Частное образовательное учреждение
высшего образования
«Брянский институт управления и бизнеса»

УТВЕРЖДАЮ
Заведующий кафедрой информатики и программного обеспечения
Т.М. Хвостенко
«29» августа 2024 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Укрупненная группа направлений и специальностей	090000 Информатика и вычислительная техника
Направление подготовки:	09.03.03 Прикладная информатика
Профиль:	Прикладная информатика

Разработала: Гришанова Т.В.

Брянск 2024

СОДЕРЖАНИЕ

1. Аннотация к дисциплине

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденный приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. №922 (с изменениями и дополнениями от: 26 ноября 2020 г., 8 февраля 2021 г.).

Место дисциплины в структуре основной профессиональной образовательной программы

Настоящая дисциплина включена в обязательную часть Блока1 учебных планов по направлению подготовки 09.03.03 Прикладная информатика уровень бакалавриата.

Дисциплина изучается на 2 курсе в 4 семестре, зачет с оценкой при очной форме обучения, на 3 курсе в 6 семестре, зачет с оценкой, контрольная работа при очно-заочной форме обучения, на 5 курсе в 10 семестре, зачет с оценкой, контрольная работа при заочной форме обучения.

Цель изучения дисциплины:

формирование у обучающихся системы знаний в области теории и практики информационной безопасности

Задачи:

- изучить принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
- изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;
- приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;
- формирование практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2.Учитывает основные требования информационной безопасности при решении задач профессиональной деятельности

ПК-3. Способность разрабатывать архитектуру информационной системы и согласовывать ее с заинтересованными сторонами

ПК-3.2 Определять требования информационной безопасности к архитектуре информационных системы

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

- Процесс изучения дисциплины направлен на формирование компетенций, предусмотренных ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата) и на основе профессионального стандарта «Специалист по информационным системам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н (зарегистрирован Министерством юстиции Российской Федерации 24 декабря 2014 г., регистрационный № 35361), с изменением, внесенным приказом Министерства труда и

социальной защиты Российской Федерации от 12 декабря 2016 г. № 727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный № 45230)

Код компетенции	**Результаты освоения ОПОП (содержание компетенций)**	**Индикаторы достижения компетенций**	**Формы образовательной деятельности, способствующие формированию и развитию компетенции**
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2.Учитывает основные требования информационной безопасности при решении задач профессиональной деятельности **Знать**: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Уметь**: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Владеть**: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности..	Контактная работа: Лекции Практические занятия Самостоятельная работа
ПК-3.	Способность разрабатывать архитектуру информационной системы и согласовывать ее с заинтересованными сторонами	ПК-3.2 Определять требования информационной безопасности к архитектуре информационных системы **Знать:** методы и средства обеспечения информационной безопасности*;* основные технические средства и методы защиты информации. **Уметь:** проводить анализ угроз информационной безопасности; применять на практике основные обще методические принципы информационной безопасности **Владеть:** навыками комплексного обеспечения информационной безопасности; выполнять полный объем работ, связанный с выполнением информационной безопасности	Контактная работа: Лекции Практические занятия Самостоятельная работа

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

3.1 Объём дисциплины по видам учебных занятий (в часах)

Объём дисциплины	Всего часов		
	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость дисциплины	108		
Контактная работа обучающихся с преподавателем (всего)	60	30	36
Аудиторная работа (всего):	60	30	36
в том числе:			
Лекции	30	10	16
семинары, практические занятия	30	20	20
лабораторные работы			
Внеаудиторная работа (всего):			
в том числе:			
Самостоятельная работа обучающихся (всего)	48	78	68
Вид промежуточной аттестации обучающегося – дифференцированный зачет, контрольная работа			4

4.Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Тематическая структура дисциплины

№ п.п	Наименование модуля	№ п.п.	Тема	Вырабатываемая компетенция
1	Концепция информационной безопасности.	1	Актуальность информационной безопасности.	ОПК-3.2, ПК-3.2
		2	Пользователи и злоумышленники в Интернет	
		3	Лицензирование и сертификация в области защиты информации.	
		4	Основные нормативные руководящие документы	
2	Угрозы информации.	5	Виды угроз информационной безопасности РФ	ОПК-3.2, ПК-3.2
		6	Информационная безопасность сетей.	
		7	Способы совершения компьютерных преступлений.	
		8	Уязвимость сети Интернет.	
		9	Обеспечение информационной безопасности.	
3	Виды возможных нарушений информационной системы.	10	Компьютерные преступления.	ОПК-3.2, ПК-3.2
		11	Вредоносные программы.	
		12	Вирусы.	

		13	Признаки заражения компьютера	
		14	Антивирусное программное обеспечение.	
4	Информационная безопасность информационных систем.	15	Теория информационной безопасности информационных систем.	ОПК-3.2, ПК-3.2
		16	Криптографические способы защиты информации.	
		17	Организация информационной безопасности компании.	
		18	Угрозы информационной безопасности для автоматизированной системы обработки информации	
		19	Контроль доступа к информации	

4.2 Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

для очной формы обучения

№п/п	Разделы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)							Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации *(по семестрам)*
			Всего	Из них аудиторные занятия				Самостоя	Контроль	Курсовая
				Лекции	.Практикум. Лаборатор	Практическ.занятия /семинары					
1	Концепция информационной безопасности	4	27	8		7		12			Опрос, тестирование
2	Угрозы информации.	4	27	8		7		12			Опрос, тестирование
3	Виды возможных нарушений информационной системы	4	27	7		8		12			Опрос, решение задач
4	Информационная безопасность информационных систем	4	27	7		8		12			Опрос, решение задач
	Контроль	4									
			108	**30**		**30**		**48**			**(дифференцированный**

											зачет)

