Аннотация к рабочей программе дисциплины «Оценка рисков и угроз»

Цель преподавания дисциплины

Дисциплина «Оценка рисков и угроз» изучается с целью обучения студентов основам оценки рисков при проектировании политик информационной безопасности и выработке адекватных средств предотвращения несанкционированного доступа.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны изучить:

– основные понятия теории управление рисками;

– методики технологии управления рисками;

– технологии управления рисками;

– принципы разработки корпоративных методик анализа рисков.

– современные методы и средства анализа и управление рисками информационных систем компаний.

Компетенции, формируемые в результате освоения дисциплины

Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК – 13).

Разделы дисциплины

Оценка информационных рисков. Управление рисками. Основные понятия. Методики и технологии управления рисками. Разработка корпоративной методики анализа рисков. Современные методы и средства анализа и управление рисками информационных систем компаний.

МИНОБРНАУКИ РОССИИ
ЮЗго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

Т.А. Ширабакина
(подпись, инициалы, фамилия)
«2» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Оценка рисков и угроз

направление подготовки (специальность) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность и на основании учебного плана направления подготовки 10.03.01 Информационная безопасность , одобренного Учёным советом университета, протокол №3 «30» 01 2017г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры информационной безопасности № 9 «1» февраля 2017г.

Зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
Доцент кафедры ИБ Ханис А.Л.

Согласовано:

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 1 «28» 08 2017г. на заседании кафедры информационной безопасности
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №5 «30» 01 2018г. на заседании кафедры информационной безопасности, 29.06.18, №12
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности, 27.06.19, №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Дисциплина "Оценка рисков и угроз" изучается с целью обучения студентов основам оценки рисков при проектировании политик информационной безопасности и выработке адекватных средств предотвращения несанкционированного доступа.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны изучить:

- основные понятия теории управление рисками;
- методики технологии управления рисками;
- технологии управления рисками;
- принципы разработки корпоративных методик анализа рисков.
- современные методы и средства анализа и управление рисками информационных систем компаний.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

обучающиеся должны **знать:**

- понятие информационных рисков
- методики количественного и качественного оценивания рисков
- принципы управления рисками;
- принципы классификации рисков;

уметь:

- применять известные методики оценки рисков;
- разрабатывать корпоративную политику управления рисками
- анализировать и классифицировать риски.

владеть:

- методами проведения анализа рисков информационной безопасности;
- навыками разделения рисков на приемлемые и неприемлемые .

У обучающихся формируются следующие компетенции:

способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК – 13).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам базовой части профессионального цикла (Б1.В.ДВ.11.1). Изучается на 4 курсе в 8 семестре

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

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицу, 108 часов

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54,1
в том числе:	
лекции	36
лабораторные занятия	не предусмотрено
практические занятия	18
экзамен	не предусмотрено
зачет	0,1
Аудиторная работа (всего):	107,9
в том числе:	
лекции	36
лабораторные занятия	не предусмотрено
практические занятия	18
Самостоятельная работа обучающихся (всего)	53,9
Контроль/экз (подготовка к экзамену)	0

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

4.1 Содержание дисциплины

Таблица 4.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Оценка информационных рисков.	Обработка информационных рисков. Положение о применимости. Документированные процедуры. Обучение сотрудников компании как способ снижения рисков. Управление ИБ. Внедрение процедур системы управления ИБ
2	Управление рисками. Основные понятия.	Система управления рисками. Этапы процесса управления риском. Методики оценивания рисков. Модель угроз и уязвимостей. Модель оценки рисков на основе модели информационных потоков
3	Методики и технологии управления рисками.	Качественные методики управления рисками. Метод COBRA. . Метод RA Software Tool Количественные методики управления рисками. Метод CRAMM. CRAMM как инструментарий аудитора.
4	Разработка корпоративной методики анализа рисков.	Постановка задачи разработки корпоративной методики анализа рисков. Сценарий анализа информационных рисков компании. Методы оценивания информационных рисков. Табличные методы оценки рисков. Оценка рисков по двум факторам. Разделение рисков на приемлемые и неприемлемые
5	Современные методы и средства анализа и управление рисками информационных систем компаний.	Обоснование необходимости инвестиций в информационную безопасность компании. Основные этапы оценки риска Методика FRAP. Матрица рисков. Методика OCTAVE. Профиль угрозы. Разработка стратегии и планов безопасности. Методика Risk Watch. Определение категорий защищаемых ресурсов.

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ П п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Оценка информационных рисков.	2			У-1,2,8 МУ-2	УО	ПК – 13
2.	Управление рисками. Основные понятия.	2		1	У-1-3, 4,6 МУ-1,2	УО ЗПР	ПК – 13
3.	Методики и технологии управления рисками.	4		2	У-1, 5 МУ-1,2	УО ЗПР	ПК – 13
4.	Разработка корпоративной методики анализа рисков.	4		2	У-2,3 МУ-1,2	УО ЗПР	ПК – 13
5.	Современные методы и средства анализа и управление рисками информационных систем компаний.	6		4	У-1-3 МУ-1,2	УО ЗПР	ПК – 13
	ИТОГО	18					

УО – устный опрос, ЗПР – практическая работа

4.1. Лабораторные работы и практические занятия

4.1.1. Практические занятия

Таблица 4.3 – Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1.	Методы оценивания информационных рисков. Табличные методы оценки рисков	4
2.	Оценка рисков по двум факторам	4
3.	Разделение рисков на приемлемые и неприемлемые. Оценка рисков по трем факторам	4
4.	Методика анализа рисков Microsoft	6

№	Наименование практического занятия	Объем, час.
1	2	3
Итого**:**		18

4.2. Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Оценка информационных рисков.	1 неделя	8
2	Управление рисками. Основные понятия.	2 неделя	8
3	Методики и технологии управления рисками.	4 неделя	16
4	Разработка корпоративной методики анализа рисков.	6 неделя	16
5	Современные методы и средства анализа и управление рисками информационных систем компаний.	9 неделя	24
Итого			72

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно- методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

– путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 по направлению подготовки 10.03.01 «Информационная безопасность телекоммуникационных систем» реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках дисциплины предусмотрены встречи с экспертами и специалистами. Удельный вес занятий, проводимых в интерактивных формах, составляет 24,8% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на практических занятиях по темам лекций.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Образовательные технологии	Объем, час.
1	2	3	4
1	Методы оценивания информационных рисков. Табличные методы оценки рисков	Разбор конкретных ситуаций	2
2	Оценка рисков по двум факторам	Разбор конкретных ситуаций	2
Итого:			4

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК – 13)	История информационного противоборства	Основы управления информационной безопасностью	Экономика защиты информации; Оценка рисков и угроз;

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень (удовлетворительно)	Продвинутый уровень (хорошо)	Высокий уровень (отлично)
1	**2**	**3**	**4**	**5**

ПСК-13/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	**Знать:** – терминологию теории управления рисками. **Уметь:** – применять типовые методики для получения характеристик рисков и угроз. **Владеть:** – базовыми навыками оценки рисков информационной безопасности.	**Знать:** – основные методики оценки рисков. **Уметь:** – использовать основные модели оценки рисков для получения количественных и качественных оценок рисков. **Владеть:** – навыками оценки рисков информационной безопасности.	**Знать:** – теоретические основы, лежащие в основе современных методик управления рисками. **Уметь:** – использовать модели оценки рисков для формирования политики управления рисками и проектирования системы управления рисками. **Владеть:** – навыками оценки рисков информационной безопасности и проектирования систем управления корпоративными рисками.

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

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ зада-	

					ний	
1	2	3	4	5	6	7
1	Оценка информационных рисков.	ПК-13	Лекция, СРС	Вопросы для УО	1-5	Согласно табл.7.2
2	Управление рисками. Основные понятия.	ПК-13	Лекция, СРС, практическое занятие	Вопросы для УО	1-5	Согласно табл.7.2
				Вопросы к ПР 1	1-5	
3	Методики и технологии управления рисками.	ПК-13	Лекция, СРС, практическое занятие	Вопросы для УО	1-5	Согласно табл.7.2
				Вопросы к ПР 2	1-5	
4	Разработка корпоративной методики анализа рисков.	ПК-13	Лекция, СРС, практическое занятие	Вопросы для УО	1-5	Согласно табл.7.2
				Вопросы к ПР 3	1-5	
5	Современные методы и средства анализа и управление рисками информационных систем компаний.	ПК-13	Лекция, СРС, практическое занятие	Вопросы для УО	1-5	Согласно табл.7.2
				Вопросы к ПР 4	1-5	

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 4. «Методики и технологии управления рисками».

1. В чём заключаются преимущества и недостатки качественных методик управления рисками?
2. Опишите метод COBRA.
3. Опишите метод RA Software Tool
4. Возможно ли применение метода RA Software Tool для описание рисков в системах, обрабатывающих гостайну и почему?

5. Опишите метод CRAMM.
6. Какой из методов управления рисками наиболее предпочтителен в национальной системе стандартов информационной безопасности и почему?
7. Как использовать метод CRAMM в аудите информационной безопасности?

