Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Задорожная Людмила Ивановна
Должность: Проректор по учебной работе
Дата подписания: 03.10.2023 10:17:08
Уникальный программный ключ:
faa404d1aeb2a023b5f4a331ee5ddc540496512d

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Майкопский государственный технологический университет»

Факультет информационных систем в экономике и юриспруденции

Кафедра Информационной безопасности и прикладной информатики

УТВЕРЖДАЮ
Проректор по учебной работе
_____Л.И. Задорожная
«_____» _____ 20___г.

РАБОЧАЯ ПРОГРАММА

по дисциплине	**Б1.О.22 Основы информационной безопасности**
по направлению подготовки	10.03.01 Информационная безопасность
по профилю подготовки (специализации)	Организация и технология защиты информации
квалификация (степень) выпускника	Бакалавр
форма обучения	Очная,
год начала подготовки	2023

Майкоп

Рабочая программа составлена на основе ФГОС ВО и учебного плана МГТУ по направлению подготовки (специальности) 10.03.01 Информационная безопасность

Составитель рабочей программы:

старший преподаватель кафедры информационной безопасности и прикладной информатики,	Подписано простой ЭП 19.09.2023	Брикова Ирина Викторовна
(должность, ученое звание, степень)	(подпись)	(Ф.И.О.)

Рабочая программа утверждена на заседании кафедры:

Информационной безопасности и прикладной информатики
(название кафедры)

Заведующий кафедрой:

22.09.2023	Подписано простой ЭП 22.09.2023	Чундышко Вячеслав Юрьевич
	(подпись)	(Ф.И.О.)

Согласовано:

Руководитель ОПОП
заведующий выпускающей кафедрой
по направлению подготовки (специальности)

22.09.2023	Подписано простой ЭП 22.09.2023	Чундышко Вячеслав Юрьевич
	(подпись)	(Ф.И.О.)

Согласовано:

НБ МГТУ
(название подразделения)

22.09.2023	Подписано простой ЭП 22.09.2023	И. Б. Берберьян
	(подпись)	(Ф.И.О.)

1. Цели и задачи учебной дисциплины (модуля)

Цель курса «Основы информационной безопасности» - изучение вопросов теории и практики обеспечения информационной безопасности личности, общества и государства; основных общеметодологических принципов теории информационной безопасности; методов нарушения конфиденциальности, целостности и доступности информации; методов и средств обеспечения информационной безопасности, а также проблем безопасности автоматизированных систем, включая вопросы определения модели нарушителя и требований к защите информации.

Для реализации поставленной цели необходимо решить следующие **задачи:**

- формирование терминологического фундамента;

- изучение основ теории информационной безопасности;

- изучение методов и средств обеспечения информационной безопасности;

- обучение определению причин, видов, источников и каналов утечки, искажения информации;

- ознакомление с основными нормативными документами.

2. Место дисциплины (модуля) в структуре ОП по направлению подготовки (специальности)

«Основы информационной безопасности» является учебным курсом, входящим в обязательный перечень базовой части.

Дисциплина основана на знаниях научных основ и закономерностей развития общества.

Дисциплина направлена на получение базовых знаний по вопросам обеспечения информационной безопасности, определение основных направлений развития этой предметной области.

Текущая аттестация осуществляется в форме контроля СР и контрольных работ. Промежуточная оценка успеваемости выставляется по результатам сдачи экзамена и учитывает оценки, получаемые обучающимися во время текущей аттестации.



3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Процесс изучения дисциплины направлен на формирование следующей(их) компетенции(й):

ОПК-1.1	Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации
ОПК-1.2	Умеет классифицировать и оценивать угрозы информационной безопасности
ОПК-1.3	Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире
ОПК-9.1	Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
ПК-5.1	Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
ПК-5.2	Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации
ПК-5.3	Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации

4. Объем дисциплины (модуля) и виды учебной работы. Общая трудоемкость дисциплины

Объем дисциплины и виды учебной работы по очной форме обучения.

		Формы контроля (количество)	Виды занятий					Итого часов	з.е.
		Эк	Лек	Пр	КРАт	Контроль	СР		
Курс 1	Сем. 2	1	34	17	0.35	26.65	66	**144**	4

5. Структура и содержание учебной и воспитательной деятельности при реализации дисциплины

5.1. Структура дисциплины для очной формы обучения.

Сем	Раздел дисциплины	Неделя семестра	Виды учебной работы, включая самостоятельную работу и трудоемкость (в часах)								Формы текущего/промежуточной контроля успеваемости текущего (по неделям семестра), промежуточной аттестации (по семестрам)
			Лек	Лаб	ПР	СРП	КРАт	Контроль	СР	СЗ	
1	2	3	4	5	6	7	8	9	10	11	12
2	Введение. Исторические аспекты возникновения и развития информационной безопасности	1	2								Блиц-опрос
2	Основные понятия и определения сферы информацион-ной безопасности	2	2					2	4		Блиц-опрос
2	Базовые принципы информационной безопасности	3	2					2	4		Блиц-опрос
2	Информация - наиболее ценный ресурс современного общества	4	2		2			2	6		Тестирование
2	Проблемы информационной войны	5	2		2			2	6		Обсуждение рефератов
2	Организационно-правовое обеспече-ние информацион-ной безопасности	6	2		2			2	6		Обсуждение рефератов
2	Информационные системы. Общие положения. Информация как продукт. Информационные услуги	7	2					2	4		Блиц-опрос
2	Угрозы информации	8-9	4		2			2	6		Обсуждение рефератов
2	Методы и модели оценки уязвимости информации	10	2					2	4		Блиц-опрос
2	Методы определения требований к защите информации	11-12	4					2	4		Блиц-опрос
2	Анализ существующих методик определения требований к защите информации	13	2		2			2	6		Обсуждение рефератов
2	Функции и задачи защиты информации. Стратегии защиты информации	14-15	4		2			2	6		Тестирование
2	Способы и средства защиты информации	16	2		2			2	4		Блиц-опрос
2	Информационная безопасность в условиях функционирования глобальных сетей.	17	2		3		0.35	2.65	6		Обсуждение рефератов
	ИТОГО:		**34**		**17**		**0.35**	**26.65**	**66**		

5.4. Содержание разделов дисциплины (модуля) «Основы информационной безопасности», образовательные технологии

Лекционный курс

Сем	Наименование темы дисциплины	Трудоемкость (часы)			Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
		ОФО	ЗФО	ОЗФО				
1	2	3	4	5	6	7	8	9
2	Введение. Исторические аспекты возникновения и развития информационной безопасности	2			Цели, задачи, предмет, содержание и задачи курса. Место курса среди других дисциплин. Структура курса. Понятие информационной безопасности. Этапы развития средств информационных коммуникаций.	ОПК-1.1;	Знать: Уметь: Владеть:	, Лекция-беседа
2	Основные понятия и определения сферы информационной безопасности	2			Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Информационная безопасность и защита информации. Информация. Показатели информации: важность, пол-нота, адекватность, релевантность, толерантность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Информационная сфера.	ОПК-1.1;	Знать: Уметь: Владеть:|/textarea|	

, Лекция-беседа

2	Базовые принципы информационной безопасности	2			Влияние информатизации общества на составляющие информационной безопасности. Основные принципы построения системы	ОПК-1.1;	Знать: Уметь: Владеть:|/textarea|	

					информационной безопасности. Требования к системе защиты информации. Этапы формирования системы защиты информации. Комплексность защиты информации: целевая, инструментальная, структурная, функциональная, временная.				

