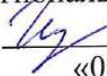


Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косогорова Людмила Алексеевна
Должность: Ректор
Дата подписания: 13.07.2023 10:35:35
Уникальный программный ключ:
4a47ce4135cc0671229e80c031ce72a914b0b6b4



**Частное образовательное учреждение высшего образования
«ИНСТИТУТ УПРАВЛЕНИЯ, БИЗНЕСА И ТЕХНОЛОГИЙ»**

Секция «Прикладной информатики и математики»

УТВЕРЖДАЮ:
Проректор по учебной работе и
региональному развитию
 Шульман М.Г.
«05» июля 2023 г.

Рабочая программа учебной дисциплины

Информационная безопасность

Направление подготовки

09.03.03 Прикладная информатика

Направленность (профиль) подготовки:

Прикладная информатика в экономике

Квалификация (степень) выпускника:

Бакалавр

Форма обучения:

Очная, очно-заочная, заочная

Составитель программы:
Левинзон В.С., к.т.н., доцент,
зав. кафедрой «Менеджмент»

Калуга
2023

СОДЕРЖАНИЕ

1.	Аннотация к дисциплине.....	3
2.	Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы.....	4
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.....	5
3.1.	Объем дисциплины по видам учебных занятий (в часах).....	5
4.	Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.....	5
4.1.	Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах).....	5
4.2.	Содержание дисциплины, структурированное по разделам для очной формы обучения (для очно – заочной и заочной формы обучения в соответствии с .4.1).....	7
5.	Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	9
6.	Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине	10
6.1.	Описание показателей и критериев оценивания компетенций, описание шкал оценивания.....	10
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.....	11
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.....	14
6.3.1.	Типовые задания для проведения текущего контроля обучающихся.....	14
6.3.2.	Типовые задания для проведения промежуточной аттестации обучающихся.....	18
6.4.	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.....	23
7.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	25
8.	Методические указания для обучающихся по освоению дисциплины.....	25
9.	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	29
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 системы.....	30
10.1.	Лицензионное программное обеспечение.....	30
10.2.	Электронно-библиотечная система.....	30
10.3.	Современные профессиональные базы данных.....	30
10.4.	Информационные справочные системы.....	31
11.	Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.....	31

1. Аннотация к дисциплине

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 «Прикладная информатика», утвержденного Приказом Министерства образования и науки Российской Федерации от 19 сентября 2017г. № 922. Данная дисциплина в соответствии с учебным планом института является обязательной для изучения.

Место дисциплины в структуре основной профессиональной образовательной программы:

Настоящая дисциплина является частью Технологического модуля, включена в обязательную часть Блока1 учебных планов по направлению подготовки 09.03.03 Прикладная информатика, уровень бакалавриата.

Для изучения дисциплины, необходимы знания и умения из дисциплин, изучаемых ранее по учебному плану. Согласно учебному плану дисциплина «Информационная безопасность» изучается на 3 курсе в 5 семестре для очной формы обучения, на 4 курсе в 7 семестре для очно-заочной формы обучения и на 3 курсе в 6 семестре для заочной формы обучения, форма контроля – экзамен и курсовая работа.

Цель изучения дисциплины: в ознакомлении с комплексом проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов.

Задачи изучения дисциплины:

- а) овладение теоретическими, практическими и методическими вопросами классификации угроз информационным ресурсам;
- б) ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации;
- в) изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи;
- г) приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;
- д) 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:

ПК-2. Способен осуществлять проектирование программного обеспечения ИС и разрабатывать техническую документацию на его компоненты.

ПК-3. Способен вводить в эксплуатацию и осуществлять сопровождение ИС на всех этапах ее жизненного цикла, включая ее презентацию и начальное обучение пользователей.

УК-10. Способен формировать нетерпимое отношение к коррупционному поведению

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 по направлению подготовки 09.03.03 «Прикладная информатика, профиль «Прикладная информатика в экономике» с учетом требований предъявляемых к выпускнику на основе Федерального закона от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации», Федерального государственного образовательного стандарта высшего образования к уровню высшего образования бакалавр, утвержденного приказом Минобрнауки России от 19 сентября 2017 г. № 922; на основе профессионального стандарта «Специалист по информационным системам», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н (с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. № 727н).

Код компетенции	Результаты освоения ОПОП (содержание компетенций)	Индикаторы достижения компетенций	Формы образовательной деятельности, способствующие формированию и развитию компетенции
ПК-2.	Способен осуществлять проектирование программного обеспечения ИС и разрабатывать техническую документацию на его компоненты	<p>ПК-2.1. Способен использовать современные языки и системы программирования, технологии проектирования программного обеспечения.</p> <p>ПК-2.2. Способен сформулировать требования к разрабатываемому программному обеспечению, выполнить его реализацию и оформить техническую документацию на его компоненты.</p> <p>ПК-2.3. Способен осуществлять проектирование программного обеспечения конкретной ИС и разработку технической документации на ее компоненты.</p>	<p><u>Контактная работа:</u> Лекции Практические занятия <u>Самостоятельная работа</u> <u>Курсовая работа</u></p>
ПК-3.	Способен вводить в эксплуатацию и осуществлять сопровождение ИС на всех этапах ее жизненного цикла, включая ее презентацию и начальное обучение пользователей	<p>ПК-3.1. Способен использовать знания методологических и технических основ ввода ИС в эксплуатацию.</p> <p>ПК-3.2. Способен организовать репозиторий хранения данных о создании ИС, вводе ее в эксплуатацию и модификации в процессе жизненного цикла.</p> <p>ПК-3.3. Способен осуществлять инсталляцию программного обеспечения ИС, его тестирование и начальное обучение пользователей.</p>	<p><u>Контактная работа:</u> Лекции Практические занятия <u>Самостоятельная работа</u> <u>Курсовая работа</u></p>

УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1. Знает понятие и признаки коррупции, направления противодействия коррупции, сущность профессиональной деформации. УК-10.2. Выявляет и дает оценку коррупционного поведения и содействует его пресечению. УК-10.3. Владеет нетерпимым отношением к коррупционному поведению, уважительным отношением к праву и закону.	<u>Контактная работа:</u> Лекции Практические занятия <u>Самостоятельная работа</u> <u>Курсовая работа</u>
-------	--	---	--

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 5 зачетных единиц.

3.1 Объем дисциплины по видам учебных занятий (в часах)

Объем дисциплины	Всего часов		
	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость дисциплины	180		
Контактная работа обучающихся с преподавателем (всего)	54	20	18
Аудиторная работа (всего):	54	20	18
в том числе:			
Лекции	18	8	6
семинары, практические занятия	36	12	12
лабораторные работы			
Внеаудиторная работа (всего):	108	151	153
в том числе:			
Самостоятельная работа обучающихся (всего)	108	151	153
Вид промежуточной аттестации обучающегося – экзамен и курсовая работа	18	9	9

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

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

для очной формы обучения

№ п/п	Разделы и темы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации <i>(по семестрам)</i>	
			Всего	Из них аудиторные занятия			Самостоятельная работа	Контрольная работа		Курсовая работа
				Лекции	Практикум. Лаборатор	Практическ.занятия /семинары				
1	Концепция информационной безопасности.	5	32,4	3,6		7,2	21,6			Опрос
2	Угрозы информации	5	32,4	3,6		7,2	21,6			Коллоквиум
3	Виды возможных нарушений информационной системы	5	32,4	3,6		7,2	21,6			Опрос
4	Информационная безопасность информационных систем	5	32,4	3,6		7,2	21,6			Коллоквиум
5	Методы и средства защиты компьютерной информации	5	32,4	3,6		7,2	21,6			Опрос
	Экзамен и курсовая работа	5	18							экзамен и курсовая работа
	ИТОГО		180	18		36	108			18 (экзамен и курсовая работа)

для очно-заочной формы обучения

№ п/п	Разделы и темы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Вид оценочного средства текущего контроля успеваемости, промежуточной аттестации <i>(по семестрам)</i>	
			Всего	Из них аудиторные занятия			Самостоятельная работа	Контрольная работа		Курсовая работа
				Лекции	Практикум. Лаборатор	Практическ.занятия /семинары				
1	Концепция информационной безопасности.	7	34,2	1,6		2,4	30,2			Опрос

2	Угрозы информации	7	34,2	1,6		2,4		30,2		Коллоквиум
3	Виды возможных нарушений информационной системы	7	34,2	1,6		2,4		30,2		Опрос
4	Информационная безопасность информационных систем	7	34,2	1,6		2,4		30,2		Коллоквиум
5	Методы и средства защиты компьютерной информации	7	34,2	1,6		2,4		30,2		Опрос
	Экзамен и курсовая работа	7	9							экзамен и курсовая работа
	ИТОГО		180	8		12		151		9 (экзамен и курсовая работа)

для заочной формы обучения

№ п/п	Разделы и темы 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			Самостоятельная работа	Контрольная работа	Курсовая работа	
				Лекции	Практикум. Лаборатор	Практическ.занятия /семинары				
1	Концепция информационной безопасности.	6	34,2	1,2		2,4		30,6		Опрос
2	Угрозы информации	6	34,2	1,2		2,4		30,6		Коллоквиум
3	Виды возможных нарушений информационной системы	6	34,2	1,2		2,4		30,6		Опрос
4	Информационная безопасность информационных систем	6	34,2	1,2		2,4		30,6		Коллоквиум
5	Методы и средства защиты компьютерной информации	6	34,2	1,2		2,4		30,6		Опрос
	Экзамен и курсовая работа	6	9							экзамен и курсовая работа
	ИТОГО		180	6		12		153		9 (экзамен и курсовая работа)

4.2 Содержание дисциплины, структурированное по разделам для очной формы обучения (для очно – заочной и заочной формы обучения- в соответствии с п.4.1)

Раздел 1. Концепция информационной безопасности.

Тема №1. Актуальность информационной безопасности.

Национальные интересы РФ в информационной сфере и их обеспечение. Основные

нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Тема №2. Лицензирование и сертификация в области защиты информации.

Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования.

Тема №3. Основные нормативные руководящие документы. Международные стандарты информационного обмена. Критерии безопасности компьютерных систем. «Оранжевая книга». Руководящие документы Гостехкомиссии.

Раздел 2. Угрозы информации.

Тема №4. Информационная безопасность сетей.

Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ.

Тема №5. Способы совершения компьютерных преступлений.

Тема №6. Уязвимость сети Интернет.

Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.

Раздел 3. Виды возможных нарушений информационной системы.

Тема №7. Компьютерные преступления.

Классификация компьютерных преступлений. Виды противников или «нарушителей».

Тема №8. Вредоносные программы.

Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам.

Тема №9. Вирусы.

Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.

Раздел 4. Информационная безопасность информационных систем.

Тема №10. Теория информационной безопасности информационных систем.

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Тема №11. Криптографические способы защиты информации.

Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись.

Тема №12. Организация информационной безопасности компании. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.

Раздел 5. Методы и средства защиты компьютерной информации.

Тема №13. Обеспечения информационной безопасности.

Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре.

Тема №14. Контроль доступа к информации.

Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта).

Тема №15. Методы и средства защиты информации.

Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите

информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.

Тема №16. Антивирусное ПО.

Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

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

Самостоятельная работа представляет собой обязательную часть основной образовательной программы и выполняемую обучающимся внеаудиторных занятий в соответствии с заданиями преподавателями.

Выполнение этой работы требует инициативного подхода, внимательности, усидчивости, активной мыслительной деятельности. Основу самостоятельной работы составляет деятельностный подход, когда цели обучения ориентированы на формирование умений решать типовые и нетиповые задачи, которые могут возникнуть в будущей профессиональной деятельности, где студентам предстоит проявить творческую и социальную активность, профессиональную компетентность и знание конкретной дисциплины. Результат самостоятельной работы контролируется преподавателем по дисциплине.

Наименование темы	Дополнение - вопросы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Учебно-методическое обеспечение	Форма контроля
Концепция информационной безопасности.	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме, работа с интернет источниками	Опрос
Угрозы информации	Угрозы информационной безопасности для АСОИ	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме, работа с интернет источниками	Коллоквиум
Виды возможных нарушений информационной системы	Хакерские утилиты и прочие вредоносные программы.	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме, работа с интернет источниками	Опрос
Информационная безопасность информационных систем	Методы криптографии.	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме, работа с интернет источниками	Коллоквиум
Методы и средства защиты компьютерной информации	Источники компьютерных вирусов	Работа в библиотеке, включая ЭБС. Дидактическое тестирование	Литература к теме, работа с интернет источниками	Опрос

6. Оценочные материалы для проведения 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	<p>«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.</p> <p>«Не зачтено» - имеются существенные пробелы в знании основного материала по разделу, а также допущены принципиальные ошибки при изложении материала.</p>	УК-10, ПК-2, ПК-3
2	Доклад-презентация	Публичное выступление по представлению полученных результатов в программе Microsoft PowerPoint	<p>«5» – 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;</p> <p>«4» – некорректное оформление презентации, грамотное использование терминологии, в основном свободное изложение рассматриваемых проблем, докладчик частично правильно ответил на все вопросы в ходе дискуссии;</p> <p>«3» – отсутствие презентации, докладчик</p>	УК-10. ПК-2, ПК-3

			испытывал затруднения при выступлении и ответе на вопросы в ходе дискуссии; «2» - докладчик не раскрыл тему	
3	Коллоквиум	Беседа преподавателя с учащимися на определенную тему из учебной программы	«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 основного материала по разделу, а также допущены принципиальные ошибки при изложении материала.	УК-10, ПК-2, ПК-3
4	Тестирование	Тестирование можно проводить в форме: <ul style="list-style-type: none"> • 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%.	УК-10, ПК-2, ПК-3

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

№ п/п	Форма контроля/ коды оцениваемых компетенций	Процедура оценивания	Шкала и критерии оценки, балл
1.	Экзамен –	Правильность ответов на	оценка «отлично» - обучающийся должен

	УК-10, ПК-2, ПК-3	<p>все вопросы (верное, четкое и достаточно глубокое изложение идей, понятий, фактов и т.д.);</p> <p>Сочетание полноты и лаконичности ответа;</p> <p>Наличие практических навыков по дисциплине (решение задач или заданий);</p> <p>Ориентирование в учебной, научной и специальной литературе;</p> <p>Логика и аргументированность изложения;</p> <p>Грамотное комментирование, приведение примеров, аналогий;</p> <p>Культура ответа.</p>	<p>дать полные, исчерпывающие ответы на вопросы экзаменационного билета, 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;</p> <p>оценка «хорошо» - обучающийся должен дать полные ответы на вопросы, указанные в экзаменационном билете. 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. 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;</p> <p>оценка «удовлетворительно» - обучающийся должен в целом дать ответы на вопросы, предложенные в экзаменационном билете, ориентироваться в системе дисциплины «Информационная безопасность», знать основные категории предмета. Оценка «удовлетворительно» предполагает, что материал в основном изложен грамотным языком;</p> <p>оценка «неудовлетворительно» предполагает, что обучающимся либо не дан ответ на вопрос билета, либо обучающийся не знает основных категорий, не может определить предмет дисциплины.</p>
2.	Тестирование (на экзамене) – УК-10, ПК-2, ПК-3	<p>Полнота знаний теоретического контролируемого материала.</p> <p>Количество правильных ответов</p>	<p>«отлично» - процент правильных ответов 80-100%;</p> <p>«хорошо» - процент правильных ответов 65-79,9%;</p> <p>«удовлетворительно» - процент правильных ответов 50-64,9%;</p> <p>«неудовлетворительно» - процент правильных ответов менее 50%.</p>
3.	Курсовая работа	<p>Выполняется в письменной форме. При оценке курсовой работы учитывается:</p> <ol style="list-style-type: none"> 1. Правильность оформления курсовой работы 2. Уровень 	<p>«отлично» - содержание работы полностью раскрывает утвержденную тему и соответствует квалификационным требованиям, предъявляемым к подобного рода работам, выполненная работа свидетельствует о знании основных теоретических концепций, монографий по</p>

