



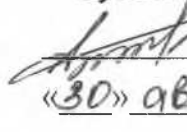
МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖИ РЕСПУБЛИКИ КРЫМ

Государственное бюджетное образовательное учреждение высшего образования
Республики Крым
«Крымский инженерно-педагогический университет имени Февзи Якубова»
(ГБОУВО РК КИПУ имени Февзи Якубова)

Кафедра мировой экономики и экономической теории

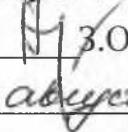
СОГЛАСОВАНО

Руководитель ОПОП

 И.Г. Курочкина
«30» августа 20 21 г.

УТВЕРЖДАЮ

Заведующий кафедрой

 З.О. Адаманова
«30» августа 20 21 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 «Информационная безопасность»

направление подготовки 38.03.01 Экономика
профиль подготовки «Цифровая экономика»

факультет экономики, менеджмента и информационных технологий

Симферополь, 2021

Рабочая программа дисциплины Б1.В.ДВ.03.02 «Информационная безопасность» для бакалавров направления подготовки 38.03.01 Экономика. Профиль «Цифровая экономика» составлена на основании ФГОС ВО, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 12.08.2020 № 954.

Составитель

рабочей программы


подпись

Г.Х. Аджимет, доц.

Рабочая программа рассмотрена и одобрена на заседании кафедры мировой экономики и экономической теории

от 24 августа 2021 г., протокол № 1

Заведующий кафедрой


подпись

З.О. Адаманова

Рабочая программа рассмотрена и одобрена на заседании УМК факультета экономики, менеджмента и информационных технологий

от 27 августа 2021 г., протокол № 1

Председатель УМК


подпись

К.М. Османов

1.Рабочая программа дисциплины Б1.В.ДВ.03.02 «Информационная безопасность» для бакалавриата направления подготовки 38.03.01 Экономика, профиль подготовки «Цифровая экономика».

2.Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

2.1. Цель и задачи изучения дисциплины (модуля)

Цель дисциплины (модуля):

– формирование знаний об информационной безопасности в условиях цифровой экономики и применения на практике методов и средств защиты информации, а также практических навыков для понимания роли и перспектив развития информационных процессов и информатизации общества.

Учебные задачи дисциплины (модуля):

- изучение общих понятий об информационной безопасности в цифровой экономике и стратегии защиты информации;
- приобретение теоретических навыков в изучении основ организации и регулирования информационной безопасности;
- рассмотрение и изучение проблем и перспектив обеспечения информационной безопасности.

2.2. Планируемые результаты освоения дисциплины

Процесс изучения дисциплины Б1.В.ДВ.03.02 «Информационная безопасность» направлен на формирование следующих компетенций:

ПК-2 - Способен обобщать и анализировать большие объемы финансовой информации, осуществлять расчет и прогнозирование финансовых показателей в целях повышения эффективности бизнеса с использованием информационных технологий

В результате изучения дисциплины студент должен:

Знать:

- основы понятия информационной безопасность, ее особенности в цифровой экономике, системы, задачи, цели и составляющие на всех уровнях обеспечения (ПК-2.3);
- методы и процедуры государственного контроля в сфере информационной безопасности (ПК-2.2);
- внутренние и внешние факторы и условия, влияющие на информационную безопасность (ПК-2.1);

Уметь:

- использовать информацию о современных проблемах обеспечения информационной безопасности в различных сферах и секторах российской цифровой экономики в свете глобализации мировой экономики (ПК-2.2);

- анализировать и давать оценку рискам и факторам, снижающим информационную безопасность (ПК-2.1);

Владеть:

- методами расчета эффективности использования индикаторов информационной безопасности (ПК-2.3);
- умением выявлять и анализировать угрозы информационной безопасности при осуществлении профессиональной деятельности (ПК-2.2).

3. Место дисциплины в структуре ОПОП.

Дисциплина Б1.В.ДВ.03.02 «Информационная безопасность» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений учебного плана.

