

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ  
федеральное государственное автономное образовательное учреждение высшего  
образования  
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 82

УТВЕРЖДАЮ

Руководитель образовательной программы

доц., к.э.н., доц.

(должность, уч. степень, звание)

И.В. Романова

(инициалы, фамилия)



(подпись)

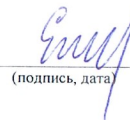
« 27 » 06 20 24 г

Лист согласования рабочей программы дисциплины

Программу составил (а)

к.э.н., доцент

(должность, уч. степень, звание)



(подпись, дата)

Е.И. Карасева

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 82

«20» июня 2024 г, протокол № 11

Заведующий кафедрой № 82

д.э.н., проф.

(уч. степень, звание)



(подпись, дата)

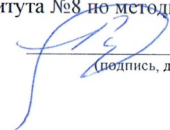
А.С. Будагов

(инициалы, фамилия)

Заместитель директора института №8 по методической работе

доц., к.э.н., доц.

(должность, уч. степень, звание)



(подпись, дата)

Л.В. Рудакова

(инициалы, фамилия)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационное обеспечение безопасности предпринимательства»  
(Наименование дисциплины)

Код направления подготовки/ специальности	38.05.01
Наименование направления подготовки/ специальности	Экономическая безопасность
Наименование направленности	Экономическая безопасность
Форма обучения	очная
Год приема	2024

## Аннотация

Дисциплина «Информационное обеспечение безопасности предпринимательства» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 38.05.01 «Экономическая безопасность» направленности «Экономическая безопасность». Дисциплина реализуется кафедрой «№82».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-1 «Способен проводить расчеты, связанные с осуществлением функций внутреннего контроля, принимать участие в работе отдела внутреннего контроля и разрабатывать задания по осуществлению функций внутреннего контроля, включающие расчетную и аналитическую части»

Содержание дисциплины охватывает круг вопросов, связанных с умением выявлять угрозы и решать задачи, связанные с обеспечением информационной безопасности. В курсе рассматриваются вопросы защиты коммерческой тайны, служебной тайны, персональных данных, финансовой информации, а также методов внутреннего контроля по управлению рисками включающее как расчетные так и аналитические части.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: практические занятия, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов.

Язык обучения по дисциплине «русский»

## 1. Перечень планируемых результатов обучения по дисциплине

### 1.1. Цели преподавания дисциплины

Целью дисциплины «Информационное обеспечение безопасности предпринимательства» является получение обучающимися необходимых навыков связанных с обеспечением информационной безопасности и «представление возможности обучающимся развить и продемонстрировать навыки выявления внутренних и внешних угроз. Содержание курса призвано показать значимость решения проблем обеспечения информационной безопасности на результаты коммерческой деятельности организации. Дисциплина «Информационное обеспечение безопасности предпринимательства» предназначена для понимания проблем реализации комплексной защиты автоматизированных систем (АС) предпринимательства, решения вопросов адекватной защиты информационных ресурсов компаний (предприятий, организаций) всех видов собственности, а также вопросов связанных с внутренним контролем рисков для деятельности предприятия

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-1 Способен проводить расчеты, связанные с осуществлением функций внутреннего контроля, принимать участие в работе отдела внутреннего контроля и разрабатывать задания по осуществлению функций внутреннего контроля, включающие расчетную и аналитическую части	ПК-1.У.2 уметь использовать информацию и методики оценки рисков для деятельности предприятия

## 2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Оценка рисков»

Информатика Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

– Преддипломная практика

### 3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№10
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	6/ 216	6/ 216
<b>Из них часов практической подготовки</b>	30	30
<b>Аудиторные занятия, всего час.</b>	30	30
в том числе:		
лекции (Л), (час)		
практические/семинарские занятия (ПЗ), (час)	30	30
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	36	36
<b>Самостоятельная работа, всего (час)</b>	150	150
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: \*\* кандидатский экзамен