		<p>сформированности компетенций. 3. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей. 4. Уровень знания фактического материала в объеме программы. 5. Логика, структура и грамотность изложения письменной работы. 6. Умение связать теорию с практикой. 7. Умение делать обобщения, выводы.</p>	<p>рассматриваемой проблеме (их авторов и источников, в которых они изложены), теоретические выводы и практические предложения автора соответствуют сформулированным во введении задачам, вытекают из содержания работы и основываются на законодательных и иных нормативно-правовых актах, в работе в полной мере использованы современные литературные источники, в работе обобщены данные эмпирического исследования автора, собранные в конкретном органе, учреждении, в работе применены адекватные гипотезам методы научных исследований, оформление работы соответствует установленным требованиям, по теме работы студент имеет научные публикации или выступления на конференции, студент грамотно выступает на защите, убедительно отвечает на вопросы комиссии.</p> <p>«хорошо» - содержание работы раскрывает утвержденную тему и соответствует квалификационным требованиям, предъявляемым к такого рода работам по специальности, выполненная работа свидетельствует о знании основных теоретических концепций, монографий по рассматриваемой проблеме (их авторов и источников, в которых они изложены), другой учебной литературы, теоретические выводы, практические предложения по повышению эффективности деятельности органа, учреждения основываются на законодательных и иных нормативно-правовых актах, в работе использованы современные литературные источники, обобщенные данные эмпирического исследования автора, собранные в конкретном органе, учреждении, в работе применены адекватные гипотезам методы математической обработки, выводы и предложения автора соответствуют сформулированным во введении задачам и вытекают из содержания работы, оформление работы соответствует установленным требованиям, в работе имеются отдельные упущения в изложении некоторых вопросов, в оформлении полученных результатов, студент грамотно выступает на защите, убедительно отвечает на вопросы комиссии</p> <p>«удовлетворительно» - содержание работы не полностью раскрывает утвержденную тему, но, вместе с тем, соответствует квалификационным требованиям, предъявляемым к подобного рода работам по специальности, выполненная работа</p>
--	--	---	--

			<p>свидетельствует о недостаточном знании автором основных теоретических концепций, монографий по рассматриваемой проблеме, другой учебной литературы, теоретические выводы, практические предложения по повышению эффективности деятельности органа, учреждения основываются на законодательных и иных нормативно-правовых актах, статистическая обработка выполнена не полностью или неадекватно подобраны методы математической обработки, выводы и предложения автора не полностью соответствуют сформулированным во введении задачам и не вытекают из содержания работы, имеются незначительные нарушения требований по оформлению работы, студент, выступая на защите, отвечает не на все вопросы комиссии.</p> <p>«неудовлетворительно» - содержание работы не раскрывает утвержденную тему, выполненная работа свидетельствует о незнании автором основных теоретических концепций, монографий по рассматриваемой проблеме, другой учебной литературы, а также нормативно-правовых актов, в работе отсутствуют теоретические выводы, практические предложения, нет ссылок на используемые источники, отсутствуют материалы эмпирического исследования автора, не использованы методы математической статистики, работа оформлена с нарушением требований, предъявляемых к работам данного вида, студент, выступая на защите, не отвечает на вопросы комиссии.</p>
--	--	--	---

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. Примерные тестовые задания для текущего контроля

Примерная тематика реферативных обзоров

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.

10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
12. Виды угроз безопасности информации.
13. Основные принципы добывания информации.
14. Процедура идентификации, как основа процесса обнаружения объекта.
15. Методы синтеза информации.
16. Методы несанкционированного доступа к информации.
17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
18. Способы наблюдения с использованием технических средств.

Примерные тестовые задания

1. Задание.

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

1. 1988;
2. 1991;
3. 1994;
4. 1997;
5. 2002.

2. Задание.

Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

3. Задание.

В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. Задание.

Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

5. Задание.

Хакер – это:

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

6. Задание.

Активный перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

7. Задание.

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

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

8. Задание.

По среде обитания классические вирусы разделяются:

1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.

9. Задание.

Шифрование методом подстановки:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, затыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

10. Задание.

Метод защиты информации ограничение доступа заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;

3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

11. Задание.

Перехват, который неправомерно использует технологические отходы информационного процесса, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. Задание.

Спам, периодически проводящий рассылки не рекламных сообщений:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

13. Задание.

Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от ...

1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;
4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.

14. Задание.

Попытка одного субъекта выдать себя за другого - это:

1. пассивная атака;
2. модификация потока данных»
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.

15. Задание.

В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить:

1. должностное лицо;
2. терминал;
3. распечатка;
4. форма и размеры лица;
5. оператор.

16. Задание.

Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;

5. сторож.

6.3.2. Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в форме экзамена и защиты курсовой работы.

