Аннотация к рабочей программе дисциплины «Оценка рисков информационной безопасности»

Цель преподавания дисциплины

Целью преподавания дисциплины «Оценка рисков информационной безопасности» является изложение основных направлений развития рынка информации, принципов и методов защиты информации, методов определения основных показателей экономической эффективности защиты информации, способов определения затрат на информационную безопасность, оценки и минимизации коммерческого риска, оценки рисков при проектировании политик информационной безопасности и выработке адекватных средств предотвращения несанкционированного доступа.

Задачи изучения дисциплины

– изучение основных направлений развития рынка информации, принципов и методов защиты информации, методов определения основных показателей экономической эффективности защиты информации, способов определения затрат на информационную безопасность;

– изучение способов оценки и минимизации коммерческого риска;

– изучение теории управление рисками, методов и методик технологии управления рисками;

– изучение принципов разработки корпоративных методик анализа рисков, современных методов и средств анализа и управления рисками информационных систем компаний;

– овладение навыками организации работ по обеспечению информационной безопасности в автоматизированных системах;

– оценка эффективности выполнения задач по обслуживанию защищённых автоматизированных систем;

– изучение состава, структуры и функций службы защиты информации;

– изучение основных типов инцидентов информационной безопасности;

– изучение основ построения и модернизации системы защиты информации автоматизированной системы (АС);

– изучение функционирования систем мониторинга безопасности АС.

Компетенции, формируемые в результате освоения дисциплины

Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах (ПК-9);

Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности (ПК-10).

Разделы дисциплины

Основные понятия и содержание дисциплины «Оценка рисков информационной безопасности». 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

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____М.О. Таныгин
(подпись, инициалы, фамилия)

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Оценка рисков информационной безопасности
(наименование дисциплины)

ОПОП ВО 10.03.01 Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины Оценка рисков информационной безопасности составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета (протокол № 6 «26» 02 2021 г.).

Рабочая программа дисциплины Оценка рисков информационной безопасности обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, на заседании кафедры информационной безопасности Протокол №1«30» 08 2021г.

Зав. кафедрой Таныгин М.О.

Разработчик программы

к.воен.н., доцент ~~Х~~анис А.Л.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Оценка рисков информационной безопасности пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета протокол № 6 «26» 02 2021 г., на заседании кафедры ИБ №11 от 30.06.21.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа дисциплины Оценка рисков информационной безопасности пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета протокол № _ «__» _____ 20_ г., на заседании кафедры _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины «Оценка рисков информационной безопасности» является изложение основных направлений развития рынка информации, принципов и методов защиты информации, методов определения основных показателей экономической эффективности защиты информации, способов определения затрат на информационную безопасность, оценки и минимизации коммерческого риска, оценки рисков при проектировании политик информационной безопасности и выработке адекватных средств предотвращения несанкционированного доступа.