для очно-заочной формы обучения

№п/п	Разделы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)							Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации *(по семестрам)*
			Всего	Из них аудиторные занятия			Самостоя	Контроль	Курсовая	
				Лекции	.Практикум. Лаборатор	Практическ.занятия /семинары				
1	Концепция информационной безопасности	6	27	4		5	18			Опрос, тестирование
2	Угрозы информации.	6	27	2		5	20			Опрос, тестирование
3	Виды возможных нарушений информационной системы	6	27	2		5	20			Опрос, решение задач
4	Информационная безопасность информационных систем	6	27	2		5	20			Опрос, решение задач
	Контроль	6								
			108	**10**		**20**	**78**			**(дифференцированный зачет)**

для заочной формы обучения

№п/п	Разделы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации *(по семестрам)*
			Всего	Из них аудиторные занятия	Самостоя	Контроль	Курсовая	

				Лекции	.Практикум. Лаборатор	Практическ.занятия /семинары					
1	Концепция информационной безопасности	10	26	4		5		17			Опрос, тестирование
2	Угрозы информации.	10	26	4		5		17			Опрос, тестирование
3	Виды возможных нарушений информационной системы	10	26	4		5		17			Опрос, решение задач
4	Информационная безопасность информационных систем	10	26	4		5		17			Опрос, решение задач
	Контроль	10	4								
			108	**16**		**20**		**68**			**4 (дифференцированный зачет)**

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа обучающихся при изучении курса «Информационная безопасность» предполагает, в первую очередь, работу с основной и дополнительной литературой. Результатами этой работы становятся выступления на практических занятиях, участие в обсуждении.

Методика самостоятельной работы предварительно разъясняется преподавателем и в последующем может уточняться с учетом индивидуальных особенностей обучающихся. Время и место самостоятельной работы выбираются обучающимися по своему усмотрению с учетом рекомендаций преподавателя.

Самостоятельную работу над дисциплиной следует начинать с изучения рабочей программы дисциплины «Информационная безопасность», которая содержит основные требования к знаниям, умениям и навыкам обучаемых. Обязательно следует вспомнить рекомендации преподавателя, данные в ходе установочных занятий. Затем – приступать к изучению отдельных разделов и тем в порядке, предусмотренном программой.

Получив представление об основном содержании раздела, темы, необходимо изучить материал с помощью учебников, указанных в разделе 7 указанной программы. Целесообразно составить краткий конспект или схему, отображающую смысл и связи основных понятий данного раздела и включенных в него тем. Затем, как показывает опыт, полезно изучить выдержки из первоисточников. При желании можно составить их краткий конспект. Обязательно следует записывать возникшие вопросы, на которые не удалось ответить самостоятельно.

Наименование раздела	Вопросы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Учебно-методическое обеспечение	Форма контроля
Концепция информационной безопасности	Основные нормативные руководящие документы	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Опрос, доклад-презентация
Угрозы информации.	Виды угроз информационной безопасности РФ	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации	Литература к теме, работа с интернет источниками	Опрос, доклад-презентация
Виды возможных нарушений информационной системы	Антивирусное программное обеспечение.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Опрос, доклад-презентация
Информационная безопасность информационных систем	Теория информационной безопасности информационных систем.	Работа в библиотеке, включая ЭБС. Подготовка доклада-презентации.	Литература к теме, работа с интернет источниками	Опрос, доклад-презентация

6. Оценочные материалы для проведения текущей и промежуточной аттестации обучающихся по дисциплине «Информационная безопасность»

6.1. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Шкала и критерии оценки, балл	Критерии оценивания компетенции
1.	Опрос	Сбор первичной информации по выяснению уровня усвоения пройденного материала	«Зачтено» - если обучающийся демонстрирует знание материала по разделу, основанные на знакомстве с обязательной литературой и современными публикациями; дает логичные, аргументированные ответы на поставленные вопросы. Также оценка «зачтено» ставится, если обучающимся допущены незначительные неточности в ответах, которые он исправляет путем наводящих вопросов со стороны преподавателя. «Не зачтено» - имеются существенные пробелы в знании	ОПК-3.2, ПК-3.2

			основного материала по разделу, а также допущены принципиальные ошибки при изложении материала.	
2	Доклад-презентация	Публичное выступление по представлению полученных результатов в программе Microsoft PowerPoint	«отлично» – доклад выполнен в соответствии с заявленной темой, презентация легко читаема и ясна для понимания, грамотное использование терминологии, свободное изложение рассматриваемых проблем, докладчик правильно ответил на все вопросы в ходе дискуссии; «хорошо» – некорректное оформление презентации, грамотное использование терминологии, в основном свободное изложение рассматриваемых проблем, докладчик частично правильно ответил на все вопросы в ходе дискуссии; «удовлетворительно» – отсутствие презентации, докладчик испытывал затруднения при выступлении и ответе на вопросы в ходе дискуссии; «неудовлетворительно» - докладчик не раскрыл тему	ОПК-3.2, ПК-3.2
3	Тестирование	Тестирование можно проводить в форме: • компьютерного тестирования, т.е. компьютер произвольно выбирает вопросы из базы данных по степени сложности; • письменных ответов, т.е. преподаватель задает вопрос и дает несколько вариантов ответа, а студент на отдельном листе записывает номера вопросов и номера соответствующих ответов	«отлично» - процент правильных ответов 80-100%; «хорошо» - процент правильных ответов 65-79,9%; «удовлетворительно» - процент правильных ответов 50-64,9%; «неудовлетворительно» - процент правильных ответов менее 50%.	ОПК-3.2, ПК-3.2
4	Контрольная работа	Умение логически излагать материал по теме контрольной работы Умение правильно отвечать на вопросы по теме контрольной работы	«отлично» – контрольная работа выполнена в соответствии с заявленной темой и всеми требованиями, предъявляемыми к контрольной работе; тема контрольная работы раскрыта полностью; доклад сопровождается презентацией, которая легко читаема и ясна для понимания; студент грамотно использует терминологию и свободно излагает суть рассматриваемой проблемы, правильно отвечает на все вопросы по теме	ОПК-3.2, ПК-3.2