Примерная тематика курсовых работ

1. Блок защиты информации каналов управления автоматизированной системы спутниковой связи
2. Внедрение системы обнаружения вторжений в ...
3. Выбор технологии проектирования систем защиты информации
4. Защита информации при использовании электронной почты.
5. Защита от SQL атак
6. ЗКИ. Получение лицензии. Возможности лицензиата
7. Имитация многолучевого канала на основе IEEE 802.11b
8. Информационная безопасность предприятия...
9. Использование стандарта IEEE 802.1x на предприятии для защиты от несанкционированного доступа»
10. Использование системы TOR при ведении двойной бухгалтерии
11. Исследование ошибок к операционных системах
12. Комплексная защита информации на предприятии ...
13. Комплексная защита информации на примере какого-нибудь предприятия...
14. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему
15. Комплексный подход к обеспечению защиты конфиденциальной информации в компании ...
16. Концепция политики безопасности и систем контроля доступа для локальных вычислительных сетей.
17. Модель системы управления информационной безопасностью в условиях неопределенности воздействия
18. Модернизация комплекса антивирусной защиты ...
19. Обеспечение информационной безопасности в ...
20. Организация защиты персональных данных в ...
21. Организация защиты персональных данных в организации
22. Организация порядка установления внутриобъектного спецрежима на объекте информатизации ...
23. Организация противодействия угрозам безопасности персонала организации на примере ...
24. Основные направления, принципы и методы обеспечения информационной безопасности
25. Построение типовой модели угроз безопасности информации кредитной организации...
26. Проблемы информационной безопасности банков.
27. Разработка алгоритма и программного обеспечения маскирования данных, исследование вопросов стойкости к частотному анализу
28. Разработка комплекса режимных мероприятий по сохранности конфиденциальной информации на примере ...
29. Разработка комплексной защиты информации
30. Разработка комплексной системы защиты коммерческой информации.
31. Разработка корпоративной сети авиапредприятия с подключением удаленных филиалов по каналам VPN

32. Разработка мер по технической защите конфиденциальной информации в организации...
33. Разработка политики безопасности ...
34. Разработка политики информационной безопасности.
35. Разработка предложений по созданию системы защиты информации в локальной вычислительной сети ...
36. Разработка проекта по созданию защищенной корпоративной сети с применением технологий VPN
37. Разработка системы защиты информации предприятия на примере ...
38. Разработка системы защиты конфиденциальной информации в процессинговой компании
39. Разработка системы защиты персональных данных в предприятии...
40. Разработка системы информационной безопасности банка
41. Разработка системы управления кадровой безопасностью организации
42. Разработка средств защиты информации на предприятии ...
43. Разработка типового проекта защиты локальной вычислительной сети предприятия
44. Система защиты персональных данных на предприятии
45. Система обеспечения защиты информации в переговорной комнате ...
46. Системы управления обменными пунктами валют. организация защиты баз данных
47. Создание Концепции ИБ
48. Создание службы безопасности на предприятии.
49. Средства и способы защиты информации по ПЭМИН, аттестация объектов, помещений и информ.систем.
50. ЭЦП (проблемы использования и применения в России и т.п.)

Типовые вопросы к экзамену

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 ограничения доступа к информации.
7. Предотвращение технических сбоев оборудования.
8. Методы взлома компьютерных систем. Атаки на уровне систем управления базами данных.
9. Методы взлома компьютерных систем. Атаки на уровне операционной системы.
10. Методы взлома компьютерных систем. Атаки на уровне сетевого программного обеспечения.
11. Методы взлома компьютерных систем. Защита системы от взлома.
12. Характеристика троянских программ. Возникновение троянских программ.
13. Характеристика троянских программ. Где и как часто встречаются троянские программы.
14. Характеристика троянских программ. Распознавание троянской программы.
15. Программные закладки и их классификация.
16. Модели воздействия программных закладок на компьютеры.
17. Защита системы от программных закладок.
18. Разновидность ПЗ (имитаторы, фильтры и заместители).
19. Парольные взломщики. Защита системы от клавиатурных шпионов. Парольная защита операционных систем.

20. Взлом парольной защиты ОС UNIX.
21. Взлом парольной защиты ОС Windows NT.
22. Информационная безопасность компьютерной сети. Характеристика и назначение сканеров.
23. Информационная безопасность компьютерной сети. Характеристика и назначение анализаторов протоколов
24. Информационная безопасность компьютерной сети. Защита от анализаторов протоколов.
25. Значение и современные методы шифрования информации в информатизированном обществе
26. Методологические основы технологии шифрования программными средствами.
27. Применение и проблемы стандартизации криптографических алгоритмов.
28. Средства безопасности ОС Windows 2003. Понятия и термины защиты данных. Характеристики безопасности.
29. Средства безопасности ОС Windows 2003. Применение шифрования с открытым и закрытым ключами.
30. Средства безопасности ОС Windows 2003. Алгоритмы и компоненты Windows 2003 обеспечивающие шифрование данных.
31. Средства безопасности ОС Windows 2003. Протокол аутентификации Kerberos. Основы применения протокола Kerberos.
32. Средства безопасности ОС Windows 2003. Характеристика протоколов обмена сообщениями.
33. Аутентификация протокола Kerberos в доменах ОС Windows 2003.
34. Шифрующая файловая система EPS и ее архитектура.
35. Средства безопасности ОС Windows 2003. Применение EPS в ОС Windows 2003.
36. Средства безопасности ОС Windows 2003. Шифрование файлов и каталогов. Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок.
37. Средства безопасности ОС Windows 2003. Архивация и восстановление зашифрованных файлов на другом компьютере.
38. Средства безопасности ОС Windows 2003. Восстановление данных зашифрованных с помощью неизвестного личного ключа.
39. Протокол безопасности IP в ОС Windows 2003. Характеристика средств безопасности протокола IP.
40. Архитектура протокола безопасности IP в ОС Windows 2003.
41. Разработка плана безопасности IP в ОС Windows 2003.
42. Администрирование безопасности в ОС Windows 2003.
43. Использование сертификатов для обеспечения безопасности в ОС Windows 2003. Хранилища сертификатов безопасности.
44. Планирование мероприятий по защите информации.
45. Характеристика программных средств шифрования информации.
46. Применение средства криптографической защиты информации Pretty good Privacy (PGP).

