

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной и прикладной информатики

Дата подписания: 11.05.2023 18:22:25

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddb475e411a

## **Аннотация к рабочей программе дисциплины «Экономика защиты информации»**

### **Цель преподавания дисциплины**

Целью преподавания дисциплины «Экономика защиты информации» 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.

### **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;
- 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.

### **Индикаторы компетенций, формируемые в результате освоения дисциплины**

ПК-9.3 Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации.

ПК-10.1 Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации.

ПК-10.2 Обосновывает необходимость модернизации системы защиты информации автоматизированной системы.

ПК-10.4 Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем.

### **Разделы дисциплины**

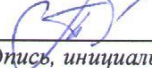
Основные понятия и содержание дисциплины «Экономика защиты информации». Экономические проблемы информационных ресурсов и защиты информации. Экономика информации, неопределённости и риска. Ценообразование на информационные продукты и услуги. Себестоимость информационных продуктов и услуг. Экономическая безопасность фирмы. Оценка эффективности создания и функционирования системы защиты информации. Страхование, как способ и метод защиты вложений.

## 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

Экономика защиты информации*(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)*

Рабочая программа дисциплины Экономика защиты информации 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 2021г.).

Рабочая программа дисциплины Экономика защиты информации 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  
Разработчик программы  
к.воен.н., доцент  
Директор научной библиотеки



Таныгин М.О.



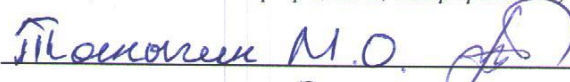
Ханис А.Л.

Макаровская В.Г.

Рабочая программа дисциплины Экономика защиты информации 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 2021г., на заседании кафедры ИБ ИИ от 30.06.22г..

(наименование кафедры, дата, номер протокола)

Зав. кафедрой



Рабочая программа дисциплины Экономика защиты информации 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 «Экономика защиты информации» 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.

### **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;
- 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**

Таблица 1.3 – Результаты обучения по дисциплине

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
ПК-9	Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах.	ПК-9.3 Сопоставляет результат работы персонала, обслуживающего защищенную автоматизированную систему, с целевыми показателями функционирования службы защиты информации.	<p><b>Знать:</b> задачи и функции службы защиты информации (СЗИ), типовые должностные обязанности персонала, обслуживающего защищенные АС, состав, документацию, характеристики и принцип работы оборудования АС, классификацию, состав, документацию, способы применения средств защиты информации в АС.</p> <p><b>Уметь:</b> настраивать оборудование АС, применять средства защиты информации в АС, осуществлять контроль работ по защите АС, проводить анализ результатов выполняемых работ.</p> <p><b>Владеть:</b> навыками применения программных и аппаратных средств защиты информации в АС, разработки архитектуры АС, контроля и анализа результатов выполняемых работ.</p>
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.	<p><b>Знать:</b> 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.</p> <p><b>Уметь:</b> 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.</p> <p><b>Владеть:</b> навыками применения программных и аппаратных</p>



<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>средств защиты информации в АС, обнаружения инцидентов и восстановления функционирования оборудования АС, контроля и анализа результатов выполняемых работ.</p>
		<p>ПК-10.2 Обосновывает необходимость модернизации системы защиты информации автоматизированной системы.</p>	<p><b>Знать:</b> 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.</p> <p><b>Уметь:</b> 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.</p> <p><b>Владеть:</b> 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.</p>
		<p>ПК-10.4 Формулирует пра-</p>	<p><b>Знать:</b> задачи и функции систем и средств мониторинга и управ-</p>

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
		вила протоколирования результатов мониторинга безопасности автоматизированных систем.	ления средствами обеспечения безопасности АС, правила эксплуатации оборудования и программных средств управления средствами защиты АС, классификацию и способы применения средств и систем защиты АС. <b>Уметь:</b> 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. <b>Владеть:</b> навыками анализа защищенности АС, эксплуатации программных средств мониторинга и управления средствами защиты 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 10.03.01 Информационная безопасность, направленность «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий». 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 АтКР)	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 «Экономика защиты информации».	Становление индустрии информации. Характеристики информации. Характеристики информационного общества. Аспекты защиты информации. Экономика защиты информации как наука, задачи экономики защиты информации. Экономические проблемы ЗИ. Информация как товар.



2	Экономические проблемы информационных ресурсов и защиты информации.	Производственные ресурсы предприятия и служб защиты информации. Информационные технологии. Финансовые ресурсы организации. Информационные технологии. Финансовые ресурсы организации. Основные этапы инновационного процесса. Инновационный проект. Эффективность инноваций.
3	Экономика информации, неопределенности и риска.	Выбор в условиях неопределенности. Неопределенность и риск. Информационные продукты и услуги. Основные виды информационных услуг.
4	Ценообразование на информационные продукты и услуги. Себестоимость информационных продуктов и услуг.	Сущность и состав себестоимости. Специфические принципы учета информационных затрат. Основные направления расходов на защиту информации. Ценовая политика организации. Методы расчета цен на информационные продукты.
5	Экономическая безопасность фирмы.	Роль информации в предпринимательской деятельности. Стратегическая информация предприятия. Стратегическая информация предприятия. Способы несанкционированного доступа к конфиденциальной информации и показатели эффективности добывания информации.
6	Оценка эффективности создания и функционирования системы защиты информации. Страхование, как способ и метод защиты вложений.	Методы наращивания и дисконтирования. Модифицированная норма доходности. Сущность, содержание и виды рисков. Способы оценки степени риска. Сущность, содержание и виды страхования. Страхование информационных рисков. Организационно-правовые формы организация страховой деятельности.

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 «Экономика защиты информации».	2	-	-	У-1-8, У-9, У-10 МУ-2	УО- 2	ПК-9, ПК-10
2	Экономические проблемы информационных ресурсов и защиты информации.	2	-	1	У-1-8, У-11, У-12, МУ-1,2	УО – 4, ЗПР - 4	ПК-9, ПК-10
3	Экономика информации, неопределенности и риска.	2	-	2	У-1- 8, У-9- У-13, МУ-1,2	УО-6, ЗПР - 6	ПК-9, ПК-10
4	Ценообразование на информационные продукты и услуги. Себестоимость информационных продуктов и услуг.	2	-	3	У-1- 8, У-9, У-14, МУ-1,2	УО-10, ЗПР - 10	ПК-9, ПК-10

5	Экономическая безопасность фирмы.	2	-	4	У-1-8, У-9, У-12- МУ-1,2	УО-14, ЗПР - 14	ПК-9, ПК-10
6	Оценка эффективности создания и функционирования системы защиты информации. Страхование, как способ и метод защиты вложений.	2	-	5	У-1-8, У-10-14 МУ-1,2	УО-18, ЗПР - 18	ПК-9, ПК-10
	Всего	36					

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 занятия	Объем, час.
1	Система конфиденциальной информации коммерческой организации.	4
2	Коммерческая тайна организации.	4
3	Минимизация риска и защита информации при заключении договоров.	4
4	Организация работ при подборе кадров и контроле сотрудников.	4
5	Защита информации в условиях возникновения чрезвычайных ситуаций.	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 «Экономика защиты информации».	2 неделя	8,9
2	Экономические проблемы информационных ресурсов и защиты информации.	4 неделя	9
3	Экономика информации, неопределенности и риска.	6 неделя	9
4	Ценообразование на информационные продукты и услуги. Себестоимость информационных продуктов и услуг.	10 неделя	9
5	Экономическая безопасность фирмы.	16 неделя	9

6	Оценка эффективности создания и функционирования системы защиты информации. Страхование, как способ и метод защиты вложений.	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 УП и 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:
  - методических рекомендаций, пособий по организации самостоятельной работы студентов;
  - вопросов к зачету;
  - методических указаний к выполнению практических работ и т.д.

*типографией университета:*

- помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

## 6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

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.

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения практиченских занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю, специализации) программы бакалавриата.

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, представителями работодателей (командная работа, разбор конкретных ситуаций, и др.);

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

## 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.	Оценка рисков информационной безопасности Экономика защиты информации.
ПК-10. Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности.	Оценка рисков информационной безопасности.	Оценка рисков информационной безопасности.	Оценка рисков информационной безопасности Экономика защиты информации. Производственная преддипломная практика.

### 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 персо-	Знать: задачи и функции службы защиты информации, типовые	Знать: состав, документацию, характеристики и прин-	Знать: классификацию, состав, документацию, способы

	нала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации.	должностные обязанности персонала, обслуживающего защищённые АС. Уметь: настраивать оборудование АС. Владеть: навыками применения программных и аппаратных средств защиты информации в АС.	ции работы оборудования АС. Уметь: применять средства защиты информации в АС. Владеть: навыками разработки архитектуры АС.	применения средств защиты информации в АС. Уметь: осуществлять контроль работ по защите АС, проводить анализ результатов выполняемых работ. Владеть: навыками контроля и анализа результатов выполняемых работ.
ПК-10/ завершающий.	<p>ПК-10.1 Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации.</p> <p>ПК-10.2 Обосновывает необходимость модернизации системы защиты информации автоматизированной системы.</p>	<p>Знать: типовые инциденты информационной безопасности АС. Уметь: классифицировать инциденты информационной безопасности АС. Владеть: навыками применения программных и аппаратных средств защиты информации в АС.</p> <p>Знать: задачи и функции службы защиты информации, типовые должностные обязанности персонала, обслуживающего защищённые АС. Уметь: проводить анализ инцидентов информационной безопасности АС.</p>	<p>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.</p> <p>Знать: состав, документацию, характеристики и принцип работы оборудования АС. Уметь: определять уязвимые места системы безопасности АС, разрабатывать архитектуру сети с</p>	<p>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.</p> <p>Знать: классификацию, состав, документацию, способы применения средств защиты информации в АС, типовые инциденты информационной безопасности АС и способы их предотвращения.</p>

	<p>ПК-10.4          Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем.</p>	<p>Владеть: навыками анализа инцидентов информационной безопасности АС.</p> <p>Знать: задачи и функции систем и средств мониторинга и управления средствами обеспечения безопасности АС.</p> <p>Уметь: проводить анализ защищенности АС.</p> <p>Владеть: Навыками анализа защищенности АС.</p>	<p>учётом уязвимых мест.</p> <p>Владеть: навыками определения уязвимых мест системы безопасности АС, принятия мер для восстановления функционирования системы.</p> <p>Знать: правила эксплуатации оборудования и программных средств управления средствами защиты АС.</p> <p>Уметь: разрабатывать правила протоколирования результатов мониторинга АС.</p> <p>Владеть: навыками эксплуатации программных средств мониторинга и управления средствами защиты АС.</p>	<p>Уметь: разрабатывать состав и требования к системам информационной безопасности АС в интересах модернизации АС.</p> <p>Владеть: навыками разработки архитектуры сетей с учётом уязвимых мест, разработки предложений по составу и требованиям к системам информационной безопасности АС в рамках модернизации АС.</p> <p>Знать: классификацию и способы применения средств и систем защиты АС.</p> <p>Уметь: настраивать оборудование и программных средств мониторинга и управления средствами защиты АС, средства и системы защиты АС.</p> <p>Владеть: навыками разработки правил протоколирования результатов мониторинга АС, настройки оборудования и программных средств мониторинга и управления средствами защиты АС, средств и систем защиты АС.</p>
--	--	--	---	---



**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 «Экономика защиты информации».	ПК-9, ПК-10	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
2	Экономические проблемы информационных ресурсов и защиты информации.	ПК-9, ПК-10	Лекция, практическая работа №1, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
				КВЗПР №1	1-12	
3	Экономика информации, неопределенности и риска.	ПК-9, ПК-10	Лекция, практическая работа №2, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
				КВЗПР №2	1-13	
4	Ценообразование на информационные продукты и услуги. себестоимость информационных продуктов и услуг.	ПК-9, ПК-10	Лекция, практическая работа №3, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
				КВЗПР №3	1-13	
5	Экономическая безопасность фирмы.	ПК-9, ПК-10	Лекция, практическая работа №4, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
				КВЗПР №4	1-11	
6	Основные понятия и содер-	ПК-9, ПК-10	Лекция, практиче-	Вопросы для устного опроса	1-11	Согласно таблице 7.2

	жание дисциплины «Экономика защиты информации».		ская работа №5, СРС	КВЗПР №5	1-11	
--	---	--	---------------------	----------	------	--

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) 1. «Основные понятия и содержание дисциплины «Экономика защиты информации».

1. Становление индустрии информации.
2. Назовите основные элементы системы защиты информации.
3. Экономика защиты информации как наука, задачи экономики защиты информации.
4. Назовите экономические проблемы защиты информации.
5. Организация как объект защиты информации.

Контрольные вопросы для защиты практической работы №1:

1. Какова роль информации в проведении конкурентной борьбы?
2. Почему информация также является товаром?
3. Какими основными свойствами обладает информация как товар?
4. Какими другими свойствами обладает информация как товар?
5. Что представляет собой рынок информации в России?

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 компьютерного 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. Затраты на обеспечение информационной безопасности предприятия можно подразделить на:

- А) Периодические.
- Б) Единовременные.
- В) Разовые.
- Г) Постоянные.

Задание в открытой форме:

1. Экономическая безопасность предприятия характеризуется.....
2. В процессе функционирования предприятие подвергается следующим угрозам.....
3. При построении эффективной системы информационного обеспечения необходимо решать задачи.....
4. Создание системы защиты информации на предприятии обеспечивает.....

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
		Г	Затраты на контроль за действиями персонала

Компетентностно-ориентированная задача:

Компания А стоит перед выбором между двумя вариантами решений по защите информации. Вариант 1: внедрение новой системы безопасности стоит 100000 долларов и приведет к сокращению потенциальных убытков от утечек информации на 60%. Вариант 2: найм дополнительного персонала стоит 50000 долларов в год и приведет к сокращению потенциальных убытков на 40%. Какой вариант решения является более экономически выгодным для компании А? Ответ обоснуйте.

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 «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 «Система конфиденциальной информации коммерческой организации»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Практическая работа №2 «Коммерческая тайна организации»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Практическая работа №3 «Минимизация риска и защита информации при заключении договоров»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Практическая работа №4 «Организация работ при подборе кадров и контроле сотрудников»	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%

Практическая работа №5 «Защита информации в условиях возникновения чрезвычайных ситуаций»	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. 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).

URL: <https://biblioclub.ru/index.php?page=book&id=573397> (дата обращения: 23.08.2021).- Режим доступа: по подписке – Текст : электронный.

6. Тихомиров, Н. П. Теория риска : учебник / Н. П. Тихомиров, Т. М. Тихомирова ; Российский экономический университет им. Г.В. Плехана.

нова. – 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). – Текст : электронный.

7. Ханис, Андрей Леонидович. 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. - Текст : непосредственный.

8. Ханис, Андрей Леонидович. 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. - Текст : электронный.

## **8.2 Дополнительная учебная литература**

9. 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. 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.

5. 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). – Текст : электронный.

10. 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). – Текст : электронный.



11. Остапенко, Е. А. Финансовая среда и предпринимательские риски : учебное пособие / Е. А. Остапенко, Т. Г. Гурнович. – Ставрополь : Севквой, 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). – Текст : электронный.

12. 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). – Текст : электронный.

13. 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). – Текст : электронный.

14. 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). – Текст : электронный.

### **8.3 Перечень методических указаний**

1. Экономика защиты информации : методические указания по выполнению практических работ студентов всех форм обучения / Юго-Зап. гос. ун-т; сост.: А.Л. Ханис. - Курск, 2021. - 26 с. - Текст : электронный.

2. Экономика защиты информации : 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. Компьютерные 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 «Экономика защиты информации» 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 «Экономика защиты информации»: 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 немислима 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 «Экономика защиты информации» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Экономика защиты информации» - 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)**

MicrosoftOffice 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 лабораторий кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aок 21". Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

## **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 присут-

ствии 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
	Изменённых	Заменённых	Аннулированных	Новых			