4. Объем дисциплины (модуля)

(в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся)

Семестр	Общее кол-во часов	кол-во зач. единиц	Контактные часы						СР	Контроль (время на контроль)
			Всего	лек	лаб. зан.	прак. т.зан.	сем. зан.	ИЗ		
4	108	3	50	22		28			31	Экз (27 ч.)
Итого по ОФО	108	3	50	22		28			31	27

5. Содержание дисциплины (модуля) (структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий)

Наименование тем (разделов, модулей)	Количество часов														Форма текущего контроля
	очная форма							заочная форма							
	Всего	в том числе						Всего	в том числе						
		л	лаб	пр	сем	ИЗ	СР		л	лаб	пр	сем	ИЗ	СР	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Раздел 1. Информационная безопасность. Средства и методы защиты информации															
Тема 1. Основы информационной безопасности	12	4		4			4								тестовый контроль
Тема 2. Нормативно-правовое обеспечение информационной безопасности	10	2		4			4								тестовый контроль

Тема 3. Организационное обеспечение информационной безопасности	9	2		4			3								презентация
Тема 4. Средства и методы защиты информации	11	4		4			3								презентация
Раздел 2. Методы обеспечения информационной безопасности. Информационная безопасность экономических систем в национальной безопасности страны.															
Тема 5. Программно- аппаратные средства и методы обеспечения информационной безопасности	7	2		2			3								презентация
Тема 6. Криптографические методы защиты информации	7	2		2			3								тестовый контроль
Тема 7. Эффективность методов защиты информации в корпоративных вычислительных сетях и сети Интернет	9	2		4			3								презентация
Тема 8. Технологии построения защищенных систем	8	2		2			4								презентация
Тема 9. Информационная безопасность экономических систем в национальной безопасности страны	8	2		2			4								тестовый контроль; презентация
Всего часов за 4 семестр	81	22		28			31								
Форма промеж. контроля	Экзамен - 27 ч.														
Всего часов дисциплине	81	22		28			31								
часов на контроль	27														

5. 1. Тематический план лекций

№ лекц	Тема занятия и вопросы лекции	Форма проведения (актив., интерак.)	Количество часов	
			ОФО	ЗФО
1.	Тема 1. Основы информационной безопасности <i>Основные вопросы:</i> 1. Информационная безопасность. Основные понятия. 2. Модели информационной безопасности. 3. Виды защищаемой информации.	Акт.	4	
2.	Тема 2. Нормативно-правовое обеспечение информационной безопасности <i>Основные вопросы:</i> 1. Основные нормативно-правовые акты в области информационной безопасности. 2. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.	Акт.	2	
3.	Тема 3. Организационное обеспечение информационной безопасности <i>Основные вопросы:</i> 1. Организационное обеспечение информационной безопасности. 2. Политика безопасности. 3. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.	Акт.	2	
4.	Тема 4. Средства и методы защиты информации <i>Основные вопросы:</i> 1. Рассмотрение примеров методов защиты от промышленного шпионажа и экономической разведки. 2. Изучение настроек средств антивирусной защиты информации. 3. Создание защищенного канала связи средствами виртуальной частной сети.	Акт.	4	
5.	Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности	Акт.	2	

	<p><i>Основные вопросы:</i></p> <ol style="list-style-type: none"> 1. Основные виды сетевых и компьютерных угроз. 2. Средства и методы защиты от сетевых компьютерных угроз. 3. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. 4. Методы обеспечения информационной безопасности. 			
6.	<p>Тема 6. Криптографические методы защиты информации</p> <p><i>Основные вопросы:</i></p> <ol style="list-style-type: none"> 1. Анализ возможностей методов криптографии, которые могут быть использованы в целях защиты данных. 2. Применение криптографических систем шифрования данных. 3. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. 4. Использование средств стеганографии. 	Акт.	2	
7.	<p>Тема 7. Эффективность методов защиты информации в корпоративных вычислительных сетях и сети Интернет</p> <p><i>Основные вопросы:</i></p> <ol style="list-style-type: none"> 1. Исследование эффективности методов защиты информации в корпоративных вычислительных сетях. 2. Исследование эффективности методов защиты информации в глобальной сети Интернет. 	Акт.	2	
8.	<p>Тема 8. Технологии построения защищенных систем</p> <p><i>Основные вопросы:</i></p> <ol style="list-style-type: none"> 1. Основные регуляторы в сфере построения защищенных систем обработки информации. 2. Организационно-технологические меры защиты целостности информации. 3. Целостность данных в АС. Защита от угрозы нарушения целостности информации на уровне содержания 	Акт.	2	

9.	Тема 9. Информационная безопасность экономических систем в национальной безопасности страны <i>Основные вопросы:</i> 1. Информационная безопасность и информационные технологии. 2. Средства защиты информации. 3. Разработка сетевых аспектов политики безопасности. 4. Безопасность программной среды. Правила этикета при работе с компьютерной сетью.	Акт.	2	
Итого			22	0