Контрольные вопросы для защиты практической работы №1:

1. Назовите критерии, по которым какая-либо процедура обеспечения ИБ может быть названа необходимой в бизнес-процессах компании.
2. Кто выполняет оценку риска?
3. В чём заключается методика FRAP.
4. Как формируется матрица рисков.
5. Недостатки матричного представления рисков
6. Что такое профиль угрозы?
7. Сопоставьте преимущества и недостатки методик Risk Watch и OCTAVE.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

7.4. Рейтинговый контроль изучения учебной дисциплины

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Практическая работа №1 «Методы оценивания информационных рисков. Табличные методы оценки рисков»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Практическая работа №2 «Оценка рисков по двум факторам»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Практическая работа №3 «Разделение рисков на приемлемые и неприемлемые. Оценка рисков по трем факторам»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Практическая работа №4 «Методика анализа рисков Microsoft»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Устный опрос	8		16	
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		100	

При итоговом контроле в форме компьютерного теста студенту предлагается 20 вопросов по различным темам курса из 5 категорий сложности. Вопросы 1-й категории сложности оцениваются в 1 условный балл, 2-й – в 2 условных балла, и т. д. В каждом вопросе один правильный ответ. Полученную итоговую сумму условных баллов (максимум 60) переводят в баллы на экзамене (максимум 36) путём умножения на 0.6 и округления до целого значения.

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

8.1 Основная учебная литература

1. Санникова, И. Н. Экономическая безопасность : учебное пособие : [16+] / И. Н. Санникова, Е. А. Приходько ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 103 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575023 (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-7782-3693-6. – Текст : электронный.

2. Фомичев, А. Н. Риск-менеджмент : учебник / А. Н. Фомичев. – 7-е изд. – Москва : Дашков и К, 2020. – 372 с. : ил. – (Учебные издания для бакалавров). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=573397 (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-394-03820-4. – Текст : электронный.

3. Тихомиров, Н. П. Теория риска : учебник / Н. П. Тихомиров, Т. М. Тихомирова ; Российский экономический университет им. Г.В. Плеханова. – Москва : Юнити-Дана, 2020. – 308 с. : ил., табл., граф. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615777 (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-238-03413-3. – Текст : электронный.

4. Ханис, А. Л. Организация и управление службой защиты информации : учебное пособие для студентов, обучающихся по направлениям подготовки 10.03.01 «Информационная безопасность», 10.05.02 "Информационная безопасность телекоммуникационных систем" / А. Л. Ханис, Ю. А. Будникова ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2020. - 119 с. - Библиогр.: с. 113. - ISBN 978-5-7681-1451-0 : 270.00 р. - Текст : непосредственный.

8.2 Дополнительная учебная литература

5. Панкратов, Ф. Г. Коммерческая деятельность : учебник / Ф. Г. Панкратов, Н. Ф. Солдатова. – 13-е изд. – Москва : Дашков и К, 2017. – 500 с. : табл., схем., граф. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=452590 (дата обращения: 23.08.2021). – ISBN 978-5-394-01418-5. – Текст : электронный.

6. Суглобов, А. Е. Экономическая безопасность предприятия : учебное пособие / А. Е. Суглобов, С. А. Хмелев, Е. А. Орлова. – Москва :

Юнити-Дана, 2017. – 271 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615936 (дата обращения: 23.08.2021). – Библиогр.: с. 214-219. – ISBN 978-5-238-02378-6. – Текст : электронный.

7. Аверченков, В. И. Служба защиты информации: организация и управление : [16+] / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 186 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-9765-1271-9. – Текст : электронный.

8. Балдин, К. В. Управление рисками : учебное пособие / К. В. Балдин, С. Н. Воробьев. – Москва : Юнити-Дана, 2017. – 511 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615795 (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 5-238-00861-9. – Текст : электронный.

9. Остапенко, Е. А. Финансовая среда и предпринимательские риски : учебное пособие / Е. А. Остапенко, Т. Г. Гурнович. – Ставрополь : Секвойя, 2017. – 271 с. : ил. – (Серия «Бакалавриат»). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=485067 (дата обращения: 23.08.2021). – Библиогр. в кн. – Текст : электронный.

10. Земцова, Л. В. Страхование предпринимательских рисков: конспект лекций / Л. В. Земцова ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : ТУСУР, 2016. – 115 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480998 (дата обращения: 23.08.2021). – Библиогр. в кн. – Текст : электронный.

11. Экономическая безопасность : учебник / под ред. В. Б. Мантусова, Н. Д. Эриашвили ; Российская таможенная академия. – 4-е изд., перераб. и доп. – Москва : Юнити, 2018. – 567 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=496884 (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-238-03072-2. – Текст : электронный.

12. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

8.3 Перечень методических указаний

1. Оценка рисков информационной безопасности : методические рекомендации по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 28 с.: Библиогр.: с. 28.
2. Оценка рисков и угроз : методические рекомендации для самостоятельной работы/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2018. – 7 с.: ил. 0, табл. 0. – Библиогр.: с. 7.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
4) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
5) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
6) База данных "Патенты России"

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Оценка рисков и угроз» являются лекции, практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по

результатам тестирования, собеседования, защиты отчетов по практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Оценка рисков и угроз»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Оценка рисков и угроз» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Оценка рисков и угроз» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385

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

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l 7"TFT E700 (6 шт)

13. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Измененных	Заменённых	Аннулированных	новых			