Типовые тестовые задания для проведения промежуточной аттестации

1. Задание.

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

1. 1988;
2. 1991;
3. 1994;

4. 1997;

5. 2002.

2. Задание.

Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

3. Задание.

В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. Задание.

Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

5. Задание.

Хакер – это:

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

6. Задание.

Активный перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

7. Задание.

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

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

8. Задание.

По среде обитания классические вирусы разделяются:

1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.

9. Задание.

Шифрование методом подстановки:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

10. Задание.

Метод защиты информации ограничение доступа заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

11. Задание.

Перехват, который неправомерно использует технологические отходы информационного процесса, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. Задание.

Спам, периодически проводящий рассылки не рекламных сообщений:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;

5. пустые письма.

13. Задание.

Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от ...

1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;
4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.

14. Задание.

Попытка одного субъекта выдать себя за другого - это:

1. пассивная атака;
2. модификация потока данных»
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.

15. Задание.

В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить:

1. должностное лицо;
2. терминал;
3. распечатка;
4. форма и размеры лица;
5. оператор.

16. Задание.

Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

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 15-20 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 обучающихся по дисциплине «Информационная безопасность» проводится в соответствии с локальными нормативными актами ЧОУ ВО «ИНУПБТ» и является обязательной.

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 обучающихся по дисциплине «Информационная безопасность» проводится в соответствии с локальными нормативными актами ЧОУ ВО «ИНУПБТ» и является обязательной.

Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в соответствии с учебным планом на 3 курсе в 5 семестре для очной формы обучения; на 4 курсе в 7 семестре для очно-заочной формы обучения, на 3 курсе в 6 семестре для заочной формы обучения в виде экзамена и защиты курсовой работы в период зачетно-экзаменационной сессии в соответствии с графиком проведения.

Обучающиеся допускаются к экзамену и защите курсовой работы по дисциплине в случае выполнения ими учебного плана по дисциплине: выполнения всех заданий и мероприятий, предусмотренных программой дисциплины.

Оценка знаний обучающегося на экзамене и защите курсовой работы определяется его учебными достижениями в семестровый период и результатами текущего контроля знаний и выполнением им заданий.

Знания умения, навыки обучающегося на экзамене оцениваются как: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Знания умения, навыки обучающегося на защите курсовой работы оцениваются как: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/108227.html>
2. Информационная безопасность. Практические аспекты : учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург: Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст: электронный// Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/103997.html>
3. Суворова, Г. М. Информационная безопасность: учебное пособие/ Г. М. Суворова. — Саратов: Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/86938.html>
4. Шаньгин, В. Ф. Информационная безопасность и защита информации/ В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/87995.html>

б) дополнительная учебная литература

1. Информационная безопасность: учебное пособие/ Кирколуп сост., Е. М. Скурыдина. — Барнаул: Алтайский государственный педагогический университет, 2017. — 313 с. — ISBN 978-5-88210-898-3. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/102889.html>
2. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие/ А. В. Моргунов. — Новосибирск: Новосибирский государственный технический университет, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/98708.html>
3. Бахаров, Л. Е. Информационная безопасность и защита информации (разделы криптография и стеганография): практикум/ Л. Е. Бахаров. — Москва: Издательский Дом МИСиС, 2019. — 59 с. — ISBN 978-5-906953-94-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/98171.html>
4. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с. — ISBN 978-5-4486-0485-0. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <https://www.iprbookshop.ru/80290.html>

8. Методические указания для обучающихся по освоению дисциплины

Вид деятельности	Методические указания по организации деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и

	<p>задачам, структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Прослушивание аудио- и видеозаписей по заданной теме, решение расчетно-графических заданий, решение задач по алгоритму и др.</p>
Индивидуальные задания	<p>Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.</p>
Самостоятельная работа	<p>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</p>

	<p>работы, уровня сложности, уровня умений обучающихся. Контроль самостоятельной работы предусматривает:</p> <ul style="list-style-type: none"> • соотнесение содержания контроля с целями обучения; • объективность контроля; • валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить); • дифференциацию контрольно-измерительных материалов. <p>Формы контроля самостоятельной работы:</p> <ul style="list-style-type: none"> • 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	<p>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 семинарские занятия. Во время проведения опроса обучающийся должен уметь обсудить с преподавателем соответствующую проблематику на уровне диалога.</p>
Коллоквиум	<p>Коллоквиум (от латинского colloquium – разговор, беседа) – одна из форм учебных занятий, беседа преподавателя с учащимися на определенную тему из учебной программы. Цель проведения коллоквиума состоит в выяснении уровня знаний, полученных учащимися в результате прослушивания лекций, посещения семинаров, а также в результате самостоятельного изучения материала. В рамках поставленной цели решаются следующие задачи:</p> <ul style="list-style-type: none"> • выяснение качества и степени понимания учащимися лекционного материала; • развитие и закрепление навыков выражения учащимися своих мыслей; • расширение вариантов самостоятельной целенаправленной подготовки учащихся; • развитие навыков обобщения различных литературных источников; • предоставление возможности учащимся сопоставлять разные точки зрения по рассматриваемому вопросу. <p>В результате проведения коллоквиума преподаватель должен иметь представление:</p> <ul style="list-style-type: none"> • о качестве лекционного материала; • о сильных и слабых сторонах своей методики чтения лекций; • о сильных и слабых сторонах своей методики проведения семинарских занятий; • об уровне самостоятельной работы учащихся; • об умении обучающихся вести дискуссию и доказывать свою точку зрения; • о степени эрудированности учащихся; • о степени индивидуального освоения материала конкретными обучающимися.