5. 2. Темы практических занятий

№ занятия	Наименование практического занятия	Форма проведения (актив., интерак.)	Количество часов	
			ОФО	ЗФО
1.	Тема 1. Основы информационной безопасности <i>Основные вопросы:</i> Основы информационной безопасности	Акт.	4	
2.	Тема 2. Нормативно-правовое обеспечение информационной безопасности <i>Основные вопросы:</i> Нормативно-правовое обеспечение информационной безопасности	Акт.	4	
3.	Тема 3. Организационное обеспечение информационной безопасности <i>Основные вопросы:</i> Организационное обеспечение информационной безопасности	Акт./ Интеракт.	4	
4.	Тема 4. Средства и методы защиты информации <i>Основные вопросы:</i> Средства и методы защиты информации	Акт./ Интеракт.	4	
5.	Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности <i>Основные вопросы:</i> Программно-аппаратные средства и методы обеспечения информационной безопасности	Интеракт.	2	

6.	Тема 6. Криптографические методы защиты информации <i>Основные вопросы:</i> Криптографические методы защиты информации	Интеракт.	2	
7.	Тема 7. Эффективность методов защиты информации в корпоративных вычислительных сетях и сети Интернет <i>Основные вопросы:</i> Эффективность методов защиты информации в корпоративных вычислительных сетях и сети Интернет	Акт.	4	
8.	Тема 8. Технологии построения защищенных систем <i>Основные вопросы:</i> Технологии построения защищенных систем.	Акт.	2	
9.	Тема 9. Информационная безопасность экономических систем в национальной безопасности страны <i>Основные вопросы:</i> Информационная безопасность экономических систем в национальной безопасности страны	Акт.	2	
Итого			28	

5. 3. Темы семинарских занятий

(не предусмотрены учебным планом)

5. 4. Перечень лабораторных работ

(не предусмотрено учебным планом)

5. 5. Темы индивидуальных занятий

(не предусмотрено учебным планом)

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа по данной дисциплине включает такие формы работы как: работа с базовым конспектом; работа с литературой, чтение дополнительной литературы; подготовка к тестовому контролю; подготовка презентации; подготовка к экзамену.

6.1. Содержание самостоятельной работы студентов по дисциплине (модулю)

№	Наименование тем и вопросы, выносимые на самостоятельную работу	Форма СР	Кол-во часов
---	---	----------	--------------

	самостоятельную работу		ОФО	ЗФО
1	<p>Тема 1. Основы информационной безопасности</p> <p>Основные вопросы:</p> <p>1. Модели информационной безопасности.</p> <p>2. Виды защищаемой информации.</p>	<p>работа с литературой, чтение</p> <p>дополнительно й литературы; подготовка к тестовому контролю</p>	4	
2	<p>Тема 2. Нормативно-правовое обеспечение информационной безопасности</p> <p>Основные вопросы:</p> <p>Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.</p>	<p>работа с литературой, чтение</p> <p>дополнительно й литературы; подготовка к тестовому контролю</p>	4	
3	<p>Тема 3. Организационное обеспечение информационной безопасности</p> <p>Основные вопросы:</p> <p>1. Политика безопасности.</p> <p>2. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.</p>	<p>работа с литературой, чтение</p> <p>дополнительно й литературы; подготовка презентации</p>	3	
4	<p>Тема 4. Средства и методы защиты информации</p> <p>Основные вопросы:</p> <p>1. Изучение настроек средств антивирусной защиты информации.</p> <p>2. Создание защищенного канала связи средствами виртуальной частной сети.</p>	<p>работа с литературой, чтение</p> <p>дополнительно й литературы; подготовка презентации</p>	3	
5	<p>Тема 5. Программно-аппаратные средства и методы обеспечения информационной безопасности</p> <p>Основные вопросы:</p> <p>1. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей.</p> <p>2. Методы обеспечения информационной безопасности.</p>	<p>работа с литературой, чтение</p> <p>дополнительно й литературы; подготовка презентации; подготовка к тестовому контролю</p>	3	
6	<p>Тема 6. Криптографические методы защиты информации</p> <p>Основные вопросы:</p>	<p>работа с литературой, чтение</p> <p>дополнительно ..</p>	3	

	1. Применение криптографических систем шифрования данных. 2. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. 3. Использование средств стеганографии	й литературы; подготовка презентации		
7	Тема 7. Эффективность методов защиты информации в корпоративных вычислительных сетях и сети Интернет Основные вопросы: Исследование эффективности методов защиты информации в глобальной сети Интернет.	работа с литературой, чтение дополнительно й литературы; подготовка презентации; подготовка к тестовому контролю	3	
8	Тема 8. Технологии построения защищенных систем Основные вопросы: 1. Организационно-технологические меры защиты целостности информации. 2. Целостность данных в АС. Защита от угрозы нарушения целостности информации на уровне содержания	работа с литературой, чтение дополнительно й литературы; подготовка презентации	4	
9	Тема 9. Информационная безопасность экономических систем в национальной безопасности страны Основные вопросы: 1. Средства защиты информации. 2. Безопасность программной среды. 3. Правила этикета при работе с компьютерной сетью.	работа с литературой, чтение дополнительно й литературы; подготовка презентации	4	
	Итого		31	

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Дескрипторы	Компетенции	Оценочные средства
ПК-2		

Знать	основы понятия информационной безопасности, ее особенности в цифровой экономике, системы, задачи, цели и составляющие на всех уровнях обеспечения (ПК-2.3); методы и процедуры государственного контроля в сфере информационной безопасности (ПК-2.2); внутренние и внешние факторы и условия, влияющие на информационную безопасность (ПК-2.1)	тестовый контроль; презентация
Уметь	использовать информацию о современных проблемах обеспечения информационной безопасности в различных сферах и секторах российской цифровой экономики в свете глобализации мировой экономики (ПК-2.2); анализировать и давать оценку рискам и факторам, снижающим информационную безопасность (ПК-2.1)	тестовый контроль; презентация
Владеть	методами расчета эффективности использования индикаторов информационной безопасности (ПК-2.3); умением выявлять и анализировать угрозы информационной безопасности при осуществлении профессиональной деятельности (ПК-2.2).	экзамен

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оценочные средства	Уровни сформированности компетенции			
	Компетентность несформирована	Базовый уровень компетентности	Достаточный уровень компетентности	Высокий уровень компетентности
тестовый контроль	1-59% правильных ответов	60-74% правильных ответов	75-89% правильных ответов	90-100% правильных ответов
презентация	материал не структурирован, без учета специфики проблемы	материал слабо структурирован, не связан с ранее изученным, не выделены существенные признаки проблемы	материал структурирован, оформлен согласно требованиям, однако есть несущественные недостатки	материал структурирован, оформлен согласно требованиям

экзамен	не раскрыт полностью ни один теор. вопрос, практическое задание не выполнено или выполнено с грубыми ошибками	теоретические вопросы раскрыты с замечаниями, однако логика соблюдена. Практическое задание выполнено, но с замечаниями: намечен ход выполнения, однако не полно раскрыты возможности выполнения	работа выполнена с несущественным и замечаниями	работа выполнена полностью, оформлена по требованиям
---------	---	--	---	--

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

7.3.1. Примерные вопросы для тестового контроля

1. Под информационной безопасностью понимается...

А) 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.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это...

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

- А) целостность
- Б) достоверность
- В) конфиденциальность

5. Доступность – это...

- А) возможность за приемлемое время получить требуемую информационную услугу.
- Б) логическая независимость
- В) нет правильного ответа

6. Целостность – это..

- А) целостность информации
- Б) непротиворечивость информации
- В) защищенность от разрушения

7. 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

8. Для чего создаются информационные системы?

- А) получения определенных информационных услуг
- Б) обработки информации
- В) все ответы правильные

9. Целостность можно подразделить:

- А) статическую
- Б) динамическую
- В) структурную

10. Где применяются средства контроля динамической целостности?

- А) анализе потока финансовых сообщений
- Б) обработке данных
- В) при выявлении кражи, дублирования отдельных сообщений

7.3.2. Примерные темы для составления презентации

1. Основные понятия и определения информационной безопасности.

2. Особенности защиты информации в социально-экономических информационных системах (СЭИС).

3. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах (КЭИС).

4. Правовые меры обеспечения информационной безопасности в социально-экономических информационных системах (СЭИС).

5. Законодательные и нормативные акты Российской Федерации в области защиты информации.

- 6.Использование электронных ключей для организации информационной безопасности в КЭИС.
- 7.Организационно-административные методы защиты, применяемые в социальноэкономических информационных системах.
- 8.Формирование политики безопасности предприятия (организации).
- 9.Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).
- 10.Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.