### 4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 10					
Раздел 1. Введение		2			30
Раздел 2. Организационно-правовые методы обеспечения информационной безопасности		2			30
Раздел 3. Угрозы информационной безопасности		4			30
Раздел 4. Методы оценки рисков и их применение в деятельности организации		20			30
Раздел 5. Криптографические методы защиты		2			30
Итого в семестре:		30			150
Итого	0	30	0	0	150

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

#### 4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
	<b>Учебным планом не предусмотрено</b>

#### 4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
<b>Семестр 10</b>					
1	Цели и задачи дисциплины. Основные понятия. Способы защиты информации в прошлом.	Групповая дискуссия. Просмотр фильма	2	2	1
2	Нормативные акты РФ и международные стандарты по защите информации. Модели COSO, COBIT, ITIL. Методология непрерывности бизнеса (Business Continuity Management) Компьютерные преступления. Статьи Ответственность	Групповая дискуссия	2	2	2
3	Методы оценки рисков. Построение модели CAPM	Групповая дискуссия, Занятия по моделированию реальных условий	4	4	2
4	Методы оценки рисков. Построение модели индексный метод торговли	Групповая дискуссия, Занятия по моделированию реальных условий	4	4	3
5	Веб-скрапинг	Занятия по моделированию реальных условий	2	2	3
6	Разработка модели атак,	Занятия по моделированию	2	2	3

	информационной безопасности предприятия. Расчет риска	реальных условий			
7	Разработка модели атак, информационной безопасности предприятия. Расчет риска банковской системы, карточек, банкоматов, on-line платежей. Кардинг. Фишинг.Скиминг. PCI SDD	Групповая дискуссия, Занятия по моделированию реальных условий	4	4	4
9	Разработка модели атак, информационной безопасности предприятия. Расчет риска корпоративной безопасности. Кража пользовательских данных. Кража коммерческой информации.	Групповая дискуссия, Занятия по моделированию реальных условий	2	2	4
10	Fishing. Безопасность и способы защиты интернет магазинов. Киберпреступники. Кибератаки.	Групповая дискуссия	2	2	4
14	Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных. Источники утечки данных . Способы их защиты . Антивирусная защита. Виды вирусов, червей.	Групповая дискуссия, расчет данных	2	2	5
	Методы оценки рисков. «VAR»	Групповая дискуссия, Занятия по моделированию реальных условий	2	2	3
15	Проверка знаний	Групповая	2	2	1

	студентов	дискуссия			,2,3,4,5
Всего			30	30	

#### 4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				
Всего				

#### 4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

#### 4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 10, час
1	2	3
Изучение теоретического материала дисциплины (ТО)		
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)	40	40
Выполнение реферата (Р)	20	20
Подготовка к текущему контролю успеваемости (ТКУ)	60	60
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	30	30
Всего:	150	150

#### 5. Перечень учебно-методического обеспечения

для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

#### 6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/	Библиографическая ссылка	Количество экземпляров в
-------	--------------------------	--------------------------

URL адрес		библиотеке (кроме электронных экземпляров)
	<a href="https://znanium.com/catalog/document?id=364911">https://znanium.com/catalog/document?id=364911</a>	Информационная безопасность и защита информации / Баранова Е.К., Бабаш А.В./ Издательский центр РИОР, 2021
	<a href="https://znanium.com/read?id=364624">https://znanium.com/read?id=364624</a>	Информационная безопасность / Партыка Т.Л., Попов И.И./ Издательство ФОРУМ, 2021
005.5 К 21	Карасева, Екатерина Ивановна (канд. экон. наук). Технологии управления риском : учебно-методическое пособие / Е. И. Карасева ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2019. - 93 с. : рис., табл. - Библиогр.: с. 91 - 92 (13 назв.).	5

#### 7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
<a href="https://pro.guap.ru/">https://pro.guap.ru/</a>	прогуап
<a href="https://lms.guap.ru/new/">https://lms.guap.ru/new/</a>	лмс

#### 8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем, используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено



## 9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Класс для деловой игры компьютером	Ленс

## 10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Тесты.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 – Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся глубоко и всесторонне усвоил программный материал;</li> <li>– уверенно, логично, последовательно и грамотно его излагает;</li> <li>– опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;</li> <li>– умело обосновывает и аргументирует выдвигаемые им идеи;</li> <li>– делает выводы и обобщения;</li> <li>– свободно владеет системой специализированных понятий.</li> </ul>
«хорошо» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>– не допускает существенных неточностей;</li> <li>– увязывает усвоенные знания с практической деятельностью направления;</li> <li>– аргументирует научные положения;</li> <li>– делает выводы и обобщения;</li> <li>– владеет системой специализированных понятий.</li> </ul>
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>– допускает несущественные ошибки и неточности;</li> <li>– испытывает затруднения в практическом применении знаний направления;</li> <li>– слабо аргументирует научные положения;</li> </ul>

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	<ul style="list-style-type: none"> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> <li>– не формулирует выводов и обобщений.</li> </ul>

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	Оценить риски вероятностным методом. Сделать выводы	ПК-1.У.2
2	Рассчитать риски методом математического ожидания.	
3	Сделать выводы	
4	Рассчитать риски методом средней вероятности появления событий. Сделать выводы	
5	Сделать выводы	
6	Рассчитать риски методом максимина. Сделать выводы	
7	Рассчитать риски методом минимакса. Сделать выводы	
8	Рассчитать риски с помощью коэффициентов. Сделать	
9	выводы	
10	Рассчитать риски с помощью страхующих фондов.	
	Сделать выводы	
11	Посчитать Хэш-функцию, Сделать выводы	
12	Построить модель корпоративной безопасности. Способы защиты информации. Сделать выводы	
13	Построить модель САРМ и рассчитать ее показатели. Сделать выводы	
14	Построить Индексную модель и построить эффективный портфель. Сделать выводы	
15	Рассчитать VaR. Сделать выводы	
16	Построить модель атак. Посчитать риск. Сделать выводы	
17	Веб-скрепинг, собрать информацию, сделать выводы	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора								
	<p><b>1 Тип задания:</b> Задания с выбором одного правильного ответа, в том числе с его обоснованием Прочитайте текст и запишите ответ. Технология, которая позволяет автоматизировано собирать информацию ? 1 вэб-скрапинг 2 лендинг 3 контент анализ 4 фракталы</p> <p><b>2 Тип задания:</b> Задания с выбором нескольких правильных ответов, в том числе с его обоснованием Прочитайте текст, выберите правильные варианты ответа К электронным деньгам относятся 1 Электронные деньги на базе карт 2 Фиатные деньги, Нефиатные деньги 3 Предоплаченные одноцелевые карты (подарочные, телефонные, топливные и другие). 4 Яндекс Деньги, Paucash, Webmoney, Rupay, Cybercash и другие</p> <p><b>3 Тип задания:</b> Задания на сопоставление</p> <p>Прочитайте текст и установите соответствие. К каждой позиции, данной влевом столбце, подберите соответствующую позицию в правом столбце) Сопоставьте описание элементов методологии «деревьев отказов» и их определение:</p> <table border="1" data-bbox="347 1570 1294 2047"> <tbody> <tr> <td data-bbox="347 1570 826 1682">1 Это выполнение одного события из нескольких или комбинаций этих событий</td> <td data-bbox="826 1570 1294 1682">А . Связь «ИЛИ»</td> </tr> <tr> <td data-bbox="347 1682 826 1794">2 Это одновременное выполнение нескольких событий</td> <td data-bbox="826 1682 1294 1794">Б . Связь «И»</td> </tr> <tr> <td data-bbox="347 1794 826 1939">3 Это события которые образуются несколькими инициирующими событиями</td> <td data-bbox="826 1794 1294 1939">В «Производные события»</td> </tr> <tr> <td data-bbox="347 1939 826 2047">4 События начального уровня которые не образуются другими событиями</td> <td data-bbox="826 1939 1294 2047">Г Инициирующие события</td> </tr> </tbody> </table>	1 Это выполнение одного события из нескольких или комбинаций этих событий	А . Связь «ИЛИ»	2 Это одновременное выполнение нескольких событий	Б . Связь «И»	3 Это события которые образуются несколькими инициирующими событиями	В «Производные события»	4 События начального уровня которые не образуются другими событиями	Г Инициирующие события	ПК-1.У.2
1 Это выполнение одного события из нескольких или комбинаций этих событий	А . Связь «ИЛИ»									
2 Это одновременное выполнение нескольких событий	Б . Связь «И»									
3 Это события которые образуются несколькими инициирующими событиями	В «Производные события»									
4 События начального уровня которые не образуются другими событиями	Г Инициирующие события									