	<p>В результате проведения коллоквиума обучающийся должен иметь представление:</p> <ul style="list-style-type: none"> • об уровне своих знаний по рассматриваемым вопросам в соответствии с требованиями преподавателя и относительно других студентов группы; • о недостатках самостоятельной проработки материала; • о своем умении излагать материал; • о своем умении вести дискуссию и доказывать свою точку зрения. <p>В зависимости от степени подготовки группы можно использовать разные подходы к проведению коллоквиума. В случае, если большинство группы с трудом воспринимает содержание лекций и на практических занятиях демонстрирует недостаточную способность активно оперировать со смысловыми единицами и терминологией курса, то коллоквиум можно разделить на две части. Сначала преподаватель излагает базовые понятия, содержащиеся в программе. Это должно занять не более четверти занятия. Остальные три четверти необходимо посвятить дискуссии, в ходе которой обучающиеся должны убедиться и, главное, убедить друг друга в обоснованности и доказательности полученного видения вопроса и его соответствия реальной практике. Если же преподаватель имеет дело с более подготовленной, самостоятельно думающей и активно усваивающей смысловые единицы и терминологию курса аудиторией, то коллоквиум необходимо провести так, чтобы сами обучающиеся сформулировали изложенные в программе понятия, высказали несовпадающие точки зрения и привели практические примеры. За преподавателем остается роль модератора (ведущего дискуссии), который в конце «лишь» суммирует совместно полученные результаты.</p>
Тестирование	<p>Контроль в виде тестов может использоваться после изучения каждой темы курса. Итоговое тестирование можно проводить в форме:</p> <ul style="list-style-type: none"> • 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. <p>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 60 вопросов по всему курсу. Значит, итоговое тестирование займет целое занятие. Оценка результатов тестирования может проводиться двумя способами:</p> <ol style="list-style-type: none"> 1) по 5-балльной системе, когда ответы студентов оцениваются следующим образом: <ul style="list-style-type: none"> - «отлично» – более 80% ответов правильные; - «хорошо» – более 65% ответов правильные; - «удовлетворительно» – более 50% ответов правильные. <p>Обучающиеся, которые правильно ответили менее чем на 70% вопросов, должны в последующем пересдать тест. При этом необходимо проконтролировать, чтобы вариант теста был другой;</p> <ol style="list-style-type: none"> 2) по системе зачет-незачет, когда для зачета по данной дисциплине достаточно правильно ответить более чем на 70% вопросов.
Написание и защита курсовой работы	<p>При написании курсовой работы необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др. Основное в подготовке к защите курсовой по дисциплине «Информационная безопасность» - это повторение всего материала дисциплины, по которому необходимо защищать курсовую работу. При подготовке к</p>

	<p>написанию работы обучающийся весь объем работы должен распределять равномерно по дням, отведенным для подготовки к защите курсовой работы, контролировать каждый день выполнение намеченной работы. Подготовка к защите курсовой работы включает в себя три этапа:</p> <ul style="list-style-type: none"> • самостоятельная работа в течение семестра; • непосредственная подготовка в дни, предшествующие экзамену и защите работы по темам курса; • процедура защиты, организованная как специальная беседа преподавателя (комиссии из нескольких преподавателей) с обучающимся, рассчитанная на выяснение способности обучающегося аргументированно обосновать полученные результаты или предложенные конструкторско-технологические и организационно-экономические решения. <p>Для успешной защиты курсовой работы по дисциплине «Информационная безопасность» обучающиеся должны принимать во внимание, что:</p> <ul style="list-style-type: none"> • все основные вопросы, указанные в рабочей программе, нужно знать, понимать их смысл и уметь его разъяснить; • указанные в рабочей программе формируемые профессиональные компетенции в результате освоения дисциплины должны быть продемонстрированы студентом; • семинарские занятия способствуют получению более высокого уровня знаний и, как следствие, более высокой оценке на защите курсовой работы; • готовиться к защите курсовой работы необходимо начинать с первой лекции и первого семинара.
Подготовка к экзамену	<p>При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др. Основное в подготовке к сдаче экзамена по дисциплине - это повторение всего материала дисциплины, по которому необходимо сдавать экзамен. При подготовке к сдаче экзамена обучающийся весь объем работы должен распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнение намеченной работы. Подготовка к экзамену включает в себя три этапа:</p> <ul style="list-style-type: none"> • самостоятельная работа в течение семестра; • непосредственная подготовка в дни, предшествующие экзамену по темам курса; • подготовка к ответу на задания, содержащиеся в билетах (тестах) экзамена. <p>Для успешной сдачи экзамена по дисциплине обучающиеся должны принимать во внимание, что:</p> <ul style="list-style-type: none"> • все основные вопросы, указанные в рабочей программе, нужно знать, понимать их смысл и уметь его разъяснить; • указанные в рабочей программе формируемые профессиональные компетенции в результате освоения дисциплины должны быть продемонстрированы студентом; • семинарские занятия способствуют получению более высокого уровня знаний и, как следствие, более высокой оценке на экзамене; • готовиться к экзамену 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:

Конференц-зал. Кабинет № 203 оснащенный оборудованием:

(Ноутбук – 1 шт.; Проектор – 2 шт.; Экран – 2 шт.; Телевизор – 1 шт.; Стенды- 6 шт.
Стол – 16 шт.; Стул – 70 шт.; WEB-камера – 1 шт.;
Беспроводной микрофон – 1 шт.; Колонки – 2 шт.

Проецируемый экран – 1 шт.; Усилитель для колонок - 1 шт.; Система Video Port;
Система Skype)

Для проведения **практических и семинарских занятий** используется аудитория для семинарских и практических занятий **№ 308**, оснащенная оборудованием:

Учебный стул - 28 шт.; Офисный стол - 1 шт.; Офисный стул - 1 шт.; Шкаф - 1 шт.; Стенд - 7 шт.; Учебная доска - 1шт.; Калькулятор - 15 шт.; Набор для «Математических дисциплин» - 1 компл.; Ноутбук - 1 шт.; Экран - 1 шт.; Учебный стол - 14 шт.; Проектор - 1 шт., Трибуна – 1 шт.

Для **консультаций** используется аудитория для групповых и индивидуальных консультаций **№ 405**, оснащенная оборудованием: Интерактивная доска – 1шт, Проектор 1шт

Учебный стол – 10 шт.; Студенческая лавка (на 3 посадочных места) – 10 шт.; Офисный стол -1 шт.; Офисный стул – 1 шт.; Стенд – 6 шт.; Учебная доска -1 шт.

Для проведения **аттестаций** используется аудитория для текущего контроля и промежуточной аттестации **№ 608**, оснащенная оборудованием:

Учебная доска – 1 шт.; Учебный стол – 16 шт.; Учебный стул – 32 шт.; Офисный стол -1; шт.; Офисный стул – 1 шт.; Стенд – 10 шт.; Трибуна -1 шт.

Для **самостоятельной работы студентов** используется аудитория **№ 305**, оснащенная оборудованием:

Учебный стол – 12 шт.; Учебный стул – 24 шт.; Офисный стол – 1 шт.; Офисный стул – 1 шт.; Шкаф – 1 шт.; Стенд – 5 шт.; Учебная доска – 1 шт.; Ноутбук – 1 шт.; Принтер – 1 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 системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде Института из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

10.1 Лицензионное программное обеспечение:

1. Операционная система Microsoft Windows 10 Professional — OEM-лицензии (поставляются в составе готового компьютера);

2. Операционная система Microsoft Windows 7 Professional — OEM-лицензии (поставляются в составе готового компьютера);

3. Программный пакет Microsoft Office 2010 Professional

4. Комплексная система антивирусной защиты Kaspersky Endpoint Security;

5. 1С: Бухгалтерия 8 учебная версия;

6. Project Expert

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 наукометрическая (библиометрическая) база данных — <http://webofscience.com>
7. Полнотекстовый архив ведущих западных научных журналов на российской платформе Национального электронно-информационного консорциума (НЭИКОН) <http://neicon.ru>
8. Базы данных издательства Springer <https://link.springer.com>
9. www.minfin.ru Сайт Министерства финансов РФ
10. <http://gks.ru> Сайт Федеральной службы государственной статистики
11. www.skrin.ru База данных СКРИН (крупнейшая база данных по российским компаниям, отраслям, регионам РФ)
12. www.cbr.ru Сайт Центрального Банка Российской Федерации
13. <http://moex.com/> Сайт Московской биржи
14. www.fcsf.ru Официальный сайт Федеральной службы по финансовым рынкам (ФСФР)
15. www.rbc.ru Сайт РБК («РосБизнесКонсалтинг» - ведущая российская компания, работающая в сферах масс-медиа и информационных технологий)
16. www.expert.ru Электронная версия журнала «Эксперт»
17. <http://ecsn.ru/> «Экономические науки»

10.4. Информационные справочные системы:

1. www.consultant.ru Справочная правовая система КонсультантПлюс
2. Портал Федеральных государственных образовательных стандартов высшего образования <http://fgosvo.ru>
3. www.garant.ru Информационно-правовая система Гарант

11. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.

Для обеспечения образования инвалидов и обучающихся ограниченными возможностями здоровья по личному заявлению обучающегося разрабатывается адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения лекционного и семинарского материала.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья библиотека комплектует фонд основной учебной литературой, адаптированной к ограничению их здоровья, предоставляет возможность удаленного использования электронных образовательных ресурсов, доступ к которым организован в ЧОУ ВО «ИНУПБТ». В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале, оборудованные программами не визуального доступа к информации, экранными увеличителями и техническими средствами усиления остаточного зрения:

Microsoft Windows 7, Центр специальных возможностей, Экранная лупа;
MicrosoftWindows 7, Центр специальных возможностей, Экранный диктор;
MicrosoftWindows 7, Центр специальных возможностей, Экранная клавиатура; экранная лупа OneLoupe; речевой синтезатор «Голос».