			контрольной работы; «хорошо» – контрольная работа выполнена в соответствии с заявленной темой и всеми требованиями, предъявляемыми к контрольной работе; тема контрольной работы раскрыта полностью; доклад сопровождается презентацией, в которой имеются неточности и несущественные ошибки; студент грамотно использует терминологию и в основном свободно излагает суть рассматриваемой проблемы, правильно отвечает на большинство вопросов по теме контрольной работы; «удовлетворительно» – контрольная работа выполнена в соответствии с заявленной темой и всеми требованиями, предъявляемыми к контрольной работе; тема контрольной работы раскрыта полностью; доклад не сопровождается презентацией; студент испытывает затруднения при изложении сути рассматриваемой проблемы и при ответе на вопросы по теме контрольной работы; «неудовлетворительно» - контрольная работа выполнена с нарушением требований, предъявляемыми к контрольной работе; тема контрольной работы не раскрыта	

6.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

№	**Форма контроля/ коды оцениваемых компетенций**	**Процедура оценивания**	**Шкала и критерии оценки, балл**
3.	**Дифференцированный зачет** - ОПК-3.2	Правильность ответов на все вопросы (верное, четкое и достаточно глубокое изложение идей, понятий, фактов и т.д.); Сочетание полноты и лаконичности ответа; Наличие практических навыков по дисциплине (решение задач или заданий); Ориентирование в учебной, научной и специальной литературе; Логика и аргументированность изложения; Грамотное комментирование, приведение примеров, аналогий; Культура ответа.	1. оценка «отлично» - обучающийся должен дать полные, исчерпывающие ответы на вопросы, в частности, ответ должен предполагать знание основных понятий и их особенностей, умение правильно определять специфику соответствующих отношений, правильное решение практического задания. Оценка «отлично» предполагает наличие системы знаний по предмету, умение излагать материал в логической последовательности, систематично, грамотным языком; 2. оценка «хорошо» - обучающийся должен дать полные ответы на вопросы. Допускаются неточности при ответе, которые все же не влияют на правильность ответа. Ответ должен предполагать знание основных понятий и их особенностей, умение правильно определять специфику соответствующих отношений, правильное решение практического задания.. Оценка «хорошо» предполагает наличие системы знаний по предмету, умение излагать материал в логической последовательности, систематично, грамотным языком, однако, допускаются незначительные ошибки, неточности по названным критериям, которые все же не искажают сути соответствующего ответа; 3. оценка «удовлетворительно» - обучающийся должен в целом дать ответы на вопросы, ориентироваться в системе дисциплины «Организационное поведение», продемонстрировать правильный ход решения практического задания, знать основные категории предмета. Оценка «удовлетворительно» предполагает, что материал в основном изложен грамотным языком; 4. оценка «неудовлетворительно» предполагает, что обучающимся либо не дан ответ на вопрос билета, либо обучающийся не знает основных категорий, не может определить предмет дисциплины. 5. «зачтено» - выставляется при соответствии параметрам экзаменационной шкалы на уровнях «отлично», «хорошо», «удовлетворительно». 6. «не зачтено» - выставляется при соответствии параметрам экзаменационной шкалы на уровне «неудовлетворительно».
4.	**Тестирование (на зачете) –** ОПК-3.2	Полнота знаний теоретического	«отлично» - процент правильных ответов 80-

		контролируемого материала. Количество правильных ответов	100%; «хорошо» - процент правильных ответов 65-79,9%; «удовлетворительно» - процент правильных ответов 50-64,9%; «неудовлетворительно» - процент правильных ответов менее 50%.

6.3. Типовые контрольные задания или иные материалы, необходимые для процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

6.3.1. Типовые задания для проведения текущего контроля обучающихся

6.3.1.1. Примерная тематика контрольных работ

Теоретическая часть контрольной работы объемом 5-6 страниц должна содержать краткий литературный обзор состояния заданного для анализа вопроса.

Варианты заданий:

1. Понятие, проблемы и структура экономической безопасность предпринимательской деятельности (на примере фирм различных типов).
2. Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.
3. Информационная безопасность, история формирования.
4. Концепция информационной безопасности.
5. Основы экономической безопасности предпринимательской деятельности.
6. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
7. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
8. Информационная безопасность (по материалам зарубежных источников и литературы).
9. Правовые основы защиты конфиденциальной информации.
10. Экономические основы защиты конфиденциальной информации.
11. Организационные основы защиты конфиденциальной информации.
12. Построение и функционирование защищенного документооборота.
13. Анализ инструкции по обработке и хранению конфиденциальных документов.
14. Направления и методы защиты аудио и визуальных документов.
15. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
16. Анализ опыта защиты информации в зарубежных странах.
17. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
18. Основы технологии обработки и хранения конфиденциальных документов.
19. Назначение, виды, структура и технология функционирования системы защиты информации.

Практическая часть. Основное внимание при выполнении контрольной работы студент должен уделить подготовке ее практической части, которая предполагает принятие им самостоятельных решений в сфере разработки и описания бизнес-процесса заданной области согласно заданию. Ее объем должен составлять 5-6 страниц. С использованием методов шифрования Цезаря, Скитала, метода шифрующих таблиц, метода шифрующих таблиц с одиночной перестановкой по ключу зашифровать текст согласно варианта

Содержание задания:

1. С использованием метода шифрования Цезаря зашифровать текст согласно варианта:
1. На вкус и цвет товарища нет (K=7)
2. Гусь свинье не товарищ (K=4)
3. Зимой и летом одним цветом (K=6)
4. Волка ноги кормят (K=3)
5. Сытый голодного не разумеет (K=5)
6. День год кормит (K=7)
7. Тамбовский волк тебе товарищ (K=6)
8. Произведен запуск спутника (K=6)
9. Зашифровать текст: Корабль пошел ко дну, m = 5, n = 4
10. Зашифровать текст: Использование секретного ключа запрещено, m = 7, n = 62.