7.3.3. Вопросы к экзамену

- 1.Введение в информационную безопасность
- 2.Информационная безопасность. Основные понятия.
- 3.Модели информационной безопасности.
- 4.Виды защищаемой информации.
- 5.Правовое обеспечение информационной безопасности.
- 6.Основные нормативно-правовые акты в области информационной безопасности.
- 7.Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.
- 8.Организационное обеспечение информационной безопасности
- 9.Политика безопасности.
- 10.Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
- 11.Технические средства и методы защиты информации
- 12.Рассмотрение примеров методов защиты от промышленного шпионажа и экономической разведки.
- 13.Изучение настроек средств антивирусной защиты информации.
- 14.Создание защищенного канала связи средствами виртуальной частной сети.
- 15.Программно-аппаратные средства и методы обеспечения информационной безопасности
- 16.Основные виды сетевых и компьютерных угроз.
- 17.Средства и методы защиты от сетевых компьютерных угроз.
- 18.Цифровые подписи (Электронные подписи).
- 19.Инфраструктура открытых ключей.
- 20.Методы обеспечения информационной безопасности.
- 21.Криптографические методы защиты информации
- 22.Анализ возможностей методов криптографии, которые могут быть использованы в целях защиты данных.
- 23.Применение криптографических систем шифрования данных.

- 24.Создание зашифрованных файлов и криптоконтейнеров и их расшифрование.
- 25.Использование средств стеганографии.
- 26.Исследование эффективности методов защиты информации в корпоративных вычислительных сетях (Инtranет) и глобальной сети Интернет
- 27.Исследование эффективности методов защиты информации в корпоративных вычислительных сетях (Инtranет).
- 28.Исследование эффективности методов защиты информации в глобальной сети Интернет.
- 29.Основные технологии построения защищенных систем.
- 30.Основные регуляторы в сфере построения защищенных систем обработки информации.
- 31.Организационно-технологические меры защиты целостности информации.
- 32.Целостность данных в АС.
- 33.Защита от угрозы нарушения целостности информации на уровне содержания.
- 34.Место информационной безопасности экономических систем в национальной безопасности страны.
- 35.Информационная безопасность и информационные технологии.
- 36.Средства защиты информации.
- 37.Разработка сетевых аспектов политики безопасности.
- 38.Безопасность программной среды.
- 39.Правила этикета при работе с компьютерной сетью.
- 40.Коррупционные преступления.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

7.4.1. Оценивание тестового контроля

Критерий оценивания	Уровни формирования компетенций		
	Базовый	Достаточный	Высокий
Правильность ответов	не менее 60% тестовых заданий	не менее 73% тестовых заданий	не менее 86% тестовых заданий

7.4.2. Оценивание презентации

Критерий оценивания	Уровни формирования компетенций		
	Базовый	Достаточный	Высокий
Раскрытие темы учебной дисциплины	Тема раскрыта частично: не более 3 замечаний	Тема раскрыта частично: не более 2 замечаний	Тема раскрыта

Подача материала (наличие, достаточность и обоснованность графического оформления: схем, рисунков, диаграмм, фотографий)	Подача материала соответствует указанным параметрам частично, не более 3 замечаний	Подача материала соответствует указанным параметрам частично, не более 2 замечаний	Подача материала полностью соответствует указанным параметрам
Оформление презентации (соответствие дизайна всей презентации поставленной цели; единство стиля включаемых в презентацию рисунков; обоснованное использование анимационных эффектов)	Презентация оформлена с замечаниями по параметру или параметрам: не более 3 замечаний	Презентация оформлена с замечаниями по параметру или параметрам: не более 2 замечаний	Презентация оформлена без замечаний

7.4.3. Оценивание экзамена

Критерий оценивания	Уровни формирования компетенций		
	Базовый	Достаточный	Высокий
Полнота ответа, последовательность и логика изложения	Ответ полный, но есть замечания, не более 3	Ответ полный, последовательный, но есть замечания, не более 2	Ответ полный, последовательный, логичный
Правильность ответа, его соответствие рабочей программе учебной дисциплины	Ответ соответствует рабочей программе учебной дисциплины, но есть замечания, не более 3	Ответ соответствует рабочей программе учебной дисциплины, но есть замечания, не более 2	Ответ соответствует рабочей программе учебной дисциплины
Способность студента аргументировать свой ответ и приводить примеры	Ответ аргументирован, примеры приведены, но есть не более 3 несоответствий	Ответ аргументирован, примеры приведены, но есть не более 2 несоответствий	Ответ аргументирован, примеры приведены
Осознанность излагаемого материала	Материал усвоен и излагается осознанно, но есть не более 3 несоответствий	Материал усвоен и излагается осознанно, но есть не более 2 несоответствий	Материал усвоен и излагается осознанно
Соответствие нормам культуры речи	Речь, в целом, грамотная, соблюдены нормы культуры речи, но есть замечания, не более 4	Речь, в целом, грамотная, соблюдены нормы культуры речи, но есть замечания, не более 2	Речь грамотная, соблюдены нормы культуры речи
Качество ответов на вопросы	Есть замечания к ответам, не более 3	В целом, ответы раскрывают суть вопроса	На все вопросы получены исчерпывающие ответы

7.5. Итоговая рейтинговая оценка текущей и промежуточной аттестации студента по дисциплине

По учебной дисциплине «Информационная безопасность» используется 4-балльная система оценивания, итог оценивания уровня знаний обучающихся предусматривает экзамен. В зачетно-экзаменационную ведомость вносится оценка по четырехбалльной системе. Обучающийся, выполнивший не менее 60 % учебных поручений, предусмотренных учебным планом и РПД, допускается к экзамену. Наличие невыполненных учебных поручений может быть основанием для дополнительных вопросов по дисциплине в ходе промежуточной аттестации. Обучающийся, получивший не менее 3 баллов на экзамене, считается аттестованным.

Шкала оценивания текущей и промежуточной аттестации студента

Уровни формирования компетенции	Оценка по четырехбалльной шкале
	для экзамена
Высокий	отлично
Достаточный	хорошо
Базовый	удовлетворительно
Компетенция не сформирована	неудовлетворительно

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература.

№ п/п	Библиографическое описание	Тип (учебник, учебное пособие, учебно-метод пособие, др.)	Кол-во в библи.
1.	Суворова Г.М. Информационная безопасность: Вузовское образование, 2019 г.	учебное пособие	http://www.iprb-bookshop.ru/86038
2.	Ревнивых А.В. Информационная безопасность в организациях: Новосибирский государственный университет экономики и управления «НИНХ», 2018 г.	учебное пособие	http://www.iprb-bookshop.ru/95200
3.	Басыня Е.А. Сетевая информационная безопасность и анонимизация: Новосибирский государственный технический университет, 2016 г.	учебное пособие	http://www.iprb-bookshop.ru/01510
4.	Басыня Е.А. Системное администрирование и информационная безопасность: Новосибирский государственный технический университет, 2018 г.	учебное пособие	http://www.iprb-bookshop.ru/01423

Дополнительная литература.

№ п/п	Библиографическое описание	Тип (учебник, учебное пособие, учебно-метод пособие, др.)	Кол-во в библи.
1.	Информационная безопасность [Электронный ресурс] : лабораторный практикум. - Пермь: ПГГПУ, 2018. - 87 с.	лабораторный практикум	http://e-lanbook.com/book/129509
2.	Информационная безопасность и вопросы профилактики кибер-экстремизма среди молодежи [Электронный ресурс] : сборник статей. - Москва: ФЛИНТА, 2019. - 161 с.	сборник статей	http://e-lanbook.com/book/125426

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

- 1.Поисковые системы: <http://www.rambler.ru>, <http://yandex.ru>,
- 2.Федеральный образовательный портал www.edu.ru.
- 3.Российская государственная библиотека <http://www.rsl.ru/ru>
- 4.Государственная публичная научно-техническая библиотека России URL: <http://gpntb.ru>.
- 5.Государственное бюджетное учреждение культуры Республики Крым «Крымская республиканская универсальная научная библиотека» <http://franco.crimealib.ru/>
- 6.Педагогическая библиотека <http://www.pedlib.ru/>
- 7.Научная электронная библиотека eLIBRARY.RU (РИНЦ) <http://elibrary.ru/defaultx.asp>

10. Методические указания для обучающихся по освоению дисциплины (модуля)

Общие рекомендации по самостоятельной работе бакалавров

Подготовка современного бакалавра предполагает, что в стенах университета он овладеет методологией самообразования, самовоспитания, самосовершенствования. Это определяет важность активизации его самостоятельной работы.

Самостоятельная работа формирует творческую активность бакалавров, представление о своих научных и социальных возможностях, способность вычленять главное, совершенствует приемы обобщенного мышления, предполагает более глубокую проработку ими отдельных тем, определенных программой.

Основными видами и формами самостоятельной работы студентов по данной дисциплине являются: самоподготовка по отдельным вопросам; работа с базовым конспектом; работа с литературой, чтение дополнительной литературы; подготовка к тестовому контролю; подготовка презентации; подготовка к экзамену.

Важной частью самостоятельной работы является чтение учебной литературы. Основная функция учебников – ориентировать в системе тех знаний, умений и навыков, которые должны быть усвоены по данной дисциплине будущими специалистами. Учебник также служит путеводителем по многочисленным произведениям, ориентируя в именах авторов, специализирующихся на определённых научных направлениях, в названиях их основных трудов. Вторая функция учебника в том, что он очерчивает некий круг обязательных знаний по предмету, не претендуя на глубокое их раскрытие.

