разделам дисциплины, включая темы, выносимые на самостоятельное изучение. Процедура тестирования ограничена во времени и предполагает максимальное сосредоточение обучающегося на выполнении теста, содержащего несколько тестовых заданий.

Тестирование проводится в письменной форме (на бумажном носителе) или электронной форме. Тест включает в себя 24 вопроса. Время, отводимое на выполнение теста - 30 минут. На тестирование выносится по 6 вопросов из каждого раздела дисциплины.

Бланк теста (в случае выполнения в письменной форме)
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»

Тестирование по итогам освоения дисциплины «Информационная безопасность»
Для обучающихся направления подготовки 36.03.02

ФИО_____**группа**_____
Дата_____

Уважаемые обучающиеся!

Прежде чем приступить к выполнению заданий внимательно ознакомьтесь с инструкцией:

1. Отвечая на вопрос с выбором правильного ответа, правильный, на ваш взгляд, ответ (ответы) обведите в кружок.
2. В заданиях открытой формы впишите ответ в пропуск.
3. В заданиях на соответствие заполните таблицу.
4. В заданиях на правильную последовательность впишите порядковый номер в квадрат.
4. Время на выполнение теста – 30 минут
5. За каждый верный ответ Вы получаете 1 балл, за неверный – 0 баллов. Максимальное количество полученных баллов 25.

Желаем удачи!

Типовые тестовые вопросы итогового тестирования

1. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации, называется….
а) защищенная информация
б) конфиденциальная информация
в) защищаемая информация
г) чувствительная информация
2. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации- это…
а) собственник информации
б) владелец информации
в) пользователь
г) носитель
3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена -это категория информационной безопасности называется…
а) конфиденциальность
б) целостность
в) аутентичность
г) ацеллируемость
4. Перечислите (не менее 3-х категорий информационных систем) _____
5. Снятие информации по виброакустичекому каналу- это…
а) активный перехват
б) аудиоперехват
в) видеоперехват
г) пассивный перехват
6. Несанкционированный доступ к компьютерной системе путем нахождения уязвимых мест в ее защите- это…
а) «брошь» б) «клюк» в) «компьютерный абордаж» г) «неспешный выбор»
7. Вредоносная программа для ЭВМ, способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять различные нежелательные действия, называются…
а) «логическая бомба»
б) «Троянский конь»
в) « компьютерный вирус»
г) «временная бомба»
8. К способам компьютерных преступлений относятся
а) атака
б) нострификация
в) маскарад
г) программирование
9. Мошенники , рассылающие свои послания в надежде поймать на наживу наивных и жадных –это…
а) скамер б) фракер в) фишер г) спамер

10. Конечное множество используемых для кодирования информации знаков –это…
а) текст
б) алфавит
в) ключ
г) криптосистема
11. Если символы исходного текста складываются с символами некой случайной последовательности, то это….
а) алгоритмы перестановки
б) алгоритмы замены
в) алгоритмы гаммирования
г) Комбинированные методы
12. Пользователь (потребитель) информации -это:
а) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
б) субъект , осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;
в) субъект, пользующий информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
г) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
13. Защита информации от несанкционированного доступа – это деятельность по предотвращению:
а) получаемой защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
б) 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;
в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
14. Доступ к информации -это:
а) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
в) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
15. Защита информации от утечки –это деятельность по предотвращению:
а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
б) 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;
в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

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.

Выставление оценки осуществляется с учетом описания показателей, критериев и шкал оценивания компетенций по дисциплине, представленных в таблице 1.2

10. Информационное и методическое обеспечение учебного процесса по дисциплине

В соответствии с действующими государственными требованиями для реализации учебного процесса по дисциплине обеспечивающей кафедрой разрабатывается и постоянно совершенствуется учебно-методический комплекс (УМКД), соответствующий данной рабочей программе и прилагаемый к ней. При разработке УМКД кафедра руководствуется установленными университетом требованиями к его структуре, содержанию и оформлению. В состав УМКД входят перечисленные ниже и другие источники учебной и учебно-методической информации, средства наглядности.

Предусмотренная рабочей учебной программой учебная и учебно-методическая литература размещена в фондах НСХБ и/или библиотеке обеспечивающей преподавание кафедры.

Учебно-методические материалы для обеспечения самостоятельной работы обучающихся размещены в электронном виде в ИОС ОмГАУ-Moodle (http://do.omgau.ru/course/view.php?id), где:

– *обучающийся* имеет возможность работать с изданиями ЭБС и электронными образовательными ресурсами, указанными в рабочей программе дисциплины, отправлять из дома выполненные задания и отчёты, задавать на форуме вопросы преподавателю или сокурсникам;

– *преподаватель* имеет возможность проверять задания и отчёты, оценивать работы, давать рекомендации, отвечать на вопросы (обратная связь), вести мониторинг выполнения заданий (освоения изучаемых разделов) по конкретному студенту и группе в целом, корректировать (в случае необходимости) учебно-методические материалы.

ПЕРЕЧЕНЬ
литературы, рекомендуемой
для изучения дисциплины

Автор, наименование, выходные данные	Доступ
Советов, Б. Я. Информационные технологии : учеб. для бакалавров / Б. Я. Советов, В. В. Цехановский ; С.-Петерб. гос. электротехн. ун-т. - 6-е изд. - Москва : Юрайт, 2012. - 263 с. - ISBN 978-5-9916-2016-1	НСХБ
Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 — Режим доступа: для авториз. пользователей.	http:// e.lanbook.com
Информационная безопасность : учебное пособие / составители Е. Р. Кирколуп [и др.]. — Барнаул : АлтГПУ, 2017. — 316 с. — ISBN 978-5-88210-898-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112164 — Режим доступа: для авториз. пользователей.	http:// e.lanbook.com
Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711 – Режим доступа: по подписке.	https://znanium.com
Использование облачных технологий в образовательной деятельности: руководство пользователя : учебное пособие / Т. Ю. Степанова, Л. В. Ламонина, Д. И. Гуляс, С. А. Беляков. — Омск : Омский ГАУ, 2015. — 60 с. — ISBN 978-5-89764-479-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/64855 — Режим доступа: для авториз. пользователей.	http:// e.lanbook.com
Инженерные технологии и системы : научный журнал. - Саранск : ФГБОУ ВПО "МГУ им. Н.П. Огарёва" - ISSN 2658-6525. - Текст : электронный. - URL: https://znanium.com	https://znanium.com

ПРИЛОЖЕНИЕ 1 Форма титульного листа электронной презентации

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

Факультет наименование

Кафедра наименование

Направление – (*код)* «(*наименование)*»

Презентация

по дисциплине наименование

на тему: _____

Выполнил(а): ст. ____группы

*ФИО*_____

Проверил(а): *уч. степень*, *должность*

*ФИО*_____

Омск – _____г.