2. . Зашифровать текст методом Скитала, методом шифрующих таблиц согласно варианту:
1. Это слово будет зашифровано, m=5, n=6
2. Я памятник себе воздвиг нерукотворный, m=7, n=6
3. Пусть всегда будет солнце, m=5, n=5
4. Криптография наука сложная, m=7, n=4
5. Погода сегодня хорошая, m=6, n=4
6. В Петербурге сегодня гроза, m=7, n=4
7. Состав отправляется с пути, m=7, n=4
8. Доброго времени суток, m=6, n=4
9. Корабль пошел ко дну, m = 5, n = 4
10. Использование секретного ключа запрещено, m = 7, n = 6

3. Зашифровать текст методом шифрующих таблиц с одиночной перестановкой по ключу согласно варианту:
1. Это слово будет зашифровано, m=5, n=6, слово сапоги.
2. Я памятник себе воздвиг нерукотворный, m=7, n=6, слово август
3. Пусть всегда будет солнце, m=5, n=5, слово буква.
4. Криптография наука сложная, m=7, n=4, слово рога.
5. Погода сегодня хорошая, m=6, n=4, слово слон.
6. В Петербурге сегодня гроза, m=7, n=4, слово крот.
7. Состав отправляется с пути, m=7, n=4, слово муха.
8. Доброго времени суток, m=6, n=4, слово икра.
9. Корабль пошел ко дну, m = 5, n = 4, слово стол
10. Использование секретного ключа запрещено, m = 7, n = 6, слово пример

6.3.1.2. Примерные тестовые задания для текущего контроля

Задание 1
В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?
1988;
1991;
1994;
1997;
2002.
Задание 2.
Сколько уголовных дела по ст. ст. 272 и 165 УК РФ было возбуждено в 2003 г. в России?
6;
60;
160;

600;

1600.

Задание 3.

В стандарте США «Оранжевая книга» фундаментальное требование, которое относится к группе Стратегия:

индивидуальные субъекты должны идентифицироваться;

контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;

необходимо иметь явную и хорошо определенную систему обеспечения безопасности;

вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;

гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

Задание 4.

Сертификации подлежат:

средства криптографической защиты информации;

средства выявления закладных устройств и программных закладок;

защищенные технические средства обработки информации;

защищенные информационные системы и комплексы телекоммуникаций;

Задание 5.

Первый по времени открытый правовой нормативный акт, который регулировал вопросы оборота средств криптографической защиты информации, был принят в …

1989 г.

1991 г.

1993 г.

1995 г.

1997 г.

Задание 6.

Естественные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;

корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

Задание 7.

Искусственные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;

корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

Задание 8.

К основным непреднамеренным искусственным угрозам АСОИ относится:

физическое разрушение системы путем взрыва, поджога и т.п.;

неправомерное отключение оборудования или изменение режимов работы устройств и программ;

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

Задание 9.

К основным непреднамеренным искусственным угрозам АСОИ относится:

физическое разрушение системы путем взрыва, поджога и т.п.;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

Задание 10.

Активный перехват информации это – перехват, который:

заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

неправомерно использует технологические отходы информационного процесса;

осуществляется путем использования оптической техники;

осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Задание 11.

Пассивный перехват информации это – перехват, который:

заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

неправомерно использует технологические отходы информационного процесса;

осуществляется путем использования оптической техники;

осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Задание 12.

Хакер – это:

лицо, которое взламывает интрасеть в познавательных целях;

мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;

лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

плохой игрок в гольф, дилетант;

мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

Задание 13.

Фракер – это:

лицо, которое взламывает интрасеть в познавательных целях;

мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;

лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
плохой игрок в гольф, дилетант;
мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

Задание 14.

Кодификатор Генерального Секретариата Интерпола был интегрирован в автоматизированную систему поиска в …

1989 г.
1991 г.
1993 г.
1995 г.
1997 г.

Задание 15.

Преступление, обозначенное кодом QR , означает, что это …

несанкционированный доступ и перехват;
изменение компьютерных данных;
компьютерное мошенничество;
незаконное копирование;
компьютерный саботаж;
прочие компьютерные преступления.

Задание 16.

Спам, который распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

черный пиар;
фишинг;
нигерийские письма;
источник слухов;
пустые письма.

Задание 17.

Для взаимной проверки подлинности пользователей используются:

Механизм запроса-ответа
Механизм аутентификации
Механизм отметки времени ("временной штемпель")
Механизм регистрации
Алгоритмы шифрования

Задание 18.

Для исследования программы в статическом режиме используются:

Отладчики
Компиляторы
Дизассемблеры
Мониторы отладки

Задание 19.

Перечислите какие из перечисленных программ не являются отладчиками?

SoftIce
AFD
IDA
Turbo Debugger
DiskEdit

6.3.2. Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в форме зачета.

6.3.2.1. Типовые вопросы к зачету с оценкой

1. Необходимость защиты информации
2. Сохранность защищаемой информации: сущность и основные виды. Сущность понятия "защищаемая информация"
3. Разновидность защищаемой информации и ее носителей.
4. Компьютерные вирусы и их классификация
5. Характеристика антивирусного программного обеспечения
6. Способы ограничение доступа к информации
7. Методы взлома компьютерных систем. Атаки на уровне систем управления базами данных
8. Методы взлома компьютерных систем. Атаки на уровне операционной системы
9. Методы взлома компьютерных систем. Атаки на уровне сетевого программного обеспечения.
10. Методы взлома компьютерных систем. Защита системы от взлома.
11. Характеристика троянских программ. Возникновение троянских программ.
12. Характеристика троянских программ. Распознавание троянской программы.
13. Программные закладки и их классификация
14. Модели воздействия программных закладок на компьютеры
15. Защита системы от программных закладок. Разновидность ПЗ (имитаторы, фильтры и заместители).
16. Парольные взломщики. Защита системы от клавиатурных шпионов. Парольная защита операционных систем.
17. Взлом парольной защиты ОС UNIX
18. Взлом парольной защиты ОС Windows
19. Информационная безопасность компьютерной сети. Характеристика и назначение сканеров.
20. Информационная безопасность компьютерной сети. Защита от анализаторов протоколов.
21. Значение и современные методы шифрования информации в информационном обществе
22. Методологические основы технологии шифрования программными средствами.
23. Применение и проблемы стандартизации криптографических алгоритмов.
24. Средства безопасности ОС Windows. Понятия и термины защиты данных. Характеристики безопасности.
25. Средства безопасности ОС Windows. Применение шифрования с открытым и закрытым ключами.
26. Средства безопасности ОС Windows. Протокол аутентификации Kerberos. Основы применения протокола Kerberos.
27. Средства безопасности ОС Windows. Характеристика протоколов обмена сообщениями.
28. Аутентификация протокола Kerberos в доменах ОС Windows.
29. Средства безопасности ОС Windows. Применение EPS в ОС Windows.
30. Средства безопасности ОС Windows. Шифрование файлов и каталогов. Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок.
31. Средства безопасности ОС Windows. Архивация и восстановление зашифрованных файлов на другом компьютере
32. Средства безопасности ОС Windows. Восстановление данных зашифрованных с помощью неизвестного личного ключа.

33. Протокол безопасности IP в ОС Windows. Характеристика средств безопасности протокола IP.

34. Архитектура протокола безопасности IP в ОС Windows.

35. Администрирование безопасности в ОС Windows.

36. Использование сертификатов для обеспечения безопасности в ОС Windows. Хранилища сертификатов безопасности.

37. Планирование мероприятий по защите информации

38. Применение средства криптографической защиты информации Pretty good Privacy (PGP).

6.3.2.2 Итоговое тестирование

Задание 1

В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?

1988;
1991;
1994;
1997;
2002.

Задание 2.

Сколько уголовных дела по ст. ст. 272 и 165 УК РФ было возбуждено в 2003 г. в России?

6;
60;
160;
600;
1600.

Задание 3.

В стандарте США «Оранжевая книга» фундаментальное требование, которое относится к группе Стратегия:

индивидуальные субъекты должны идентифицироваться;

контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;

необходимо иметь явную и хорошо определенную систему обеспечения безопасности;

вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;

гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

Задание 4.

Сертификации подлежат:

средства криптографической защиты информации;

средства выявления закладных устройств и программных закладок;

защищенные технические средства обработки информации;

защищенные информационные системы и комплексы телекоммуникаций;

Задание 5.

Первый по времени открытый правовой нормативный акт, который регулировал вопросы оборота средств криптографической защиты информации, был принят в …

1989 г.
1991 г.
1993 г.
1995 г.
1997 г.

Задание 6.

Естественные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;

корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

Задание 7.

Искусственные угрозы безопасности информации вызваны:

деятельностью человека;

ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;

корыстными устремлениями злоумышленников;

ошибками при действиях персонала.

Задание 8.

К основным непреднамеренным искусственным угрозам АСОИ относится:

физическое разрушение системы путем взрыва, поджога и т.п.;

неправомерное отключение оборудования или изменение режимов работы устройств и программ;

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

Задание 9.

К основным непреднамеренным искусственным угрозам АСОИ относится:

физическое разрушение системы путем взрыва, поджога и т.п.;

чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

нелегальное внедрение и использование неучтенных программ игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения служебных обязанностей;

перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

Задание 10.

Активный перехват информации это – перехват, который:

заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

неправомерно использует технологические отходы информационного процесса;

осуществляется путем использования оптической техники;

осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Задание 11.

Пассивный перехват информации это – перехват, который:

заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

неправомерно использует технологические отходы информационного процесса;

осуществляется путем использования оптической техники;

осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

Задание 12.

Хакер – это:

лицо, которое взламывает интрасеть в познавательных целях;

мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;

лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

плохой игрок в гольф, дилетант;

мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

Задание 13.

Фракер – это:

лицо, которое взламывает интрасеть в познавательных целях;

мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;

лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;

плохой игрок в гольф, дилетант;

мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

Задание 14.

Кодификатор Генерального Секретариата Интерпола был интегрирован в автоматизированную систему поиска в …

1989 г.

1991 г.

1993 г.

1995 г.

1997 г.

Задание 15.

Преступление, обозначенное кодом QR , означает, что это …

несанкционированный доступ и перехват;

изменение компьютерных данных;

компьютерное мошенничество;

незаконное копирование;

компьютерный саботаж;

прочие компьютерные преступления.

Задание 16.

Спам, который распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

черный пиар;

фишинг;

нигерийские письма;

источник слухов;

пустые письма.

Задание 17.

Для взаимной проверки подлинности пользователей используются:

Механизм запроса-ответа

Механизм аутентификации

Механизм отметки времени ("временной штемпель")

Механизм регистрации

Алгоритмы шифрования

Задание 18.

Для исследования программы в статическом режиме используются:

Отладчики

Компиляторы

Дизассемблеры

Мониторы отладки

Задание 19.

Перечислите какие из перечисленных программ не являются отладчиками?

SoftIce

AFD

IDA

Turbo Debugger

DiskEdit

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

С целью определения уровня овладения компетенциями, закрепленными за дисциплиной, в заданные преподавателем сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося. Все виды текущего контроля осуществляются на практических занятиях. Исключение составляет устный опрос, который может проводиться в начале или конце лекции в течение 10-15 мин. с целью закрепления знаний терминологии по дисциплине. При оценке компетенций принимается во внимание формирование профессионального мировоззрения, определенного уровня включённости в занятия, рефлексивные навыки, владение изучаемым материалом.

Процедура оценивания компетенций обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки.

2. Многоступенчатость: оценка (как преподавателем, так и обучающимися группы) и самооценка обучающегося, обсуждение результатов и комплекс мер по устранению недостатков.

3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.

4. Соблюдение последовательности проведения оценки.

Текущая аттестация обучающихся.

Текущая аттестация по дисциплине «Информационная безопасность» проводится в форме опроса и контрольных мероприятий по оцениванию фактических результатов обучения обучающихся и осуществляется преподавателем дисциплины.

Объектами оценивания выступают:

1. учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

2. степень усвоения теоретических знаний в качестве «ключей анализа»;

3. уровень овладения практическими умениями и навыками по всем видам учебной работы;

4. результаты самостоятельной работы (изучение книг из списка основной и дополнительной литературы).

Активность обучающегося на занятиях оценивается на основе выполненных обучающимся работ и заданий, предусмотренных данной рабочей программой дисциплины.

Кроме того, оценивание обучающегося проводится на текущем контроле по дисциплине. Оценивание обучающегося на контрольной неделе проводится преподавателем независимо от

наличия или отсутствия обучающегося (по уважительной или неуважительной причине) на занятии. Оценка носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период.

Оценивание обучающегося носит комплексный характер и учитывает достижения обучающегося по основным компонентам учебного процесса за текущий период с выставлением оценок в ведомости.

Промежуточная аттестация обучающихся. Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в соответствии с учебным планом в виде зачета в период экзаменационной сессии в соответствии с графиком проведения.

Обучающиеся допускаются к зачету по дисциплине в случае выполнения им учебного плана по дисциплине: выполнения всех заданий и мероприятий, предусмотренных программой дисциплины.

Оценка знаний обучающегося на зачете определяется его учебными достижениями в семестровый период и результатами текущего контроля знаний и выполнением им заданий.

Знания умения, навыки обучающегося на зачете оцениваются как: «зачтено», «не зачтено».

Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная учебная литература:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022 — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — Режим доступа: https://www.iprbookshop.ru/97562.html .— ЭБС «IPRbooks»

б) дополнительная литература

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — Режим доступа: https://www.iprbookshop.ru/89453.html .— ЭБС «IPRbooks»

8. Методические указания для обучающихся по освоению дисциплины

Вид деятельности	Методические указания по организации деятельности студента
Лекция	Лекция – форма обучения студентов, при которой преподаватель последовательно излагает основной материал темы учебной дисциплины. Лекция – это важный источник информации по каждой учебной дисциплине. Она ориентирует студента в основных проблемах изучаемого курса, направляет самостоятельную работу над ним. Для лекций по каждому предмету должна быть отдельная тетрадь для лекций. Прежде всего, запишите имя, отчество и фамилию лектора, оставьте место для списка рекомендованной литературы, пособий, справочников. Будьте внимательны, когда лектор объявляет тему лекции, объясняет Вам место, которое занимает новый предмет в Вашей подготовке и чему новому Вы сможете научиться. Опытный студент знает, что, как правило, на первой лекции преподаватель обосновывает свои требования, раскрывает особенности чтения курса и способы сдачи зачета или экзамена. Отступите поля, которые понадобятся для различных пометок, замечаний и вопросов. Запись содержания лекций очень индивидуальна, именно поэтому

	трудно пользоваться чужими конспектами. Не стесняйтесь задавать вопросы преподавателю! Чем больше у Вас будет информации, тем свободнее и увереннее Вы будете себя чувствовать! Базовые рекомендации: - не старайтесь дословно конспектировать лекции, выделяйте основные положения, старайтесь понять логику лектора; - точно записывайте определения, законы, понятия, формулы и т.д.; - передавайте излагаемый материал лектором своими словами; - наиболее важные положения лекции выделяйте подчеркиванием; - создайте свою систему сокращения слов; - привыкайте просматривать, перечитывать перед новой лекцией предыдущую информацию; - дополняйте материал лекции информацией; - задавайте вопросы лектору; - обязательно вовремя восполняйте возникшие пробелы. Правила тактичного поведения и эффективного слушания на лекциях: - Слушать (и слышать) другого человека - это настоящее искусство, которое очень пригодится в будущей профессиональной деятельности экономиста. - Если преподаватель «скучный», но Вы чувствуете, что он действительно владеет материалом, то скука - это уже Ваша личная проблема (стоит вообще спросить себя, а настоящий ли Вы студент, если Вам не интересна лекция специалиста?). Существует очень полезный прием, позволяющий студенту-экономисту оставаться в творческом напряжении даже на лекциях заведомо «неинтересных» преподавателей. Прием прост – постарайтесь всем своим видом показать, что Вам «все-таки интересно» и Вы «все-таки верите», что преподаватель вот-вот скажет что-то очень важное. И если в аудитории найдутся хотя бы несколько таких студентов, внимательно и уважительно слушающих преподавателя, то может произойти «маленькое чудо», когда преподаватель «вдруг» заговорит с увлечением, начнет рассуждать смело и с озорством (иногда преподаватели сами ищут в аудитории внимательные и заинтересованные лица и начинают читать свои лекции, частенько поглядывая на таких студентов, как бы «вдохновляясь» их доброжелательным вниманием). Если это кажется невероятным (типа того, что «чудес не бывает»), просто вспомните себя в подобных ситуациях, когда с приятным собеседником-слушателем Вы вдруг обнаруживаете, что говорите намного увереннее и даже интереснее для самого себя. - Если Вы в чем-то не согласны с преподавателем, то совсем не обязательно тут же перебивать его и, тем более, высказывать свои представления, даже если они и кажутся Вам верными. Перебивание преподавателя на полуслове - это верный признак невоспитанности. Вопросы следует задавать либо после занятий (для этого их надо кратко записать, чтобы не забыть), либо выбрав момент, когда преподаватель сделал хотя бы небольшую паузу, и обязательно извинившись. Правила конспектирования на лекциях: - Не следует пытаться записывать подряд все то, о чем говорит преподаватель. Даже если студент владеет стенографией, записывать все высказывания просто не имеет смысла: важно уловить главную мысль и основные факты. - Желательно оставлять на страницах поля для своих заметок (и делать эти заметки либо во время самой лекции, либо при подготовке к семинарам и зачету). - Естественно, желательно использовать при конспектировании сокращения, которые каждый может «разработать» для себя самостоятельно (лишь бы самому легко было потом разобраться с этими сокращениями). - Стараться поменьше использовать на лекциях диктофоны, поскольку

	потом трудно будет «декодировать» неразборчивый голос преподавателя, все равно потом придется переписывать лекцию (а с голоса очень трудно готовиться к ответственным экзаменам), наконец, диктофоны часто отвлекают преподавателя тем, что студент ничего не делает на лекции (за него, якобы «работает» техника) и обычно просто сидит, глядя на преподавателя немигающими глазами (взглядом немного скучающего «удава»), а преподаватель чувствует себя неуютно и вместо того, чтобы свободно размышлять над проблемой, читает лекцию намного хуже, чем он мог бы это сделать (и это не только наши личные впечатления: очень многие преподаватели рассказывают о подобных случаях). .
Практические занятия	Практическое занятие – это одна из форм учебной работы, которая ориентирована на закрепление изученного теоретического материала, его более глубокое усвоение и формирование умения применять теоретические знания в практических, прикладных целях. Особое внимание на практических занятиях уделяется выработке учебных или профессиональных навыков. Такие навыки формируются в процессе выполнения конкретных заданий – упражнений, задач и т.п. – под руководством и контролем преподавателя. Готовясь к практическому занятию, тема которого всегда заранее известна, студент должен освежить в памяти теоретические сведения, полученные на лекциях и в процессе самостоятельной работы, подобрать необходимую учебную и справочную литературу. Только это обеспечит высокую эффективность учебных занятий. Отличительной особенностью практических занятий является активное участие самих студентов в объяснении вынесенных на рассмотрение проблем, вопросов; преподаватель, давая студентам возможность свободно высказаться по обсуждаемому вопросу, только помогает им правильно построить обсуждение. Такая учебная цель занятия требует, чтобы учащиеся были хорошо подготовлены к нему. В противном случае занятие не будет действенным и может превратиться в скучный обмен вопросами и ответами между преподавателем и студентами. При подготовке к практическому занятию: - проанализируйте тему занятия, подумайте о цели и основных проблемах, вынесенных на обсуждение; - внимательно прочитайте материал, данный преподавателем по этой теме на лекции; - изучите рекомендованную литературу, делая при этом конспекты прочитанного или выписки, которые понадобятся при обсуждении на занятии; - постарайтесь сформулировать свое мнение по каждому вопросу и аргументирование его обосновать; - запишите возникшие во время самостоятельной работы с учебниками и научной литературой вопросы, чтобы затем на практическом занятии получить на них ответы. В процессе работы на практическом занятии: - внимательно слушайте выступления других участников занятия, старайтесь соотнести, сопоставить их высказывания со своим мнением; - активно участвуйте в обсуждении рассматриваемых вопросов, не бойтесь высказывать свое мнение, но старайтесь, чтобы оно было подкреплено убедительными доводами; - если вы не согласны с чьим-то мнением, смело критикуйте его, но помните, что критика должна быть обоснованной и конструктивной, т.е. нести в себе какое-то конкретное предложение в качестве альтернативы; - после практического занятия кратко сформулируйте окончательный правильный ответ на вопросы, которые были рассмотрены. Практическое занятие помогает студентам глубоко овладеть предметом, способствует развитию у них умения самостоятельно работать с учебной литературой и первоисточниками, освоению ими методов научной

	работы и приобретению навыков научной аргументации, научного мышления. Преподавателю же работа студента на практическом занятии позволяет судить о том, насколько успешно и с каким желанием он осваивает материал курса.
Самостоятельная работа	Самостоятельная работа проводится с целью: систематизации и закрепления полученных теоретических знаний и практических умений обучающихся; углубления и расширения теоретических знаний студентов; формирования умений использовать нормативную, правовую, справочную документацию, учебную и специальную литературу; развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации; формирования профессиональных компетенций; развитию исследовательских умений обучающихся. Формы и виды самостоятельной работы: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым литературным источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; реферирование источников; составление аннотаций к прочитанным литературным источникам; составление рецензий и отзывов на прочитанный материал; составление обзора публикаций по теме; составление и разработка терминологического словаря; составление хронологической таблицы; составление библиографии (библиографической картотеки); подготовка к различным формам текущей и промежуточной аттестации (к тестированию, зачету, экзамену); выполнение домашних контрольных работ; самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, тесты; выполнение творческих заданий). Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов образовательного учреждения: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов, лабораторий и зала кодификации; компьютерные классы с возможностью работы в сети Интернет; аудитории (классы) для консультационной деятельности; учебную и учебно-методическую литературу, разработанную с учетом увеличения доли самостоятельной работы студентов, и иные методические материалы. Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Во время выполнения обучающимися внеаудиторной самостоятельной работы и при необходимости преподаватель может проводить индивидуальные и групповые консультации. Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся. Контроль самостоятельной работы предусматривает: • соотнесение содержания контроля с целями обучения; объективность контроля; • валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить); • дифференциацию контрольно-измерительных материалов. Формы контроля самостоятельной работы: • просмотр и проверка выполнения самостоятельной работы преподавателем; • организация самопроверки, • взаимопроверки выполненного задания в группе; обсуждение

	результатов выполненной работы на занятии; • проведение письменного опроса; • проведение устного опроса; • организация и проведение индивидуального собеседования; организация и проведение собеседования с группой; • защита отчетов о проделанной работе.
Опрос	Опрос - это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выявление объема знаний по определенному разделу, теме, проблеме и т.п. Проблематика, выносимая на опрос определена в заданиях для самостоятельной работы обучающегося, а также может определяться преподавателем, ведущим дисциплину. Во время проведения устного опроса обучающийся должен уметь обсудить с преподавателем соответствующую проблематику на уровне диалога.
Тестирование	Контроль в виде тестов может использоваться после изучения каждой темы курса. Итоговое тестирование можно проводить в форме: • компьютерного тестирования, т.е. компьютер произвольно выбирает вопросы из базы данных по степени сложности; • письменных ответов, т.е. преподаватель задает вопрос и дает несколько вариантов ответа, а обучающийся на отдельном листе записывает номера вопросов и номера соответствующих ответов. Для достижения большей достоверности результатов тестирования следует строить текст так, чтобы у обучающихся было не более 40 – 50 секунд для ответа на один вопрос. Итоговый тест должен включать не менее 40 вопросов по всему курсу. Значит, итоговое тестирование займет целое занятие. Оценка результатов тестирования может проводиться двумя способами: 1) по 5-балльной системе, когда ответы студентов оцениваются следующим образом: - «отлично» – более 80% ответов правильные; - «хорошо» – более 65% ответов правильные; - «удовлетворительно» – более 50% ответов правильные. Обучающиеся, которые правильно ответили менее чем на 70% вопросов, должны в последующем пересдать тест. При этом необходимо проконтролировать, чтобы вариант теста был другой; 2) по системе зачет-незачет, когда для зачета по данной дисциплине достаточно правильно ответить более чем на 70% вопросов.
Подготовка к зачету с оценкой	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др. Основное в подготовке к сдаче зачета по дисциплине «Информационная безопасность» - это повторение всего материала дисциплины, по которому необходимо сдавать зачет. При подготовке к сдаче зачета обучающийся весь объем работы должен распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнение намеченной работы. Подготовка к зачету включает в себя три этапа: • самостоятельная работа в течение семестра; • непосредственная подготовка в дни, предшествующие зачету по темам курса; • подготовка к ответу на задания, содержащиеся в билетах (тестах) зачета. Для успешной сдачи зачета по дисциплине «Организационное поведение» обучающиеся должны принимать во внимание, что: • все основные вопросы, указанные в рабочей программе, нужно знать, понимать их смысл и уметь его разъяснить; • указанные в рабочей программе формируемые компетенции в результате освоения дисциплины должны быть продемонстрированы студентом; • практические занятия способствуют получению более высокого

	• уровня знаний и, как следствие, более высокой оценке на зачете; • готовиться к зачету необходимо начинать с первой лекции и первого семинара.

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Реализация образовательного процесса по дисциплине «Информационная безопасность» осуществляется в следующих аудиториях:

1. Занятия лекционного типа - аудитория №503: 40 мест (20 столов, 40 стульев), 1 доска, 5 стендов, 1 стол преподавателя, 1 кафедра, вешалка напольная – 2 шт.

2. Для проведения практических занятий используется лаборатория для проведения практических занятий №404: 44 места (22 стола, 44 стула), 1 доска, 5 стендов, 1 кафедра, вешалка напольная – 1 шт, 12 ПЭВМ с выходом в Интернет, принтер – 1

3. Для самостоятельной работы студентов используется аудитория №506: 22 места (11 столов, 22 стула), 1 доска, 4 стенда, 1 кафедра, вешалка напольная – 1 шт, 10 ПЭВМ с выходом в Интернет, принтер - 1

4. Для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется аудитория для текущего контроля и промежуточной аттестации №503: 40 мест (20 столов, 40 стульев), 1 доска, 5 стендов, 1 стол преподавателя, 1 кафедра, вешалка напольная – 2 шт.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные систем

10.1 Лицензионное программное обеспечение:

1. Операционная система Microsoft Windows Professional XP
2. Операционная система Microsoft Windows Professional 7
3. Программные средства Microsoft Office 2007, 2010, 2013 Russian
4. Программные средства Microsoft Office Professional Plus 2007, 2013 Russian
5. Программные средства Microsoft Windows Server Standard 2008 Russian
6. Программные средства Total Commander 7.x User license
7. Программные средства WinRAR 3.x Standard license

10.2. Электронно-библиотечная система:

Электронная библиотечная система (ЭБС): http://www.iprbookshop.ru/

10.3. Современные профессиональные баз данных:

1. Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru
2. Портал "Информационно-коммуникационные технологии в образовании" http://www.ict.edu.ru
3. Научная электронная библиотека http://www.elibrary.ru/
4. Национальная электронная библиотека http://www.nns.ru/
5. Электронные ресурсы Российской государственной библиотеки http://www.rsl.ru/ru/root3489/all

6. Web of Science Core Collection — политематическая реферативно-библиографическая и наукомтрическая (библиометрическая) база данных — http://webofscience.com
7. Полнотекстовый архив ведущих западных научных журналов на российской платформе Национального электронно-информационного консорциума (НЭИКОН) http://neicon.ru

10.4. Информационные справочные системы:

1. Справочно-правовая система «КонсультантПлюс»
2. Справочная правовая система «Гарант»

Рабочую программу дисциплины составил:

Гришанова Татьяна Валерьевна, старший преподаватель кафедры информатики и программного обеспечения Частного образовательного учреждения высшего образования «Брянский институт управления и бизнеса».

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры информатики и программного обеспечения

протокол № 1 от «29» августа 2024г.

Заведующий кафедрой _____ /Т.М. Хвостенко/