Чтение рекомендованной литературы – это та главная часть системы самостоятельной учебы бакалавра, которая обеспечивает подлинное усвоение науки. Читать эту литературу нужно по принципу: «идея, теория, метод в одной, в другой и т.д. книгах».

Во всех случаях рекомендуется рассмотрение теоретических вопросов не менее чем по трем источникам. Изучение проблемы по разным источникам – залог глубокого усвоения науки. Именно этот блок, наряду с выполнением практических заданий является ведущим в структуре самостоятельной работы студентов.

Вниманию бакалавров предлагаются список литературы, вопросы к самостоятельному изучению и вопросы к экзамену.

Для успешного овладения дисциплиной необходимо выполнять следующие требования:

- 1) выполнять все определенные программой виды работ;
- 2) посещать занятия, т.к. весь тематический материал взаимосвязан между собой и, зачастую, самостоятельного теоретического овладения пропущенным материалом недостаточно для качественного его усвоения;
- 3) все рассматриваемые на занятиях вопросы обязательно фиксировать в отдельную тетрадь и сохранять её до окончания обучения в вузе;
- 4) проявлять активность при подготовке и на занятиях, т.к. конечный результат овладения содержанием дисциплины необходим, в первую очередь, самому бакалавру;
- 5) в случаях пропуска занятий по каким-либо причинам обязательно отрабатывать пропущенное преподавателю во время индивидуальных консультаций.

Внеурочная деятельность бакалавра по данной дисциплине предполагает:

- самостоятельный поиск ответов и необходимой информации по предложенным вопросам;
- выполнение практических заданий;

- выработку умений научной организации труда.

Успешная организация времени по усвоению данной дисциплины во многом зависит от наличия у бакалавра умения самоорганизовать себя и своё время для выполнения предложенных домашних заданий. Объём заданий рассчитан максимально на 2-3 часа в неделю. При этом алгоритм подготовки будет следующим:

- 1 этап – поиск в литературе теоретической информации по предложенным преподавателем вопросам;
- 2 этап – осмысление полученной информации, освоение терминов и понятий;
- 3 этап – составление плана ответа на каждый вопрос;
- 4 этап – поиск примеров по данной проблематике.

Работа с базовым конспектом

Программой дисциплины предусмотрено чтение лекций в различных формах их проведения: проблемные лекции с элементами эвристической беседы, информационные лекции, лекции с опорным конспектированием, лекции-визуализации.

На лекциях преподаватель рассматривает вопросы программы курса, составленной в соответствии с государственным образовательным стандартом. Из-за недостаточного количества аудиторных часов некоторые темы не удастся осветить в полном объеме, поэтому преподаватель, по своему усмотрению, некоторые вопросы выносит на самостоятельную работу студентов, рекомендуя ту или иную литературу.

Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям.

Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего обсуждения на практическом занятии. В случае необходимости обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в рабочей программе дисциплины.

Подготовка презентации

Требования к оформлению презентации

Презентация должна содержать не более 15 слайдов, раскрывающих тему доклада.

Первый слайд – титульный, на котором должны быть представлены: название темы доклада; фамилия, имя, отчество, учебная группа авторов доклада и год создания.

В оформлении презентаций должны быть соблюдены дизайн-эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, читаемость текстов (начертание, цвет, размер шрифтов) и другие требования, приведенные ниже.

Представление информации

Содержание информации: Используйте короткие слова и предложения. Минимизируйте количество предлогов, наречий, прилагательных. Заголовки должны привлекать внимание аудитории

Расположение информации на странице: Предпочтительно горизонтальное расположение информации. Наиболее важная информация должна располагаться в центре экрана. Если на слайде имеется графическое изображение, подпись должна располагаться под ним

Шрифты: Шрифты: Кегль для заголовков – не менее 24, для информации – не менее 22. Шрифты без засечек и строчные буквы читаются с большого расстояния легче, чем шрифты с засечками и прописные буквы.

Не рекомендуется смешивать разные типы шрифтов в одной презентации. Для выделения информации используют различные начертания: жирный, курсив

Способы выделения информации: Способы выделения наиболее важных фактов: рамки; границы, заливка; штриховка, стрелки; рисунки, диаграммы,

Объем информации: При определении объема необходимо учитывать, что человеку трудно одновременно запомнить более трех фактов, выводов, определений.

Наибольшая эффективность презентации достигается, когда ключевые пункты отображаются по одному на каждом отдельном слайде или выводятся на слайд поэтапно

Виды слайдов: Для обеспечения разнообразия следует использовать разные виды слайдов: с текстом; с таблицами; с диаграммами.

Оформление слайдов.

Стиль: Соблюдайте единый стиль оформления, не отвлекающий от самой презентации. Вспомогательная информация (управляющие кнопки) не должны преобладать над основной информацией (текстом, иллюстрациями)

Фон: Для фона предпочтительны холодные тона

Использование цвета: На одном слайде рекомендуется использовать не более трех цветов: один для фона, один для заголовка, один для текста. Для фона и текста используйте контрастные цвета.

Анимационные эффекты: Используйте возможности компьютерной анимации для представления информации на слайде. Не стоит злоупотреблять различными анимационными эффектами, они не должны отвлекать внимание от содержания информации на слайде

Подготовка к тестовому контролю

Основное достоинство тестовой формы контроля – это простота и скорость, с которой осуществляется первая оценка уровня обученности по конкретной теме, позволяющая, к тому же, реально оценить готовность к итоговому контролю в иных формах и, в случае необходимости, откорректировать те или иные элементы темы.

Подготовка к тестированию

1. Уточните объем материала (отдельная тема, ряд тем, раздел курса, объем всего курса), по которому проводится тестирование.
2. Прочтите материалы лекций, учебных пособий.
3. Обратите внимание на характер заданий, предлагаемых на практических занятиях.
4. Составьте логическую картину материала, выносимого на тестирование (для продуктивной работы по подготовке к тестированию необходимо представлять весь подготовленный материал как систему, понимать закономерности, взаимосвязи в рамках этой системы).

Подготовка к экзамену

Экзамен является традиционной формой проверки знаний, умений, компетенций, сформированных у студентов в процессе освоения всего содержания изучаемой дисциплины. В случае проведения экзамена студент получает баллы, отражающие уровень его знаний.

Правила подготовки к экзаменам:

- Лучше сразу сориентироваться во всем материале и обязательно расположить весь материал согласно экзаменационным вопросам.
- Сама подготовка связана не только с «запоминанием». Подготовка также предполагает и переосмысление материала, и даже рассмотрение альтернативных идей.
- Сначала студент должен продемонстрировать, что он «усвоил» все, что требуется по программе обучения (или по программе данного преподавателя), и лишь после этого он вправе высказать иные, желательно аргументированные точки зрения.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (включая перечень программного обеспечения и информационных справочных систем (при необходимости))

Информационные технологии применяются в следующих направлениях:
оформление письменных работ выполняется с использованием текстового редактора;

демонстрация компьютерных материалов с использованием мультимедийных технологий;

использование информационно-справочного обеспечения, такого как: правовые справочные системы (Консультант+ и др.), онлайн словари, справочники (Грамота.ру, Интуит.ру, Википедия и др.), научные публикации.

использование специализированных справочных систем (электронных учебников, справочников, коллекций иллюстраций и фотоизображений, фотобанков, профессиональных социальных сетей и др.).

OpenOffice Ссылка: <http://www.openoffice.org/ru/>

Mozilla Firefox Ссылка: <https://www.mozilla.org/ru/firefox/new/>

Libre Office Ссылка: <https://ru.libreoffice.org/>

Do PDF Ссылка: <http://www.dopdf.com/ru/>

7-zip Ссылка: <https://www.7-zip.org/>

Free Commander Ссылка: <https://freecommander.com/ru>

be Reader Ссылка: <https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html>попо

Gimp (графический редактор) Ссылка: <https://www.gimp.org/>

ImageMagick (графический редактор) Ссылка: <https://imagemagick.org/script/index.php>

VirtualBox Ссылка: <https://www.virtualbox.org/>

Adobe Reader Ссылка: <https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html>

Операционная система Windows 8.1 Лицензионная версия по договору №471\1 от 11.12.2014 г.

Электронно-библиотечная система Библиокомплектатор

Национальна электронная библиотека - федеральное государственное бюджетное учреждение «Российская государственная библиотека» (ФГБУ «РГБ»)

Редакция Базы данных «ПОЛПРЕД Справочники»

Электронно-библиотечная система «ЛАНЬ»

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

-учебная аудитория с видеопроекторным оборудованием и экраном для демонстрации презентаций в ходе проведения лекционных и практических занятий, а также учебная аудитория с компьютерами с выходом в сеть Интернет (для самостоятельной работы обучающихся).