	<p><b>Тип задания:</b> Задание на установление правильной последовательности</p> <p>Прочитайте текст и установите последовательность</p> <p><b>Текст задания:</b> Расставьте этапы расчета и построения сценария</p> <ol style="list-style-type: none"> <li>1. Задать вершины</li> <li>2. Установить связи между вершинами</li> <li>3. Задать вероятности инициирующих событий</li> <li>4. Установить параметры расчета</li> <li>5. Нажать на запуск</li> </ol>	
	<p><b>5 Тип задания:</b> Задания с развернутым ответом</p> <p>Прочитайте определение и запишите ответ и от каких 3-х параметров он зависит</p> <p>Что такое - Стоимость под риском (<i>value at risk, VaR</i>)</p>	

Система оценивания тестовых заданий:

1 тип) Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора считается верным, если правильно указана цифра и приведены конкретные аргументы, используемые при выборе ответа. Полное совпадение с верным ответом оценивается 1 баллом, неверный ответ или его отсутствие – 0 баллов.

2 тип) Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора считается верным, если правильно указаны цифры и приведены конкретные аргументы, используемые при выборе ответов. Полное совпадение с верным ответом оценивается 1 баллом, если допущены ошибки или ответ отсутствует – 0 баллов.

3 тип) Задание закрытого типа на установление соответствия считается верным, если установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого столбца). Полное совпадение с верным ответом оценивается 1 баллом, неверный ответ или его отсутствие – 0 баллов

4 тип) Задание закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр. Полное совпадение с верным ответом оценивается 1 баллом, если допущены ошибки или ответ отсутствует – 0 баллов.

5 тип) Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте. Правильный ответ за задание оценивается в 3 балла, если допущена одна ошибка \ неточность \ ответ правильный, но не полный - 1 балл, если допущено более 1 ошибки \ ответ неправильный \ ответ отсутствует – 0 баллов

Перечень тем

контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

#### 11. Методические указания для обучающихся по освоению дисциплины

##### 11.1. Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимся практических занятий:

- закрепление, углубление, расширение и детализация знаний при решении конкретных задач;
- развитие познавательных способностей, самостоятельности мышления, творческой активности;
- овладение новыми методами и методиками изучения конкретной учебной дисциплины;
- выработка способности логического осмысления полученных знаний для выполнения заданий;
- обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

##### Требования к проведению практических занятий

№	Названия практического задания	Описание
1	Цели и задачи дисциплины. Основные понятия. Способы защиты информации в прошлом	Студенты готовят материал из различных источников и идет дискуссия в группе, по основным понятиям ИБ, а также какие цели и задачи дисциплины. Смотрят фильм о способах защиты информации в прошлом.
2	Нормативные акты РФ и международные стандарты по защите информации. Модели COSO, COBIT, ITIL. Методология непрерывности бизнеса (Business Continuity Management) Компьютерные преступления. Статьи Ответственность	Студенты готовят материал из различных источников, и идет дискуссия в группе по нормативным актам, законам, стандартам по информационной безопасности. Студенты готовят материал из различных источников, и идет дискуссия в группе по Модели COSO, COBIT, ITIL. Методология непрерывности бизнеса (Business Continuity Management). Студенты готовят материал из различных источников, и