1.2 Задачи дисциплины

- изучение основных направлений развития рынка информации, принципов и методов защиты информации, методов определения основных показателей экономической эффективности защиты информации, способов определения затрат на информационную безопасность;
- изучение способов оценки и минимизации коммерческого риска;
- изучение теории управление рисками, методов и методик технологии управления рисками;
- изучение принципов разработки корпоративных методик анализа рисков, современных методов и средств анализа и управления рисками информационных систем компаний;
- овладение навыками организации работ по обеспечению информационной безопасности в автоматизированных системах;
- оценка эффективности выполнения задач по обслуживанию защищённых автоматизированных систем;
- изучение состава, структуры и функций службы защиты информации;
- изучение основных типов инцидентов информационной безопасности;
- изучение основ построения и модернизации системы защиты информации автоматизированной системы (АС);
- изучение функционирования систем мониторинга безопасности АС.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-9	Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах.	ПК-9.3 Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации.	***Знать:*** понятие информационных рисков, методики количественного и качественного оценивания рисков, принципы управления рисками, принципы классификации рисков, задачи и функции службы защиты информации (СЗИ), типовые должностные обязанности персонала, обслуживающего защищённые АС, состав, документацию, характеристики и принцип работы оборудования АС, классификацию, состав, документацию, способы применения средств защиты информации в АС. ***Уметь:*** применять известные методики оценки рисков, разрабатывать корпоративную политику управления рисками, анализировать и классифицировать риски, настраивать оборудование АС, применять средства защиты информации в АС, осуществлять контроль работ по защите АС, проводить анализ результатов выполняемых работ. ***Владеть:*** методами проведения анализа рисков информационной безопасности, навыками разделения рисков на приемлемые и неприемлемые, навыками применения программных и аппаратных средств защиты информации в АС, разработки архитектуры АС, контроля и анализа результатов выполняе-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			мых работ.
ПК-10	Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности.	ПК-10.1 Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации.	***Знать:*** понятие информационных рисков, методики количественного и качественного оценивания рисков, принципы управления рисками, принципы классификации рисков, типовые инциденты информационной безопасности АС, состав, документацию, характеристики и принцип работы оборудования АС, классификацию, состав, документацию, способы применения систем и средств защиты информации в АС. ***Уметь:*** применять известные методики оценки рисков, разрабатывать корпоративную политику управления рисками, анализировать и классифицировать риски, классифицировать инциденты информационной безопасности АС, применять средства защиты информации в АС, определять уязвимые узлы в системе информационной безопасности, осуществлять контроль функционирования систем и средств защиты АС, проводить анализ результатов выполняемых работ. ***Владеть:*** методами проведения анализа рисков информационной безопасности, навыками применения программных и аппаратных средств защиты информации в АС, обнаружения инцидентов и восстановления функционирования оборудования АС, контроля и анализа результатов выполняемых работ.
		ПК-10.2 Обосновывает необ-	***Знать:*** понятие информационных рисков, методики количе-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		ходимость модернизации системы защиты информации автоматизированной системы.	ственного и качественного оценивания рисков, задачи и функции службы защиты информации (СЗИ), типовые должностные обязанности персонала, обслуживающего защищённые АС, состав, документацию, характеристики и принцип работы оборудования АС, классификацию, состав, документацию, способы применения средств защиты информации в АС, типовые инциденты информационной безопасности АС и способы их предотвращения. ***Уметь:*** применять известные методики оценки рисков, разрабатывать корпоративную политику управления рисками, проводить анализ инцидентов информационной безопасности АС, определять уязвимые места системы безопасности АС, разрабатывать архитектуры сети с учётом уязвимых мест, разрабатывать состав и требования к системам информационной безопасности АС в интересах модернизации АС. ***Владеть:*** навыками разделения рисков на приемлемые и неприемлемые, навыками анализа инцидентов информационной безопасности АС, определения уязвимых мест системы безопасности АС, принятия мер для восстановления функционирования системы, разработки архитектуры сетей с учётом уязвимых мест, разработки предложений по составу и требованиям к системам информационной безопасности АС в рамках модернизации АС.
		ПК-10.4	***Знать:*** понятие информацион-

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
		Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем.	ных рисков, принципы управления рисками, принципы классификации рисков, задачи и функции систем и средств мониторинга и управления средствами обеспечения безопасности АС, правила эксплуатации оборудования и программных средств управления средствами защиты АС, классификацию и способы применения средств и систем защиты АС. ***Уметь:*** применять известные методики оценки рисков, разрабатывать корпоративную политику управления рисками, проводить анализ защищенности АС, разрабатывать правила протоколирования результатов мониторинга АС, настраивать оборудования и программных средств мониторинга и управления средствами защиты АС, средства и системы защиты АС. ***Владеть:*** методами проведения анализа рисков информационной безопасности, навыками анализа защищенности АС, эксплуатации программных средств мониторинга и управления средствами зашиты АС, разработки правил протоколирования результатов мониторинга АС, настройки оборудования и программных средств мониторинга и управления средствами защиты АС, средств и систем защиты АС.

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Элективная дисциплина «Экономика защиты информации» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)») основной профессиональной образовательной программы – программы бакалавриата (специалитета, магистратуры) 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем. Дисциплина 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 трудоемкость (объем) дисциплины составляет 3 зачетные единицы (з.е.), 108 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	54
в том числе:	
лекции	36
лабораторные занятия	0
практические занятия	18
Самостоятельная работа обучающихся (всего)	53,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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

4.1 Содержание дисциплины

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел, (тема) дисциплины	Содержание

1	2	3
1	Основные понятия и содержание дисциплины «Оценка рисков информационной безопасности».	Становление индустрии информации. Характеристики информации. Характеристики информационного общества. Аспекты защиты информации. Экономика защиты информации как наука, задачи оценки информационных рисков. Экономические проблемы ЗИ. Информация как товар.
2	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.
3	Управление рисками. Основные понятия.	Система управления рисками. Этапы процесса управления риском. Методики оценивания рисков. Модель угроз и уязвимостей. Модель оценки рисков на осно-
4	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.
5	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.
6	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 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Основные понятия и содержание дисциплины «Оценка рисков информационной безопасности».	2	-	-	У-1-6, У-7, У-10 МУ-2	УО- 2	ПК-9, ПК-10
2	Оценка информационных рисков.	2	-	1	У-1-6, У-7, У-10, МУ-1,2	УО – 4, ЗПР - 4	ПК-9, ПК-10

3	Управление рисками. Основные понятия.	2	-	2	У-1- 5, У-7- У-13, МУ-1,2	УО-6, ЗПР - 6	ПК-9, ПК-10
4	Методики и технологии управления рисками.	2	-	3	У-1-5,У-6, У-9, У-10, МУ-1,2	УО-10, ЗПР - 10	ПК-9, ПК-10
5	Разработка корпоративной методики анализа рисков.	2	-	4	У-1-6, У-8, У-9, У-10-У-15, МУ-1,2	УО-14, ЗПР - 14	ПК-9, ПК-10
6	Современные методы и средства анализа и управление рисками информационных систем компаний.	2	-	5	У-1-6, У-7, У-10-У-18 МУ-1,2	УО-18, ЗПР - 18	ПК-9, ПК-10
	Всего	36	0	18			

УО – устный опрос, ЗПР – практическая работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 - Практические занятия

№	Наименование практического (семинарского) занятия	Объем, час.
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.	4
5	Минимизация риска и защита информации при заключении договоров.	2
Итого		18

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Основные понятия и содержание дисциплины «Оценка рисков информационной безопасности».	2 неделя	8,9

2	Оценка информационных рисков.	4 неделя	9
3	Управление рисками. Основные понятия.	6 неделя	9
4	Методики и технологии управления рисками.	10 неделя	9
5	Разработка корпоративной методики анализа рисков.	16 неделя	9
6	Современные методы и средства анализа и управление рисками информационных систем компаний.	18 неделя	9
Итого			53,9

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 за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

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

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

–методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методи-

ческой литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-9. Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах.	Организация и управление службой защиты информации. Работа с конфиденциальной информацией.	Организация и управление службой защиты информации. Работа с конфиденциальной информацией.	Экономика защиты информации. Подготовка к процедуре защиты и защита выпускной квалификационной работы.
ПК-10. Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности.	Экономика защиты информации.	Экономика защиты информации.	Экономика защиты информации. Производственная преддипломная практика. Подготовка к процедуре защиты и защита выпускной квалификационной работы.

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа из п.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ПК-9, завершающий.	ПК-9.3 Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации.	Знать: терминологию теории управления рисками, задачи и функции службы защиты информации, типовые должностные обязанности персонала, обслуживающего защищённые АС. Уметь: применять типовые методики для получения характеристик рисков ИБ, настраивать оборудование АС. Владеть: базовыми навыками оценки рисков информационной безопасности, навыками применения программных и аппаратных средств защиты информации в АС.	Знать: основные методики оценки рисков, состав, документацию, характеристики и принцип работы оборудования АС. Уметь: использовать основные модели оценки рисков для получения количественных и качественных оценок рисков, применять средства защиты информации в АС. Владеть: навыками навыками оценки рисков информационной безопасности, разработки архитектуры АС.	Знать: теоретические основы, лежащие в основе современных методик управления рисками, классификацию, состав, документацию, способы применения средств защиты информации в АС. Уметь: использовать модели оценки рисков для формирования политики управления рисками и проектирования системы управления рисками, осуществлять контроль работ по защите АС, проводить анализ результатов выполняемых работ. Владеть: навыками оценки рисков информационной безопасности и проекти-

				рования систем управления корпоративными рисками, контроля и анализа результатов выполняемых работ.
ПК-10, завершающий.	ПК-10.1 Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информаци.	Знать: терминологию теории управления рисками, типовые инциденты информационной безопасности АС. Уметь: применять типовые методики для получения характеристик рисков ИБ, классифицировать инциденты информационной безопасности АС. Владеть: базовыми навыками оценки рисков информационной безопасности, навыками применения программных и аппаратных средств защиты информации в АС.	Знать: состав, документацию, характеристики и принцип работы оборудования АС. Уметь: применять средства защиты информации в АС, определять уязвимые узлы в системе информационной безопасности. Владеть: навыками обнаружения инцидентов и восстановления функционирования оборудования АС.	Знать: классификацию, состав, документацию, способы применения систем и средств защиты информации в АС. Уметь: осуществлять контроль функционирования систем и средств защиты АС, проводить анализ результатов выполняемых работ. Владеть: навыками контроля и анализа результатов выполняемых работ.
	ПК-10.2 Обосновывает необходимость модернизации системы защиты информации автоматизированной системы.	Знать: терминологию теории управления рисками, задачи и функции службы защиты информации, типовые должностные обязанности персонала, обслуживающего защищённые АС. Уметь: применять типовые методики для получения характеристик рисков ИБ, проводить анализ инцидентов информационной безопасности	Знать: состав, документацию, характеристики и принцип работы оборудования АС. Уметь: определять уязвимые места системы безопасности АС, разрабатывать архитектуры сети с учётом уязвимых мест. Владеть: навыками определения уязвимых мест систе-	Знать: классификацию, состав, документацию, способы применения средств защиты информации в АС, типовые инциденты информационной безопасности АС и способы их предотвращения. Уметь: разрабатывать состав и требования к системам информационной безопасности АС

		АС. Владеть: базовыми навыками оценки рисков информационной безопасности, навыками анализа инцидентов информационной безопасности АС.	мы безопасности АС, принятия мер для восстановления функционирования системы.	в интересах модернизации АС. Владеть: навыками разработки архитектуры сетей с учётом уязвимых мест, разработки предложений по составу и требованиям к системам информационной безопасности АС в рамках модернизации АС.
	ПК-10.4 Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем.	Знать: терминологию теории управления рисками, задачи и функции систем и средств мониторинга и управления средствами обеспечения безопасности АС. Уметь: применять типовые методики для получения характеристик рисков ИБ, проводить анализ защищенности АС. Владеть: базовыми навыками оценки рисков информационной безопасности, навыками анализа защищенности АС.	Знать: правила эксплуатации оборудования и программных средств управления средствами защиты АС. Уметь: разрабатывать правила протоколирования результатов мониторинга АС. Владеть: навыками эксплуатации программных средств мониторинга и управления средствами зашиты АС.	Знать: классификацию и способы применения средств и систем защиты АС. Уметь: настраивать оборудования и программных средств мониторинга и управления средствами защиты АС, средства и системы защиты АС. Владеть: навыками разработки правил протоколирования результатов мониторинга АС, настройки оборудования и программных средств мониторинга и управления средствами защиты АС, средств и систем защиты АС.

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 основной профессиональной образовательной программы

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия и содержание дисциплины «Оценка рисков информационной безопасности».	ПК-9, ПК-10	Лекция, СРС	Вопросы для устного опроса	1-12	Согласно таблице 7.2
2	Оценка информационных рисков.	ПК-9, ПК-10	Лекция, практическая работа №1, СРС	Вопросы для устного опроса	13-15	Согласно таблице 7.2
				КВЗПР №1	1-5	
3	Управление рисками. Основные понятия.	ПК-9, ПК-10	Лекция, практическая работа №2, СРС	Вопросы для устного опроса	16-21	Согласно таблице 7.2
				КВЗПР №2	1-6	
4	Методики и технологии управления рисками.	ПК-9, ПК-10	Лекция, практическая работа №3, СРС	Вопросы для устного опроса	22-24	Согласно таблице 7.2
				КВЗПР №3	1-4	
5	Разработка корпоративной методики анализа рисков.	ПК-9, ПК-10	Лекция, практическая работа №4, СРС	Вопросы для устного опроса	25-32	Согласно таблице 7.2
				КВЗПР №4	1-4	
6	Современные методы и средства анализа и управление рисками информационных систем компаний.	ПК-9, ПК-10	Лекция, практическая работа №5, СРС	Вопросы для устного опроса	33-36	Согласно таблице 7.2
				КВЗПР №5	1-5	

СРС – самостоятельная работа студента,
КВЗПР - контрольные вопросы для защиты практических работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

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

1. Становление индустрии информации.
2. Назовите основные элементы системы защиты информации.
3. В чём заключаются преимущества и недостатки качественных методик управления рисками?
4. Опишите метод COBRA.
5. Опишите метод RA Software Tool
6. Возможно ли применение метода RA Software Tool для описание рисков в системах, обрабатывающих гостайну и почему?
7. Опишите метод CRAMM.
8. Какой из методов управления рисками наиболее предпочтителен в национальной системе стандартов информационной безопасности и почему?
9. Какие существуют способы снижения рисков?
10. Что такое система управления рисками, её назначение?

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.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачёта.

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Методы анализа риска:
А) Хаотический.
Б) Единичный.
В) Статистический.
Г) Периодический.

Задание в открытой форме:

1. Видами рисков в предпринимательской деятельности являются……..

2. В процессе функционирования предприятие подвергается следующим угрозам……..

3. К методам анализа риска относятся…….

4. Способами минимизации рисков являются……

Задание на установление правильной последовательности.

Установить в этапы построения комплексной системы защиты информации в порядке их реализации:

1. Выявление потенциально возможных угроз

2. Анализ состояния подсистем обеспечения безопасности

3. Обоснование структуры и технологии функционирования комплексной системы защиты информации

4. Предварительное обследование состояния объекта и уровня организации защиты информации

Задание на установление соответствия:

между элементами затрат и функциями затрат

1	Затраты на обслуживание системы информационной безопасности	А	Затраты на идентификацию угроз безопасности
2	Затраты на контроль работы системы безопасности	Б	Затраты на доставку и обмен конфиденциальной информации
3	Затраты на обеспечение должного качества информационных технологий и их соответствия требованиям стандартов	В	Затраты на обслуживание и настройку программно-технических средств защиты
4	Затраты, связанные с пересмотром политики информационной безопасности предприятия	Г	Затраты на контроль за действиями персонала

способов и видов информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
4	По способу восприятия	Г	Непрерывная, дискретная

Компетентностно-ориентированная задача:

Оцените величину нанесенного организации ущерба и уровень защиты предприятия по частному функциональному критерию эффективности принимаемых мер.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

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

– положение П 02.016–2018 О балльно - рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

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

Для *текущего контроля успеваемости* 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
Устный опрос по темам 1-3	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Устный опрос по темам 4-6	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
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%
Практическая работа №5 «Минимизация риска и защита информации при заключении договоров»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:
- задание в закрытой форме –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

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

8.1 Основная учебная литература

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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

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.

13. Аверченков, В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков. - 2-е изд., стер. - М. : Флинта, 2011. - 269 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=93245

14. Балабанов, И. Т. Риск-менеджмент [Текст] / И. Т. Балабанов. - М. : Финансы и статистика, 1996. - 192 с.

15. Рогов, М. А. Риск-менеджмент [Текст] : монография / М. А. Рогов. - М. : Финансы и статистика, 2001. - 120 с.

16. Волков, О. И. Экономика предприятия [Текст] : курс лекций / В. К. Скляренко. - М.: ИНФРА-М, 2002. - 274 с.

17. Экономическая безопасность [Текст]: учебное пособие / [В. А. Богомолов [и др.] ; под ред. В. А. Богомолова. - 2-е изд., перераб. и доп. - Москва : ЮНИТИ, 2014. - 295 с.

18. Ковалев, В. В. Методы оценки инвестиционных проектов [Текст] / В. В. Ковалев. - М.: Финансы и статистика, 2001. - 144 с.

19. Крысин, А. В. Безопасность предпринимательской деятельности [Текст] / А. В. Крысин. - М.: Финансы и статистика, 1996. - 380 с.

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 информационной безопасности : 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.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.» - http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компью терные системы» - http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»
5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».

5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft [официальный сайт].
8. http://www.consultant.ru Компания «Консультант Плюс» [официальный сайт].

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Оценка рисков информационной безопасности» являются лекции и 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 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 информационной безопасности»: 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 лекций, участие в групповых и индивидуальных консультациях (собеседованиях). 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 закрепления 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 информационной безопасности» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Оценка рисков информационной безопасности» - 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 №K0000000117 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 типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проектор inFocusIN24+

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14. 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			