, Лекция-беседа,

2		2			Информационное	ОПК-1.1;	Знать: Уметь:	
		2				ОПК-5.2; ПК-5.1;	Владеть:
		4				ПК-5.2; ПК-5.3;	Владеть:
		34							

5.5. Практические занятия, их наименование, содержание и объем в часах

Сем	№ раздела дисциплины	Наименование практических занятий	Объем в часах		
			ОФО	ЗФО	ОЗФО
1	2	3	4	5	6
2	Информация - наиболее ценный ресурс современного общества	Анализ информации на предмет целостности. Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации	2		
2	Проблемы информационной войны	Выявление признаков информационной войны в СМИ и сети Интернет	2		
2	Организационно-правовое обеспечение информационной безопасности	Анализ системы организационно-правовой защиты информации, составляющей государственную и коммерческую тайну.Назначение, структура и содержание Политики ИБ.Требования, предъявляемые к Политике первого уровняСвязь основных понятий информационной безопасности	2		
2	Угрозы информации	Ознакомление с алгоритмами оценки риска информационной безопасности. Вирусы. Классификация вирусов	2		
2	Анализ существующих методик определения требований к защите информации	Особенности международной защиты банковской тайны. Международная си-стема охраны интеллектуальной собственности.	2		
2	Функции и задачи защиты информации. Стратегии защиты информации	Защита информации в автоматизированных системах: особенности парольной защиты, антивирусная защита, аппаратная защита. Управление рисками информационной безопасности	2		
2	Способы и средства защиты информации	Классификации методов и средств защиты информации от утечки по техническим каналам. Функционирование программного обеспечения для информационной безопасности. Классификация программ по защите информации.	2		
2	Информационная безопасность в условиях функционирования глобальных сетей.	Сетевое сканирование. Анализ работы межсетевых экранов.	3		
	ИТОГО:		**17**		

Симуляционные занятия, их наименование, содержание и объем в часах

Учебным планом не предусмотрено

5.6. Лабораторные занятия, их наименование и объем в часах

Учебным планом не предусмотрено

5.7. Примерная тематика курсовых проектов (работ)

Учебным планом не предусмотрено

5.8. Самостоятельная работа студентов

Содержание и объем самостоятельной работы студентов

Сем	Разделы и темы рабочей программы самостоятельного изучения	Перечень домашних заданий и других вопросов для самостоятельного изучения	Сроки выполнения	Объем в часах		
				ОФО	ЗФО	ОЗФО
1	2	3	4	5	6	7
2	Основные понятия и определения сферы bнформационной безопасности	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки	2 неделя	4		
2	Базовые принципы информационной безопасности	Подбор, обобщение и ана-лиз информации из литературных источников и других информационных ресурсов по профилю подготовки	3 неделя	4		
2	Информация - наиболее ценный ресурс современного общества	Составление плана-конспекта	4 неделя	6		
2	Проблемы информационной войны	Написание реферата	5 неделя	6		
2	Организационно-правовое обеспечение, информационной безопасности	Написание реферата	6 неделя	6		
2	Информационные системы. Общие положения. Информация как продукт. Информационные услуги	Составление плана-конспекта	7 неделя	4		
2	Угрозы информации	Написание реферата	8-9 недели	6		
2	Методы и модели оценки уязвимости информации	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки	10 неделя	4		
2	Методы определения требований к защите информации	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки	11-12 недели	4		
2	Анализ существующих методик определения требований к защите информации	Написание реферата	13 неделя	6		
2	Функции и задачи защиты информации	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки	14-15 недели	6		
2	Способы и средства защиты информации	Составление плана-конспекта	16 неделя	4		
2	Информационная безопасность в условиях функционирования глобальных сетей.	Написание реферата	17 неделя	6		
	ИТОГО:			**66**		

5.9. Календарный график воспитательной работы по дисциплине

Модуль	Дата, место проведения	Название мероприятия	Форма проведения мероприятия	Ответственный	Достижения обучающихся
Модуль 3 Учебно-исследовательская и	29.02.2024 ФГБОУ ВО "МГТУ"	Как распознавать фейки, чтобы не остаться	Слайд-лекция	Брикова И.В.	ОПК-1.3;

Модуль	Дата, место проведения	Название мероприятия	Форма проведения мероприятия	Ответственный	Достижения обучающихся
научно-исследовательская деятельность		одураченным?			

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

6.1. Методические указания (собственные разработки)

Название	Ссылка
Основы сайтостроения : учебное пособие / М-во науки и высш. образования РФ, ФГБОУ ВО Майкоп. гос. технол. ун-т, Фак. информац. систем в экономике и юриспруденции, Каф. информац. безопасности и приклад. информатики ; составители: Меретукова С.К., Чундышко В.Ю., Меретуков Ш.Т., Козлова Н.Ш. - 2-е изд., перераб. - Майкоп : МГТУ, 2021. - 148 с. - Библиогр.: с. 146-147 (16 назв.). - ISBN 978-5-88941-157-4	http://lib.mkgtu.ru:8002/libdata.php?id=00061821&DOK=0BAA5B&BASE=000530
Довгаль, В.А. (Майкопский государственный технологический университет). Системы защиты информации в ведущих зарубежных странах : учеб. пособие / В.А. Довгаль ; М-во образования и науки РФ, ГОУ ВПО Майкоп. гос. технол. ун-т. - Майкоп : МГТУ, 2010. - 112 с.	http://lib.mkgtu.ru:8002/libdata.php?id=2000014830&DOK=021165&BASE=000530

6.2. Литература для самостоятельной работ

Название	Ссылка
Башлы, П.Н. Информационная безопасность и защита информации : учебник / П.Н. Баш лы, А.В. Бабаш, Е.К. Баранова. - Москва : РИОР, 2013. - 222 с. - ЭБС Знаниум. - URL: http://znanium.com/catalog/document?id=213488. - Режим доступа: по подписке	http://znanium.com/catalog/document?id=213488
Зенков, А.В. Информационная безопасность и защита информации : учебное пособие / А.В. Зенков. - 2-е изд.,пер. и доп. - Москва : Юрайт, 2023. - 107 с. - (Высшее образование). - ЭБС Знаниум. - URL: https://urait.ru/bcode/530927. - Режим доступа: по подписке. - ISBN 978-5-534-16388-9	https://urait.ru/bcode/530927
Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. - 4-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2022. - 336 с. - (Высшее образование). - ЭБС Знаниум. - URL: https://znanium.com/catalog/document?id=393765. - Режим доступа: по подписке. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7	https://znanium.com/catalog/document?id=393765
Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3 изд. - Москва : РИОР : ИНФРА-М, 2019. - 400 с. - (Высшее образование). - ЭБС Знаниум. - URL: http://znanium.com/catalog/document?id=339378. - Режим доступа: по подписке. - ISBN 978-5-369-01759-3. - ISBN 978-5-16-106478-8. - ISBN 978-5-16-013801-5	http://znanium.com/catalog/document?id=339378
Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. - Саратов : Ай Пи Эр Медиа, 2019. - 227 с. - ЭБС IPR Books. - URL: http://www.iprbookshop.ru/80290.html. - Режим доступа: по подписке. - ISBN 978-5-4486-0485-0	http://www.iprbookshop.ru/80290.html
Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. - 4-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2021. - 336 с. - (Высшее образование). - ЭБС Знаниум. - URL: http://znanium.com/catalog/document?id=364911. - Режим доступа: по подписке. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7	http://znanium.com/catalog/document?id=364911
Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. - Москва : ИНФРА-М, 2023. - 201 с. - (Высшее образование: Магистратура). - ЭБС Знаниум. - URL: https://znanium.com/catalog/document?id=420080. - Режим доступа: по подписке. - ISBN 978-5-16-014976-9. - ISBN 978-5-16-107471-8	https://znanium.com/catalog/document?id=420080
Суворова, Г.М. Информационная безопасность : учебное	https://urait.ru/bcode/531084

Название	Ссылка
пособие / Г.М. Суворова. - 2-е изд.,пер. и доп. - Москва : Юрайт, 2023. - 277 с. - (Высшее образование). - ЭБС Юрайт. - URL: https://urait.ru/bcode/531084. - Режим доступа: по подписке. - ISBN 978-5-534-16450-3	
Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3 изд. - Москва : РИОР : ИНФРА-М, 2021. - 400 с. - (Высшее образование). - ЭБС Знаниум. - URL: http://znanium.com/catalog/document?id=367588. - Режим доступа: по подписке. - ISBN 978-5-369-01759-3. - ISBN 978-5-16-106478-8. - ISBN 978-5-16-013801-5	http://znanium.com/catalog/document?id=367588
Глотина, И.М. Средства безопасности операционной системы Windows Server 2008 : учебно-методическое пособие / И.М. Глотина. - Саратов : Вузовское образование, 2018. - 141 c. - ЭБС IPR Books. - URL: http://www.iprbookshop.ru/72538.html. - Режим доступа: по подписке. - ISBN 978-5-4487-0136-8	http://www.iprbookshop.ru/72538.html
Галатенко, В.А. Основы информационной безопасности : учебное пособие / В.А. Галатенко. - Москва : Интернет-Университет Информационных Технологий, 2020. - 266 с. - ЭБС IPR Books. - URL: http://www.iprbookshop.ru/97562.html. - Режим доступа: по подписке. - ISBN 978-5-4497-0675-1	http://www.iprbookshop.ru/97562.html

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.



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

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	**ЗФО**	**ОЗФО**	
ОПК-1.1 Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации			
7			Гуманитарные аспекты информационной безопасности
2			Основы информационной безопасности
ОПК-1.2 Умеет классифицировать и оценивать угрозы информационной безопасности			
7			Гуманитарные аспекты информационной безопасности
2			Основы информационной безопасности
ОПК-1.3 Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире			
7			Гуманитарные аспекты информационной безопасности
2			Основы информационной безопасности
ОПК-9.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации			
6			Сети и системы передачи информации
2			Основы информационной безопасности
5			Организационное и правовое обеспечение информационной безопасности
6			Защита информации от утечки по техническим каналам
7			Методы и средства криптографической защиты информации
5			Техническая защита информации
6			Моделирование процессов и систем защиты информации
7			Нормативные акты и стандарты по информационной безопасности
67			Научно-исследовательская работа по организации и технологии защиты информации
ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации			
2			Основы информационной безопасности
5			Организационное и правовое обеспечение информационной безопасности
7			Основы управления информационной

Этапы формирования компетенции (номер семестр согласного учебному плану)			Наименование учебных дисциплин, формирующие компетенции в процессе освоения образовательной программы
ОФО	ЗФО	ОЗФО	
			безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
7			Нормативные акты и стандарты по информационной безопасности
ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации			
2			Основы информационной безопасности
5			Организационное и правовое обеспечение информационной безопасности
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
7			Нормативные акты и стандарты по информационной безопасности
ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации			
2			Основы информационной безопасности
5			Организационное и правовое обеспечение информационной безопасности
7			Основы управления информационной безопасностью
8			Комплексное обеспечение защиты информации объекта информатизации
7			Нормативные акты и стандарты по информационной безопасности

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

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;					
ОПК-9.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: задания для контрольной работы, тестовые

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	задания, темы рефератов, докладов, вопросы к экзамену.
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: задания для контрольной работы, тестовые задания, темы рефератов, докладов, вопросы к экзамену.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: задания для контрольной работы, тестовые задания, темы рефератов, докладов, вопросы к экзамену.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-5: Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации					
ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: задания для контрольной работы, тестовые задания, темы рефератов, докладов, вопросы к экзамену.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-1: Способен решать задачи профессиональной деятельности на основе использования теоретических и практических основ естественных и технических наук, а также математического аппарата					
ОПК-1.1 Знает понятия информации и информационной безопасности, место и роль информационной безопасности					

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
1	2	3	4	5	6
в системе национальной безопасности Российской Федерации					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: задания для контрольной работы, тестовые задания, темы рефератов, докладов, вопросы к экзамену.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-1: Способен решать задачи профессиональной деятельности на основе использования теоретических и практических основ естественных и технических наук, а также математического аппарата					
ОПК-1.2 Умеет классифицировать и оценивать угрозы информационной безопасности					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: задания для контрольной работы, тестовые задания, темы рефератов, докладов, вопросы к экзамену.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-1: Способен решать задачи профессиональной деятельности на основе использования теоретических и практических основ естественных и технических наук, а также математического аппарата					
ОПК-1.3 Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире					
Знать:	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контролирующие материалы по дисциплине, в числе которых могут быть: задания для контрольной работы, тестовые задания, темы рефератов, докладов, вопросы к экзамену.
Уметь:	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть:	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

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

Тестовые задания для текущего контроля знаний по дисциплине

1 вариант

1. С какой точки зрения сообщение представляет интерес как объект передачи по техническим каналам связи?

а) с технической;

б) с семантической;

в) с прагматической.

2. Какие два основных элемента включает понятие «информация»?

а) сведения и сообщения;

б) сведения и данные;

в) сообщения и данные.

3. К каким угрозам относится нарушение законных ограничений на распространение информации?

а) угрозам конституционным правам человека в области информационной деятельности;

б) угрозам информационному обеспечению государственной политики РФ;

в) угрозам безопасности информационных и телекоммуникационных средств и систем.

4. К каким угрозам относится блокирование деятельности государственных СМИ по информированию российской и зарубежной аудитории?

а) к угрозам конституционным правам человека в области информационной деятельности;

б) к угрозам информационному обеспечению государственной политики РФ;

в) к угрозам безопасности информационных и телекоммуникационных средств и систем.

5. К каким угрозам относится манипулирование информацией?

а) к угрозам конституционным правам человека в области информационной деятельности;

б) к угрозам информационному обеспечению государственной политики РФ;

в) к угрозам безопасности информационных и телекоммуникационных средств и систем.

6. Как называется вся накопленная информация об окружающей действительности, зафиксированная на любом материальном носителе?

а) база знаний;

б) база данных;

в) информационные ресурсы.

7. Структурная комплексность защиты информации предполагает:

а) интеграцию всех видов и направлений ИБ для достижения поставленных целей;

б) обеспечение требуемого уровня защиты во всех элементах системы обработки информации;

в) что методы защиты должны быть направлены на все выполняемые функции системы

обработки информации.

8. Что является материальной основой работы информационной системы?

а) информация;

б) информационные ресурсы;

в) информационные процессы.

9. Как называются сведения, на использование и распространение которых введены ограничения их собственником и характеризуемые понятием «тайна»?

а) защищаемая информация;

б) запатентованная информация;

в) ценная информация.

10. Свойство данных, состоящее в том, что время их сбора и переработки соответствует динамике изменения ситуации – это:

а) достоверность информации;

б) актуальность информации;

в) оперативность информации.

11. Свойство данных не подвергаться моральному старению – это:

а) кумулятивность информации;

б) актуальность информации;

в) значимость информации.

12. Служба информационной системы по запросу - это:

а) служба, обеспечивающая пользователю возможность извлекать необходимую информацию из банков данных;

б) служба, обеспечивающая непрямую связь между пользователями с применением средств промежуточного хранения;

в) служба, обеспечивающая прямую передачу информации в реальном масштабе времени.

2 вариант

1. С какой точки зрения сообщение представляет интерес как средство передачи сведений?

а) с технической;

б) с семантической;

в) с прагматической.

2. Состояние защищенности национальных интересов РФ в информационной сфере – это:

а) национальные интересы РФ;

б) информационная безопасность РФ;

в) национальная безопасность РФ.

3. К каким угрозам относится нерациональное, чрезмерное ограничение доступа к общественно необходимой информации?

а) угрозам конституционным правам человека в области информационной деятельности;

б) угрозам информационному обеспечению государственной политики РФ;

в) угрозам безопасности информационных и телекоммуникационных средств и систем.

4. К каким угрозам относится компрометация ключей и средств криптографической защиты информации?

а) к угрозам конституционным правам человека в области информационной деятельности;

б) к угрозам информационному обеспечению государственной политики РФ;

в) к угрозам безопасности информационных и телекоммуникационных средств и систем.

5. К каким угрозам относится противоправный сбор и использование информации?

а) к угрозам конституционным правам человека в области информационной деятельности;

б) к угрозам информационному обеспечению государственной политики РФ;

в) к угрозам безопасности информационных и телекоммуникационных средств и систем.

6. Функциональная комплексность защиты информации предполагает:

а) интеграцию всех видов и направлений ИБ для достижения поставленных целей;

б) обеспечение требуемого уровня защиты во всех элементах системы обработки информации;

в) что методы защиты должны быть направлены на все выполняемые функции системы обработки информации.

7. Что является функциональной основой работы информационной системы?

а) информация;

б) информационные ресурсы;

в) информационные процессы.

8. Свойство данных соответствовать состоянию объекта – это:

а) достоверность информации;

б) идентичность информации;

в) актуальность информации.

9. Сведения, содержащие государственную тайну, относятся к:

а) конфиденциальной информации;

б) ценной информации;

в) секретной информации.

10. Служба информационной системы – это:

а) совокупность действий, реализующих обеспечение доступа к информационным ресурсам системы;

б) совокупность действий и компонентов информационной системы, обеспечивающих соответствующие услуги;

в) совокупность средств для прямой передачи информации в реальном масштабе времени.

11. Как называется получение лицами в обход системы защиты с помощью программных, технических и др. средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации?

а) разглашение информации;

б) утечка информации;

в) НСД к информации.

12. Как называется главное средство закрепления информации различным способом на специальном носителе?

а) база знаний;

б) база данных;

в) документ.

Тестовые задания для контроля остаточных знаний по дисциплине

1. С какой точки зрения сообщение представляет интерес как средство воздействия на информационную модель человека?

а) с технической;

б) с семантической;



в) с прагматической.

2. Как называется возможная опасность?

а) угрозой;

б) НСД;

в) попыткой искажения информации.

3. К каким угрозам относится утечка информации по техническим каналам?

а) угрозам конституционным правам человека в области информационной деятельности;

б) угрозам информационному обеспечению государственной политики РФ;

в) угрозам безопасности информационных и телекоммуникационных средств и систем.

4. К каким угрозам относится нарушение конституционных прав и свобод человека в области массовой информации?

а) к угрозам конституционным правам человека в области информационной деятельности;

б) к угрозам информационному обеспечению государственной политики РФ;

в) к угрозам безопасности информационных и телекоммуникационных средств и систем.

5. К каким угрозам относится нарушение технологии обработки информации?

а) к угрозам конституционным правам человека в области информационной деятельности;

б) к угрозам информационному обеспечению государственной политики РФ;

в) к угрозам безопасности информационных и телекоммуникационных средств и систем.

6. Что является компонентами информатизации?

а) информация и информационные ресурсы;

б) информационные ресурсы и информационные системы;

в) информационные системы и информация.

7. Свойство данных не иметь скрытых случайных ошибок - это

а) достоверность информации;

б) кумулятивность информации;

в) актуальность информации.

8. Сведения, содержащие коммерческую тайну, относятся к:



а) секретной информации;

б) конфиденциальной информации;

в) персональным данным.

9. Свойство данных соответствовать срокам, определяемым социальными мотивами – это:

а) оперативность информации;

б) срочность информации;

в) кумулятивность информации.

10. Диалоговая служба информационной системы – это:

а) служба, обеспечивающая распределение сообщений от одного центрального источника к неограниченному числу абонентов;

б) служба, обеспечивающая непрямую связь между пользователями с применением средств промежуточного хранения сообщений;

в) служба, предоставляющая средства для прямой связи передачи информации в реальном масштабе времени.

11. Как называется умышленное или неосторожное действие должностных лиц и граждан, приведшее к оглашению охраняемых данных, а также передача таких данных по открытым техническим каналам?

а) разглашение информации;

б) утечка информации;

в) НСД к информации.

12. Как называются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления?

а) информация;

б) документ;

в) информационные ресурсы.

Темы рефератов

1. Информационная безопасность профессиональной деятельности организации.
2. Организационно-правовое обеспечение информационной безопасности бизнеса.
3. Защита информации предприятия от утечки по техническим каналам.
4. Организация информационной безопасности в коммерческом секторе. Организация системы безопасности корпоративных информационных систем.
5. Инженерно-техническая безопасность предприятия. Международно-правовые аспекты



информационной безопасности.

6. Информационная собственность и ее защита.

7. Информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения и механизмов информационной безопасности.

8. Классификация возможных угроз безопасности.

9. Существующие способы устранения угроз.

10. Компьютерные преступления, правоустанавливающие акты, взаимоотношения предприятия и правоохранительных органов.

Основные технологии построения защищенных информационных систем. Основные классификационные признаки компьютерных вирусов. Методы и технологии борьбы с компьютерными вирусами. Условия безопасной работы КС и технология обнаружения заражения вирусами. Криптографическая защита информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

Темы докладов

1. Методы защиты корпоративной информации.

2. Основные направления обеспечения безопасности коммерческого предприятия.

3. Защита персональных данных на предприятии.

4. Аудит информационной безопасности.

5. Роль информационной безопасности в сфере электронной торговли

6. Комплексный подход к созданию системы защиты информации на предприятии.

7. Угрозы информационной безопасности в таможенном секторе.

8. Международная информационная безопасность.

9. Выявление рисков нарушения информационной безопасности предприятия.

10. Защита информационной среды на предприятии.

11. Обеспечение безопасного доступа к информационным ресурсам организации.

12. Экономика информационной безопасности предприятия.

13. Комплексная информационная безопасность объекта.

14. Информационная безопасность организации и персонал.

15. Правовой статус и функции службы безопасности по обеспечению информационной безопасности бизнеса.

Кейс по дисциплине: «Основы информационной безопасности»

Связь основных понятий информационной безопасности

У менеджера компании «Аскона» есть личный электронный ящик, также что он

пользуется социальными сетями (В Кконтакте, Одноклассники и т.д). При этом он закрывает браузер не нажимая кнопку «выход», использует Internet Explorer, имеет 1-2 несложных пароля на все ресурсы, выходит в сеть в основном с рабочего места иногда из дома. Менеджер – коммуникабельная, активная девушка, участница форумов. На сайтах регистрируется под ником ***

Студенты делятся на 2 группы: «Защитники» (Админы) и «Злоумышленники» (Хакеры),

Каждая команда сообразно своим интересам определяет для менеджера:

· риски по аспектам информационной безопасности: целостность, доступность, конфидециальность;

· уязвимости;

· угрозы;

· уровень неприемлемого ущерба;

· контрмеры - политику безопасности (для защитников);

· порядок атак (для злоумышленников).

После обсуждения, студентам сообщается имя девушки и её ник (он виртуальный). Студенты выходят в Интернет, и кто первый успеет (найти почту, поменять пароли, сменить данные, чтоб не нашли другие и пр), тот и победил.

Компьютерная неграмотность персонала

В понедельник утром в фирму «Лимпид Пулс» поступил звонок от провайдера. Фирме отключили доступ к сети, потому что с адреса компьютера секретаря с 18.00 до 22.00 была совершена рассылка 2000 писем.

Секретарь фирмы – Евгения, имеет несложный пароль, состоящий из цифр, по совету системного администратора часто меняет его, но не придумывая новый, а переставляю цифры в старом, для запоминания клеит стикеры с паролем на монитор

Какие ошибки в информационном поведении сотрудницы. Как действовать в данной ситуации. Как избежать подобных ситуаций позднее?

Человеческий фактор информационной безопасности

Весьма опасны так называемые обиженные сотрудники – нынешние и бывшие.

В рекламном агентстве возник конфликт у коммерческого директора И.П. Дрога и работника технического отдела А.В. Кац. Верхолазов занимался информационной безопасностью фирмы, имел доступ почти ко всем ресурсам, базам данных, знал все пороли, знаком с порядками в организации. Известно, что Верхолазов замкнут и обидчив. Чем опасен обиженный сотрудник? Как обезопасить фирму от преднамеренного вредительства уволенного сотрудника?

Связь основных понятий информационной безопасности

В издательство «Буква» поступил звонок от провайдера. Предприятию отключили доступ к сети, потому что была зарегистрирована рассылка спама. Пришли большие счета, при сравнительно малом использовании ресурсов сети. В результате отключения Интернета были просрочены заказы, нарушена связь с несколькими клиентами,

Оказалось, что менеджеры имеют несложный пароль, в основном даты рождения. У некоторых на мониторе приклеен стикер с паролем.

Какие ошибки в информационном поведении сотрудников. Как действовать в данной ситуации. Как избежать подобных ситуаций позднее?

Основные уязвимости

Иногда изменяются содержательные данные, порой – служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) возбудила судебный иск против президента корпорации, обвиняя его в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее боссом президенту. Содержание письма для нас сейчас не важно; важно время отправки.

Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что он (босс) в указанное время разговаривал по мобильному телефону, находясь за рулем автомобиля вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние «файл против файла». Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарь знала пароль своего босса, поскольку ей было поручено его регулярное изменение), и иск был отвергнут...

Участники обсуждения делятся на защитников секретаря и защитников босса компании Oracle и доказывают правоту защищаемой стороны и возможность фальсификации доказательств противника.

История вирусов

Александр Квасов, начальник управления информационных технологий Нижегородского регионального центра-филиала ОАО АКБ «СОЮЗ»:

В конце 90-х много вирусов было настроено на остановку работоспособности компьютера – уничтожение информации в BIOS, и на жестких дисках. На себе я испытал поражение жесткого диска вирусом W95.CIH «Чернобыль». На офисных компьютерах стояла операционная система Windows 95, доступ в Интернет имел один компьютер, остальные были связаны с ним в локальной сети. 26 апреля 1999 года не загрузились все офисные компьютеры, информация на дисках стала недоступной. Данные, к счастью, удалось восстановить, однако это было не так просто. Фирма понесла большие убытки.

Пометка для педагога: напомним, что W95.CIH заражал исполняемые файлы и обладал крайне деструктивной функциональностью. Он полностью уничтожал содержимое жесткого диска и перезаписывал флэш-BIOS материнской платы, после чего заражённый компьютер вообще переставал загружаться. Наиболее уязвимы для вируса компьютеры на базе операционных систем Windows 95, 98 и Me. В этом случае вирус ищет файлы с расширением .EXE и записывает свой код в неиспользуемые части этих файлов. Размер зараженных файлов при этом практически не увеличивается, и у пользователя не возникает никаких подозрений.

Участникам обсуждения проблемы предлагается представить себя на месте сотрудников ОАО АКБ «СОЮЗ», предложить варианты обнаружения заражения, проверки, профилактики, защиты данных.

Классификация вирусов

У журналиста-фрилансера возникли проблемы с программным обеспечением:

1. Большинство программ перестают работать и "вылетают" с критической ошибкой

2. Загрузка в безопасном режиме невозможна

3. Сайты kaspersky.ru, drweb.ru, viruslist.ru и пр. не загружаются

4. Значительно снизилась производительность компьютера.



Он решил, что это - результат деятельности вируса.

Участникам обсуждения предлагается по симптомам определить, что за вирус, как его лечить

Пометка для педагога: Вирус, который Kaspersky определяет как VIRUS.WIN32.Sality.z, а Dr. Web - win32.sector.5, win32.sector.7 (подробное описание). Даже у опытных пользователей его уничтожение вызывает трудности.

Пример решения:

1. Отключаем сеть. Т.е. отключаем ADSLm Dial-up, LAN - любые сетевые подключения. Просто выдергиваем кабель.

2. Идем к неинфицированному компьютеру, т.к. на инфицированном не удастся получить доступ к сайту, и скачиваем Dr.Web CureIt!. Это бесплатное приложение, которое может работать даже без установки. Скачанное приложение по возможности записываем на CD/DVD или флешку с защитой - дабы вирус не мог испортить программу. Если испортит - вместо приветственного окошка вы увидите окно стандартного распаковщика WinRAR SFX.

3. Чиним реестр с помощью установки ключа. Соглашаемся с внесением изменений в реестр.

4. Загружаемся в безопасном режиме, удерживая длительное время сразу после включения компьютера клавишу F8. Должно появиться меню с выбором вариантов загрузки. Нам нужен «Безопасный режим».

5. Лечим компьютер от вирусов. Для этого вставляем диск с записанным Dr.Web CureIt! и проводим полную проверку компьютера.

6. Перезагружаемся в обычном режиме.

7. Вновь проводим полную проверку.

8. Устанавливаем нормальный антивирус со свежими базами.

Медиа-вирусы

Студент факультета информатики был удивлен, заметив, что во время прослушивания определенного аудиофайла, активируется запуск браузера Internet Explorer, который переходит на страницу Интернета, где пользователю предлагается скачать и установить некий файл, выдаваемый за кодек со странным названием, расширением. Студент несколько раз отвергал установку. Студент описал происходящее на форуме сайта Virusov.net.

Что узнал студент? Какой это вирус? Что он делает? Чем опасен, к чему приводит?

Пометка для педагога: Эксперты «Лаборатории Касперского» отмечают вирус GetCodec.d. По их мнению, это уникальный пример червя, заражающего аудиофайлы. Напомним, что «червь», получивший название Worm.Win32.GetCodec.a, конвертирует mp3-файлы в формат WMA (при этом сохраняя расширение mp3) и добавляет в них маркер, содержащий в себе ссылку на зараженную web-страницу. Активация маркера осуществляется автоматически во время прослушивания файла и приводит к запуску браузера Internet Explorer, который переходит на инфицированную страницу, где пользователю предлагается скачать и установить некий файл, выдаваемый за кодек. Если пользователь соглашается на установку, то на его компьютер загружается троянская программа Trojan-Proxy.Win32.Agent.arp, с помощью которой злоумышленник может получить контроль над атакованным ПК.

Почтовые вирусы

Анатолию пришло письмо с темой: «Лучшие рефераты» тело письма пустое, почтовое



вложение – иконки HTML-документа Internet Explorer.

Позднее Анатолий заметил на дисках новые файлы C:ADMIN.DLL, D:ADMIN.DLL, E:ADMIN.DLL, а так же существование файла README.EML. Неожиданное наличие открытых общих сетевых ресурсов, несколько раз случалась перегрузка сети.

Какой это вирус? Что он делает? Чем опасен, к чему приводит? Как его лечить?

Тема 3: Назначение, структура и содержание Политики ИБ

Задание 1. Вопросы для обсуждения.

1. Структура и содержание Политики ИБ.

2. Источники информации для разработки Политики ИБ.

3. Особенности корпоративных и частных Политик ИБ.

4. Жизненный цикл Политики ИБ.

5. Ответственность за выполнение Политики ИБ.

Задание 2. Кейс

Исходная ситуация:

В коммерческой организации, которая занимается поставками компьютерной техники для государственных и муниципальных органов. При сумме потенциального контракта (поставки) более 100 тысяч рублей данная компания должна участвовать в тендере, соответственно сталкиваться с конкурентной борьбой во время проведения торгов. Компания не имеет никаких внутренних документов, касающихся информационной безопасности, в том числе политики безопасности.

В процессе участия в одной из процедур торгов ответственный менеджер по торгам получает на корпоративную почту письмо с заголовком "Срочно. Документы" с неизвестного адреса. Данное письмо содержит единственный архивный файл без текста самого письма. Менеджер открывает архив, после чего автоматически запускается вирус, который не только блокирует рабочий компьютер с установленным программным обеспечением для торгов и авторизированной электронной подписью организации, но и пытается распространяться по внутренней сети компании.

Сотрудники ИТ-отдела реагируют достаточно оперативно, локализуют распространение вируса, устраняют сам вирус и последствия его действия на всех зараженных компьютерах в течение 3-х часов. Но за это время торги закрываются, и компания упускает крупный контракт (порядка миллиона рублей).

Кто, по Вашему мнению, виноват в данной ситуации (менеджер, который открывал неизвестное письмо; сотрудники ИТ-отдела, которые не предприняли превентивных мер)? Кого следует наказать?

Правильный ответ

В данном случае: виноват первый руководитель организации (например, генеральный директор), который не инициировал создание и внедрение политики безопасности.

В политике безопасности могли быть описаны правила работы с электронной почтой, отдельно могли быть представлены правила организации работы во время проведения



торгов, а также правила проведения инструктажа сотрудников. Также в политике безопасности расписываются правила передачи ответственности при проведении определенных действий.

Если политика внедрена, инструктаж проведен, менеджер расписался о проведении инструктажа, то он не только 10 раз задумается, стоит ли открывать неизвестные письма, но и будет понимать, что наказание будет грозить непосредственно ему, так как на время торгов на него будет полностью возложена ответственность за их проведение.

Задание 3:

(проект)

Тема проекта: Требования, предъявляемые к Политике первого уровня

Политика информационной безопасности организации - высокоуровневый документ, описывающий основные принципы и правила, направленные на защиту информационных ресурсов организации.

Цель выполнения проекта заключается в формировании профессиональных компетенций обучаемых, выражающихся в способности проводить анализ документации на соответствие предъявляемым требованиям.

Задание.

1. Ознакомить с предоставленными преподавателем Политиками верхнего уровня организаций различных сфер деятельности.

2. Оценить по пятибалльной шкале содержание каждого из документов по следующим пунктам:

- Определение ИБ в терминах деятельности данной организации, области действия политики, целей, задач и принципов ОИБ организации.

- Изложение намерения ОИБ, направленного па достижение указанных целей и на реализацию принципов ОИБ.

- Общие сведения об активах, подлежащих защите, их классификацию.

- Модели угроз и нарушителей (внутреннего и внешнего) ИБ, на противодействие которым ориентирована корпоративная ПолИБ.

- Высокоуровневое изложение правил и требований по ОИБ, представляющих особую важность для организации (например, обеспечение соответствия законодательным актам, нормативным документам РФ в области ОИБ и нормативным актам организации; требования к управлению ИБ; требования по предотвращению и обнаружению компьютерных вирусов и другого вредоносного ПО; требования по УНБ).

- Санкции и последствия нарушений корпоративной ПолИБ.

- Определение общих ролей и обязанностей, связанных с ОИБ, включая информирование об инцидентах ИБ.

- Перечень частных ПолИБ, развивающих и детализирующих положения корпоративной Пол ИБ, а также указание подразделений организации, ответственных за их соблюдение и/или реализацию.

- Положения по контролю реализации корпоративной ПолИБ организации.

- Ответственность за реализацию и поддержку документа.

- Условия пересмотра (выпуска новой редакции) документа.

3. Подготовить презентацию выполненного проекта.

Результат проекта. Результаты проекта представляют собой проекты Политики безопасности организации 1-го уровня и частной политики безопасности, а также презентация, отражающая основные этапы выполнения задания.

Критерии оценки.

1. Полнота проведенного анализа.

2. Полнота обоснования результатов и выводов.

3. Оформление документов.

Проект

Проект «Разработка политики безопасности»

Политика информационной безопасности организации - высокоуровневый документ, описывающий основные принципы и правила, направленные на защиту информационных ресурсов организации.

Цель выполнения проектазаключается в формировании профессиональных компетенций обучаемых, выражающихся в способности участвовать в работах по разработке и реализации политики информационной безопасности.

Задание.

4. Проанализировать информационные процессы выбранной Вами организации и выявить критически важную информацию, которую необходимо защищать.

5. Разработать политику безопасности 1-го уровня организации в соответствии с требованиями нормативных документов.

6. Разработать частную политику безопасности. Объект политики выбирается исходя из специфики деятельности организации.

7. Подготовить презентацию выполненного проекта.

Результат проекта. Результаты проекта представляют собой проекты Политики безопасности организации 1-го уровня и частной политики безопасности, а также презентация, отражающая основные этапы выполнения задания.

Критерии оценки.

4. Полнота собранной информации по организации и проведенного анализа.

5. Степень соответствия структуры подготовленных документов требованиям стандартов в сфере обеспечения безопасности.

6. Содержание Политик безопасности.

7. Оформление документов.

Примерный перечень организаций

Номер варианта	Организация	Метод оценки риска
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
13	Компания по разработке ПО для сторонних организаций	1
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
26	Гостиница	2
27	Праздничное агентство	3
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

2. Примерный перечень вопросов к экзамену по дисциплине для студентов

1. Понятие информационной безопасности. Основные определения и термины.

2. Основные понятия, общеметодологические принципы обеспечения информационной безопасности.



3. Понятие «информационный ресурс».

4.Классы информационных ресурсов.

5. Документ, как класс информационных ресурсов.

6. Обобщенная модель документа.

7.Информация и ее виды.

8. Информационное оружие и его классификация.

9. Информационная война.

10. Виды информационных войн.

11. Правовое регулирование информационных потоков в различных видах деятельности.

12. Международные и отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации.

13. Организационное регулирование защиты процессов переработки информации.

14. Информация как объект юридической защиты.

15. Основные принципы засекречивания информации.

16. Государственная система правового обеспечения защиты информации в Российской Федерации.

17. Общие положения об информационных системах.

18. Информация как продукт.

19. Информационные услуги.

20**.** Источники конфиденциальной информации в информационных системах.

21. Что приводит к неправомерному овладению конфиденциальной информацией в информационных системах.

22. Виды технических средств информационных систем.

23. Классы каналов несанкционированного получения информации**.**

24.Причины нарушения целостности информации.

25. Виды угроз информационным системам.

25 Виды потерь.

26. Убытки, связанные с информационным обменом.

27. Модель нарушителя информационных систем.

28. Эмпирический подход к оценке уязвимости информации.

29. Система с полным перекрытием.

30. Методы определения требований к защите информации.

31. Требования к безопасности информационных систем в США.

32. Требования к безопасности информационных систем в России.

33. Классы защищенности СВТ от НСД.

34. Оценка состояния безопасности ИС Франции.

35. Факторы, влияющие на требуемый уровень защиты информации.

36. Критерии оценки безопасности информационных технологий.

37. Общие положения о функциях и задачах защиты информации.

38. Методы формирования функций защиты.

39. Классы задач защиты информации.

30. Функции защиты.

31. Состояния и функции системы защиты информации.

32. Содержание способов и средств обеспечения безопасности.

33. Методы и средства защиты информации.

34. Формальные средства защиты.

35. Неформальные средства защиты.

36. Понятие глобальной информационной сети. История появления и развития всемирной сети.

37. Государственная политика обеспечения информационной безопасности в условиях функционирования глобальных сетей.

38. Современные технологии обеспечения информационной безопасности в условиях функционирования глобальных сетей.

39. Угрозы информационной безопасности функционированию глобальных сетей.

40. Виртуальные частные сети. Межсетевые экраны.

41. Фейки и способы их распознавания.

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

Требования к написанию реферата

Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.



Реферат должен быть структурирован (по главам, разделам, параграфам) и включать разделы: введение, основная часть, заключение, список использованных источников. В зависимости от тематики реферата к нему могут быть оформлены приложения, содержащие документы, иллюстрации, таблицы, схемы и т.д. Объем реферата – 15-20 страниц печатного текста, включая титульный лист, введение, заключение и список литературы.

Его задачами являются:

1. Формирование умений самостоятельной работы с источниками литературы, их систематизация;

2. Развитие навыков логического мышления;

3. Углубление теоретических знаний по проблеме исследования.

При оценке реферата используются следующие критерии:

- новизна текста;

- обоснованность выбора источника;

- степень раскрытия сущности вопроса;

- соблюдения требований к оформлению.

Критерии оценивания реферата:	
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
«удовлетвори-тельно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
«неудовлетво-рительно»	Тема реферата не раскрыта, обнаруживается существенное не понимание проблемы.

Тематика рефератов выдается преподавателем в конце семинарского занятия.

Требования к написанию доклада

Доклад – продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.



Критерии оценивания доклада:

Отметка «отлично» выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Отметка«хорошо» - основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, не выдержан объём реферата, имеются упущения в оформлении, не допускает существенных неточностей в ответе на дополнительный вопрос.

Отметка «удовлетворительно» - имеются существенные отступления от требований к докладу. В частности, тема освещена лишь частично, допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы, во время защиты отсутствует вывод.

Отметка «неудовлетворительно» - тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Требования к выполнению тестового задания

Тестирование является одним из основных средств формального контроля качества обучения. Это метод, основанный на стандартизированных заданиях, которые позволяют измерить психофизиологические и личностные характеристики, а также знания, умения и навыки испытуемого.

Основные принципы тестирования, следующие:

− связь с целями обучения - цели тестирования должны отвечать критериям социальной полезности и значимости, научной корректности и общественной поддержки;

− объективность - использование в педагогических измерениях этого принципа призвано не допустить субъективизма и предвзятости в процессе этих измерений;

− справедливость и гласность - одинаково доброжелательное отношение ко всем обучающимся, открытость всех этапов процесса измерений, своевременность ознакомления обучающихся с результатами измерений;

− систематичность – систематичность тестирований и самопроверок каждого учебного модуля, раздела и каждой темы; важным аспектом данного принципа является требование репрезентативного представления содержания учебного курса в содержании теста;

- гуманность и этичность - тестовые задания и процедура тестирования должны исключать нанесение какого-либо вреда обучающимся, не допускать ущемления их по национальному, этническому, материальному, расовому, территориальному, культурному и другим признакам;

Важнейшим является принцип, в соответствии с которым тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

− закрытая форма - является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Например, обучающемуся задается вопрос, требующий альтернативного ответа «да» или «нет», «является» или «не является», «относится» или «не относится» и т.п. Тестовое задание, содержащее вопрос в закрытой



форме, включает в себя один или несколько правильных ответов и иногда называется выборочным заданием. Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде. Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

− открытая форма - вопрос в открытой форме представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие - части слова или буквы, условные обозначения, линии или изображения элементов схемы и графика. Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

− установление соответствия - в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

− установление последовательности - предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

Критерии оценки знаний при проведении тестирования

Отметка «отлично» выставляется при условии правильного ответа не менее чем 85% тестовых заданий;

Отметка «хорошо» выставляется при условии правильного ответа не менее чем 70 % тестовых заданий;

Отметка «удовлетворительно» выставляется при условии правильного ответа не менее 50 %;

Отметка «неудовлетворительно» выставляется при условии правильного ответа менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации.

Критерии оценки знаний на экзамене

Экзамен может проводиться в форме устного опроса по билетам (вопросам) или без билетов, с предварительной подготовкой или без подготовки, по усмотрению преподавателя. Экзаменатор вправе задавать вопросы сверх билета, а также, помимо теоретических вопросов, давать задачи по программе данного курса.

Экзаменационные билеты (вопросы) утверждаются на заседании кафедры и подписываются заведующим кафедрой. В билете должно содержаться не более трех вопросов. Комплект экзаменационных билетов по дисциплине должен содержать 15—20 билетов.

Экзаменатор может проставить экзамен без опроса или собеседования тем обучающимся, которые активно участвовали в практических и лабораторных занятиях.

Отметка «отлично» - обучающийся глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает теорию с практикой. Обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, заданиями и другими видами применения знаний, показывает знания законодательного и нормативно-технического материалов, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ, обнаруживает умение самостоятельно обобщать и излагать материал, не допуская ошибок.



Отметка «хорошо» - обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми навыками при выполнении практических заданий.

Отметка «удовлетворительно» - обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.

Отметка «неудовлетворительно» **-** обучающийся не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические работы.



8. Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1. Основная литература

Название	Ссылка
Зенков, А.В. Информационная безопасность и защита информации : учебное пособие / А.В. Зенков. - 2-е изд.,пер. и доп. - Москва : Юрайт, 2023. - 107 с. - (Высшее образование). - ЭБС Знаниум. - URL: https://urait.ru/bcode/530927. - Режим доступа: по подписке. - ISBN 978-5-534-16388-9	https://urait.ru/bcode/530927
Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. - 4-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2022. - 336 с. - (Высшее образование). - ЭБС Знаниум. - URL: https://znanium.com/catalog/document?id=393765. - Режим доступа: по подписке. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7	https://znanium.com/catalog/document?id=393765
Сычев, Ю.Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. - Москва : ИНФРА-М, 2023. - 201 с. - (Высшее образование: Магистратура). - ЭБС Знаниум. - URL: https://znanium.com/catalog/document?id=420080. - Режим доступа: по подписке. - ISBN 978-5-16-014976-9. - ISBN 978-5-16-107471-8	https://znanium.com/catalog/document?id=420080
Суворова, Г.М. Информационная безопасность : учебное пособие / Г.М. Суворова. - 2-е изд.,пер. и доп. - Москва : Юрайт, 2023. - 277 с. - (Высшее образование). - ЭБС Юрайт. - URL: https://urait.ru/bcode/531084. - Режим доступа: по подписке. - ISBN 978-5-534-16450-3	https://urait.ru/bcode/531084
Галатенко, В.А. Основы информационной безопасности : учебное пособие / В.А. Галатенко. - Москва : Интернет-Университет Информационных Технологий, 2020. - 266 с. - ЭБС IPR Books. - URL: http://www.iprbookshop.ru/97562.html. - Режим доступа: по подписке. - ISBN 978-5-4497-0675-1	http://www.iprbookshop.ru/97562.html

8.2. Дополнительная литература

Название	Ссылка
Башлы, П.Н. Информационная безопасность и защита информации : учебник / П.Н. Баш лы, А.В. Бабаш, Е.К. Баранова. - Москва : РИОР, 2013. - 222 с. - ЭБС Знаниум. - URL: http://znanium.com/catalog/document?id=213488. - Режим доступа: по подписке	http://znanium.com/catalog/document?id=213488
Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3 изд. - Москва : РИОР : ИНФРА-М, 2019. - 400 с. - (Высшее образование). - ЭБС Знаниум. - URL: http://znanium.com/catalog/document?id=339378. - Режим доступа: по подписке. - ISBN 978-5-369-01759-3. - ISBN 978-5-16-106478-8. - ISBN 978-5-16-013801-5	http://znanium.com/catalog/document?id=339378
Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. - Саратов : Ай Пи Эр Медиа, 2019. - 227 с. - ЭБС IPR Books. - URL: http://www.iprbookshop.ru/80290.html. - Режим доступа: по подписке. - ISBN 978-5-4486-0485-0	http://www.iprbookshop.ru/80290.html
Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. - 4-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2021. - 336 с. - (Высшее образование). - ЭБС Знаниум. - URL: http://znanium.com/catalog/document?id=364911. - Режим доступа: по подписке. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7	http://znanium.com/catalog/document?id=364911
Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3 изд. - Москва : РИОР : ИНФРА-М, 2021. - 400 с. - (Высшее образование). - ЭБС Знаниум. - URL:	http://znanium.com/catalog/document?id=367588



Название	Ссылка
http://znanium.com/catalog/document?id=367588. - Режим доступа: по подписке. - ISBN 978-5-369-01759-3. - ISBN 978-5-16-106478-8. - ISBN 978-5-16-013801-5	
Глотина, И.М. Средства безопасности операционной системы Windows Server 2008 : учебно-методическое пособие / И.М. Глотина. - Саратов : Вузовское образование, 2018. - 141 c. - ЭБС IPR Books. - URL: http://www.iprbookshop.ru/72538.html. - Режим доступа: по подписке. - ISBN 978-5-4487-0136-8	http://www.iprbookshop.ru/72538.html

8.3. Информационно-телекоммуникационные ресурсы сети «Интернет»

Znanium.com. Базовая коллекция : электронно-библиотечная система : сайт / ООО "Научно-издательский центр Инфра-М". – Москва, 2011 - – URL: http://znanium.com/catalog (дата обновления: 06.06.2019). - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. Фонд ЭБС формируется с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. http://znanium.com/catalog/ IPRBooks. Базовая коллекция : электронно-библиотечная система : сайт / Общество с ограниченной ответственностью Компания "Ай Пи Ар Медиа". – Саратов, 2010 - . – URL: http://www.iprbookshop.ru/586.html - Режим доступа: для зарегистрир. пользователей. – Текст электронный. Является распространенным образовательным электронным ресурсом для высших и средних специальных учебных заведений, научно-исследовательских институтов, публичных библиотек, приобретающих корпоративный доступ для своих обучающихся, преподавателей и т.д. ЭБС включает учебную и научную литературу по направлениям подготовки высшего и среднего профессионального образования.ЭБС «Консультант студента». Коллекция Информационная безопасность : студенческая электронная библиотека : сайт / ООО «Политехресурс». Электронная библиотека технического вуза. – Москва, 2012. - . – URL: https://www.studentlibrary.ru/ru/catalogue/switch_kit/x2016-034.html - Режим доступа: для зарегистрир. пользователей. – Текст электронный.Является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов третьего поколения (ФГОС ВО 3+) к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы, для СПО, ВО и аспирантуры. http://www.iprbookshop.ru/586.html eLIBRARY.RU. : научная электронная библиотека : сайт. – Москва, 2000. - . – URL: https://elibrary.ru/defaultx.asp. - Режим доступа: для зарегистрир. пользователей. – Текст: электронный. Платформа eLIBRARY.RU была создана в 1999 году по инициативе Российского фонда фундаментальных исследований для обеспечения российским ученым электронного доступа к ведущим иностранным научным изданиям. С 2005 года eLIBRARY.RU начала работу с русскоязычными публикациями и ныне является ведущей электронной библиотекой научной периодики на русском языке в мире. https://elibrary.ru/defaultx.asp Периодические издания доступные обучающимся и сотрудникам ФГБОУ ВО МГТУ по подписке и на основании контрактов и лицензионных соглашений. /index.php/resursy/37-periodicheskie-izdaniya ФСТЭК России. Федеральная служба по техническому и экспортному контролю : официальный сайт. – Москва. – URL: https://fstec.ru// - Текст: электронный.Является федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации. https://fstec.ru/ Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере имени В. В. Соломатина (ВНИИНС им. В.В. Соломатина) : официальный сайт. – Москва. – URL: https://www.vniins.ru/. – Текст: электронный.ВНИИНС - это современное высокотехнологичное научно-производственное предприятие, занимающее ключевую позицию в развитии отечественной IT индустрии. Приоритетной задачей которого является создание отечественных информационных технологий, внедрение которых обеспечит технологическую независимость России от зарубежных производителей программного обеспечения. https://www.vniins.ru/ Лаборатория Касперского : официальный сайт. – Москва, 2019. - . – URL:



https://www.kaspersky.ru/. – Текст: электронный.Самый популярный в России и крупнейший в Европе производитель систем защиты от вирусов, спама и хакерских атак. Компания входит в четвёрку ведущих мировых производителей программных решений для обеспечения информационной безопасности. https://www.kaspersky.ru/ InformationSecurity. Информационная безопасность : [сайт]. – Москва, 2019. – URL: http://www.itsec.ru/news. - Текст: электронный.Портал об информационной безопасности: новости, форум, программные новинки, архив изданий по информационной безопасности. http://www.itsec.ru/news

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

9.1. Учебно-методические материалы по лекционному материалу дисциплины Б1.О.22 Основы информационной безопасности

Раздел / Тема с указанием основных учебных элементов	Методы обучения	Способы (формы) обучения	Средства обучения	Формируемые компетенции
Тема 1. Введение. Исторические аспекты возникновения и развития информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации (ОПК-1.1)
Тема 2. Основные понятия и определения сферы информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия, первоисточники	Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации (ОПК-1.1)
Тема 3. Базовые принципы информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации (ОПК-1.1)
Тема 4. Информация - наиболее ценный ресурс современного общества	**по источнику знаний:** лекция, чтение, конспектирование	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные	Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности

	по назначению: приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный		пособия	Российской Федерации (ОПК-1.1)
Тема 5. Проблемы информационной войны	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире (ОПК-1.3)
Тема 6. Организационно-правовое обеспечение информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия, первоисточники	Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации (ПК-5.1).
Тема 7. Информационные системы. Общие положения. Информация как продукт. Информационные услуги	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации (ОПК-1.1) Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации (ПК-5.1).
Тема 8. Угрозы информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Умеет классифицировать и оценивать угрозы информационной безопасности (ОПК-1.2).
Тема 9. Методы и модели	**по источнику знаний:** лекция, чтение,	Самостоятельная	Устная речь,	Умеет классифицировать и оценивать угрозы

оценки уязвимости информации	конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	работа студента, домашние задания	учебники, учебные пособия	информационной безопасности (ОПК-1.2). Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации (ПК-5.1).
Тема 10. Методы определения требований к защите информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Умеет классифицировать и оценивать угрозы информационной безопасности (ОПК-1.2). Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации (ПК-5.1).
Тема 11. Анализ существующих методик определения требований к защите информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации (ПК-5.2) Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации (ПК-5.3)
Тема 12. Функции и задачи защиты информации. Стратегии защиты информации.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Умеет классифицировать и оценивать угрозы информационной безопасности (ОПК-1.2) Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации (ПК-5.2)
Тема 13. Способы и средства защиты информации	**по источнику знаний:** лекция, чтение, конспектирование	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные	Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки

	по назначению: приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный		пособия	по техническим каналам и контроля эффективности защиты информации (ОПК-9.1) Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации (ПК-5.1). Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации (ПК-5.2
Тема 14. Информационная безопасность в условиях функционирования глобальных сетей.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире (ОПК-1.3)

9.2. Учебно-методические материалы по практическим (лабораторным) занятиям дисциплины Б1.О.22 Основы информационной безопасности

№ раздела дисциплины	Наименование практических занятий	Методы обучения	Способы (формы) обучения	Средства обучения	Формируемые компетенции
Тема 4. Информация - наиболее ценный ресурс современного общества	Анализ информации на предмет целостности. Определение коэффициентов важности, полноты, адекватности, релевантности, толерантности информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	ОПК-1.1

Тема 5. Проблемы информационной войны	Выявление признаков информационной войны в СМИ и сети Интернет	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	ОПК-1.3
Тема 6. Организационно-правовое обеспечение информационной безопасности	Понятие безопасности, ее объекты. Совет Безопасности Российской Федерации и его функции и задачи в области обеспечения безопасности. Особенности системы организационно-правовой защиты информации, составляющей государственную и коммерческую тайну.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия, первоисточники	ПК-5.1
Тема 8. Угрозы информации	Ознакомление с алгоритмами оценки риска информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	ОПК-1.2
Тема 11. Анализ существующих методик определения требований к защите информации	Особенности международной защиты банковской тайны. Международная система охраны интеллектуальной собственности.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	ПК-5.2 ПК-5.3
Тема 12. Функции и задачи защиты информации. Стратегии защиты информации	Защита информации в автоматизированных системах: особенности парольной защиты, антивирусная защита, аппаратная защита.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	ОПК-1.2 ПК-5.2
Тема 13. Способы и средства защиты информации	Классификации методов и средств защиты информации от утечки по техническим	**по источнику знаний:** лекция, чтение, конспектирование	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	ОПК-9.1

	каналам. Функционирование программного обеспечения для информационной безопасности. Классификация программ по защите информации.	**по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный			ПК-5.1 ПК-5.2
Тема 14. Информационная безопасность в условиях функционирования глобальных сетей.	Сетевое сканирование. Анализ работы межсетевых экранов.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа студента, домашние задания	Устная речь, учебники, учебные пособия	ОПК-1.3

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

10.1. Перечень необходимого программного обеспечения

Название
7-Zip Свободная лицензия
Adobe Reader DC Свободная лицензия
Cisco Packet Tracer Свободная лицензия
Microsoft Office Word 2010 Номер продукта 14.0.6024.1000 SP1 MSO 02260-018-0000106-48095
Антивирус kaspersky endpoint security Лицензионный договор от 17.02.2021 № 203-20122401
Операционная система Windows Договор от 26.05.2020 № 32009117096 Договор от 17.01.2019 № 31908696765
Офисный пакет Microsoft office 2016 Договор от 26.05.2020 № 32009117096 Договор от 17.01.2019 № 31908696765

10.2. Перечень необходимых информационных справочных систем:

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам:

Название

Для обучающихся обеспечен доступ (удаленный доступ) к следующим современным профессиональным базам данных, информационным справочным и поисковым системам:

Название

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

Наименования специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Лаборатория проектирования информационных систем (3-3-2) 385000, Республика Адыгея, г. Майкоп, ул. Пушкина, дом № 177, Учебный корпус № 3	Компьютерное рабочее место (системный блок, монитор, клавиатура, мышь) – 13 шт.; маршрутизатор; IP камеры – 2 шт.	Операционная система Windows7 Профессиональная, MicrosoftCorp., № 00371-838-5849405-85257, 23.01.2012, бессрочный.Текстовый процессор Microsoft Office Word 2010. Номер продукта 14.0.6024.1000 SP1 MSO (14.0.6024.1000) 02260-018-0000 106-48095.Антивирусные программы: Kaspersky Anti-virus 6/0 – № лицензии 26FE-000451-5729CF81, срок лицензии 07.02.2020.Cisco Packet Tracer – симулятор сети передачи данных. Производитель: CISCO Systems.Wireshark – сниффер, предназначенный для анализа трафика компьютерных сетей (Ethernet, FDDI, PPP, Token-Ring и других) в режиме реального времени, используя широковещательный режим сетевой карты. Свободно распространяемое ПО.