		идет дискуссия в группе какие статьи УК описывают компьютерные преступления и какая ответственность за это предусмотрена
3	Методы оценки рисков. Построение модели CAPM	Студенты строят модель CAPM рассчитывают показатели
4	Методы оценки рисков. Построение модели индексный метод торговли	Студенты строят модель индексного метода рассчитывают показатели
5	Веб- скрепинг	Рассматривают методы сбора информации с помощью парсинга
6	Разработка модели атак, информационной безопасности предприятия	Студенты моделируют атаки, моделируют ИС для защиты от атак, рассчитывают риск
7	Разработка модели атак Расчет риска безопасности банковской системы Безопасность банковской системы, карточек, банкоматов, on-line платежей. Кардинг. PCI SDD	Студенты моделируют атаки, моделируют ИС для защиты от атак, рассчитывают риск
8	Разработка модели атак, информационной безопасности предприятия. Расчет риска корпоративной безопасности. Кража пользовательских данных. Кража коммерческой информации.	Студенты моделируют атаки, моделируют ИС для защиты от атак, рассчитывают риск
9	Fishing. Безопасность и способы защиты интернет магазинов. Киберпреступники. Кибератаки.	Студенты готовят материал из различных источников, и идет дискуссия в группе по Fishing, Безопасности и способах защиты интернет магазинов, киберпреступники. кибератаки.
10	Антивирусная защита. Виды вирусов, червей.	Студенты готовят материал из различных источников, и идет дискуссия в группе по Антивирусной защите, Видах вирусов, червей
11	Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных . Источники угроз информационной безопасности( wi-fi, vpn, системы обнаружения и предотвращения вторжений (IDS/IPS) Защита периметра корпоративной сети. BYOD и др Антивирусная защита. Виды вирусов, червей.	Студенты готовят материал из различных источников, и идет дискуссия в группе Хэш-функциям . а также другим источником угроз информационной безопасности для предприятия. Рассчитывают показатели хеша

12	Методы оценки рисков. «VAR»	Студенты строят модель VaR рассчитываю показатели
----	--------------------------------	---

11.2. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Таблица 21 - Темы теоретического материала для самостоятельного изучения и их трудоемкость

Темы на самостоятельное изучение
1. Безопасность банковской системы, карточек, банкоматов, on-line платежей. Кардинг. PCI SDD
2. Безопасность и способы защиты электронных денег
3. Сервисные службы защиты информации
4. Нарушения в информационной сфере
5. Корпоративная безопасность. Кража пользовательских данных. Кража коммерческой информации
6. Модели защиты доступа к сети
7. Fishing. Безопасность и способы защиты интернет магазинов
8. Действия, приводящие к неправомерному овладению конфиденциальной информацией: разглашение, утечка, несанкционированный доступ
9. Наиболее распространенные угрозы доступности информационных ресурсов.
10. Вредоносное программное обеспечение, технология противодействия
11. Основные угрозы целостности, конфиденциальности
12. Безопасность dgm-системы
13. Безопасность и взлом автомобильных компьютерных систем
14. Федеральные законы «Об информации, информационных технологиях и защите информации», «О персональных данных» Правовые акты общего назначения, затрагивающие вопросы информационной безопасности Другие законы и нормативные акты.
15. Модели COSO, IDIL, COBIT и др
16. Политики безопасности компании
17. Электронная цифровая подпись (ЭЦП) и электронная подпись (ЭП) Методы криптографии

11.3. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Если студент не сдал задания по практическим работам до текущего контроля, то на при успешной сдачи экзамена он получит оценку не выше «удовлетворительно»

11.4. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Если студент сдал все работы, то он может получить оценку за экзамен как среднюю за работы. Стандартный экзамен – состоит из 3 вопросов, также могут быть заданы дополнительные или уточняющие вопросы. По результатам работы в семестре в некоторых случаях количество вопросов может быть уменьшено.



Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой