Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»

Стахановский инженерно-педагогический институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Луганский государственный университет имени Владимира Даля»

Кафедра информационных систем

УТВЕРЖДАЮ:
Директор СИПИ (филиала)
ФГБОУ ВО «ЛГУ им. В. Даля»
_____А.А. Авершин
(подпись)
«_21_» апреля 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ»

По направлению подготовки 38.05.01 Экономическая безопасность

Специализация: «Экономико-правовое обеспечение экономической безопасности»

Луганск – 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Информационная безопасность экономической деятельности» по направлению подготовки 38.05.01 Экономическая безопасность. – 25 с.

Рабочая программа учебной дисциплины «Информационная безопасность экономической деятельности» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.05.01 Экономическая безопасность, утвержденным приказом Министерства образования и науки Российской Федерации от 16 января 2017 г. № 20 (с изменениями и дополнениями от 14 апреля 2021 г.)

СОСТАВИТЕЛЬ:
канд. техн. наук, доцент Карчевский В.П.

Рабочая программа дисциплины утверждена на заседании кафедры информационных систем «18» апреля 2023 г., протокол № 9

Заведующий кафедрой
информационных систем _____ В.П. Карчевский

Переутверждена: «___» _____20___ г., протокол № _____ .

Переутверждена: «___» _____20___ г., протокол № _____ .

Согласована:
Заведующий кафедрой
социально-экономических и педагогических дисциплин _____ Н.В. Карчевская

Рекомендована на заседании учебно-методической комиссии Стахановского инженерно-педагогического института (филиала) федерального государственного бюджетного образовательного учреждения высшего образования «Луганский государственный университет имени Владимира Даля» «21» апреля 2023 г., протокол № 3.

Председатель учебно-методической комиссии
СИПИ (филиала) ФГБОУ ВО «ЛГУ им. В. Даля» _____ Н.В. Банник

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Целью изучения дисциплины «Информационная безопасность экономической деятельности» является формирование системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации в профессиональной деятельности.

Основными **задачами** изучения дисциплины «Информационная безопасность экономической деятельности» являются:

формирование умения обеспечить защиту информации и объектов информатизации;

формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов;

формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; настройка и обслуживание аппаратно-программных средств.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Информационная безопасность экономической деятельности входит в модуль «Математический и естественнонаучный». Необходимыми условиями для освоения дисциплины являются: знания направлений развития и перспектив защиты информации; основных понятий и задач информационной безопасности; видов угроз компьютерной информации; умения работать с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий (ИКТ); организовывать собственную информационную деятельность и планировать ее результаты; устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; навыки принятия решений; эксплуатации технических и программных средств информационных сетей.

Содержание дисциплины является логическим продолжением содержания дисциплин: «Информатика и информационные технологии в экономике», «Математика», «История экономических учений» и служит основой для освоения дисциплин: «Экономическая безопасность», «Планирование деятельности предприятия».

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ОПК-6. Способен использовать современные информационные технологии и	ОПК-6.1. Знает современные информационные технологии и программные средства, методы обработки информации	Знать: виды угроз компьютерной информации; программные методы защиты информации; законодательное регулирование

программные средства при решении профессиональных задач	ОПК-6.2. Умеет использовать методы и средства решения задач экономического характера с использованием информационных технологий и программных средств ОПК-6.3. Владеет навыками использования офисных программных продуктов, правовых информационных систем, поиска информации в интернет, статистической обработки информации	информационной безопасности; основные понятия и задачи информационной безопасности; виды угроз компьютерной информации; теоретические основы информационных технологий по применению ЭВМ в расчётах; понятия и определения, используемые в сфере информационной безопасности.
		Уметь: применять методы защиты компьютерной информации в различных предметных областях; работать с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий (ИКТ); организовывать собственную информационную деятельность и планировать ее результаты.
		Владеть: методами использования основных положений теории информационной безопасности в различных информационных системах; навыками формирование общих требований к организации безопасности локальных сетей с учетом анализа угроз и различных групп нарушителей; навыками принятия решений;
ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7.1. Знает перспективы развития информационных технологий и ресурсов, основные принципы работы современных информационных технологий в сетях различного уровня, принципы организации различных сервисов сети Internet ОПК-7.2. Умеет работать с различными информационными ресурсами и технологиями; использует программное обеспечение для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) ОПК-7.3. Применяет основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации при решении профессиональных задач ОПК-7.4. Владеет навыками работы в корпоративных информационных системах и глобальных компьютерных	Знать: методы и средства обеспечения информационной безопасности компьютерных систем; основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам; основные понятия и направления в защите компьютерной информации, принципы защиты информации; принципы классификации и примеры угроз безопасности компьютерным системам.
		Уметь: устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; настраивать инструменты резервного копирования и восстановления информации.
		Владеть: эксплуатации технических и программных средств информационных сетей; навыками постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей; методами системного анализа информационных систем.

	сетях; навыками использования в профессиональной деятельности сетевых средств поиска и обмена информацией	

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов (зач. ед.)**		
	Очная форма	**Очно-заочная форма**	**Заочная форма**
Объем учебной дисциплины (всего)	**180 (5 зач. ед)**	-	**180 (5 зач. ед)**
Обязательная контактная работа (всего) в том числе:	**68**	-	**16**
Лекции	34	-	8
Семинарские занятия	-	-	-
Практические занятия	34	-	8
Лабораторные работы	-	-	
Курсовая работа (курсовой проект)	-	-	
Другие формы и методы организации образовательного процесса (*расчетно-графические работы, групповые дискуссии, ролевые игры, тренинг, компьютерные симуляции, интерактивные лекции, семинары, анализ деловых ситуаций и т.п.)*	-	-	
Самостоятельная работа студента (всего)	**112**	-	**164**
Итоговая аттестация	зачет	-	зачет

4.2. Содержание разделов дисциплины

Тема 1. Информационная безопасность: основные определения и положения.

Информация и её значение. Информационное пространство. Информационная безопасность. Защита информации. Система защиты информации. Информационные ресурсы.

Тема 2. Понятие информационных угроз и их виды.

Информационные угрозы, их виды и причины возникновения Компьютерные преступления, их виды. Понятие вирусов и антивирусных программ.

Тема 3. Программное обеспечение средств защиты информации.

Средства архивации информации. Антивирусные программы. Методы обнаружения и удаления компьютерных вирусов. Криптографическая защита

информации.

Тема 4. Правовая база регулирования информационной безопасности.

Деятельность специализированных международных организаций и объединений в сфере информационной безопасности. Нормативно-правовые акты в области информационной безопасности.

Тема 5. Методы и средства обеспечения информационной безопасности.

Политика безопасности и ее принципы. Обеспечение безопасности информационных систем.

Тема 6. Организация системы защиты информации.

Организационное обеспечение информационной безопасности. Этапы построения системы защиты информации.

Тема 7. Защита информации в Интернет.

Основные сервисы сети Интернет. Угрозы информационной безопасности в локальных и глобальных сетях. Меры защиты информации в сети Интернет.

Тема 8. Информационная безопасность в профессиональной деятельности.

Защита данных в профессиональной деятельности. Пользователи и администратор баз данных. Защита в базах данных.

Тема 9. Перспективные технологии в информационной безопасности экономической деятельности.

Электронная цифровая подпись и особенности ее применения. Политика безопасности. Информационная безопасность электронной коммерции

4.3. Лекции

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1.	Информационная безопасность: основные определения и положения.	4	-	1
2.	Понятие информационных угроз и их виды.	4	-	1
3.	Программное обеспечение средств защиты информации.	4	-	1
4.	Правовая база регулирования информационной безопасности.	4	-	1
5.	Методы и средства обеспечения информационной безопасности.	4	-	1
6.	Организация системы защиты информации.	2	-	1

7.	Защита информации в Интернет.	4	-	1
8.	Информационная безопасность в профессиональной деятельности.	4	-	0,5
9.	Перспективные технологии в информационной безопасности экономической деятельности.	4	-	0,5
Итого:		**34**	**-**	**8**

4.4. Лабораторные занятия не предусмотрены учебным планом

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
Итого:				

4.5. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1.	Безопасность ввода данных в информационных системах	4	-	0,5
2.	Защита данных в информационных системах.	4	-	1
3.	Архивация данных.	4	-	1
4.	Работа с антивирусными программами.	6	-	1
5.	Работа со внешними и внутренними накопителями.	2	-	1
6.	Программные средства для работы с внешними и внутренними накопителями.	4	-	1
7.	Работа с командной строкой.	4	-	1
8.	Защита информации в сети Интернет.	2	-	1
9.	Информационная безопасность в профессиональной деятельности.	4	-	0,5
Итого:		**34**	**-**	**8**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	Заочная форма
1.	Основные понятия и определения в области информационной безопасности.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	12
2.	Утечки информации: источники, правовые и технологические аспекты борьбы.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	12

3.	Безопасность Web-браузеров.	Подготовка к лабораторным и практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
4.	Безопасность беспроводных технологий.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
5.	Виртуальные частные сети (VPN) - технологии и средства организации.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
6.	Биометрические системы аутентификации: принципы, технологии и перспективы.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
7.	Средства взлома парольных систем и противодействие им.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
8.	Спам: способы распространения, принципы и средства противодействия	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
9.	Защита персональных данных, типовые решения.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
10.	Понятие политики безопасности.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
11.	Методы поиска уязвимостей в информационных системах.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
12.	Управление программным обеспечением, как аспект обеспечения информационной безопасности. Структура, требования, задачи.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	7	-	

13.	Безопасность современных сетевых технологий. Протоколы аутентификации.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	7	-	
14.	Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.	Подготовка к практическим занятиям, к текущему и промежуточному контролю знаний и умений.	8	-	
15.		Зачет	2		2
	Итого:		**112**		**164**

4.7. Курсовые работы/проекты по дисциплине «Информационная безопасность экономической деятельности» не предполагаются учебным планом.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий: объяснительно-иллюстративного обучения (технология поддерживающего обучения, технология проведения учебной дискуссии), информационных технологий (презентационные материалы), развивающих и инновационных образовательных технологий.

Практические занятия проводятся с использованием развивающих, проблемных, проектных, информационных (использование электронных образовательных ресурсов (электронный конспект) образовательных технологий.

6. Учебно-методическое и программно-информационное обеспечение дисциплины

а) основная литература:

1.

2. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/288974

б) дополнительная литература:

1. Келдыш Н.В. Информационная безопасность. Защита информации на объектах информатизации. Учебное пособие – М.: Мир науки, 2022. – Сетевое издание. Режим доступа: https://izdmn.com/PDF/14MNNPU22.pdf

2. Васильева И.Н. Интеллектуальные системы защиты информации : учебное пособие / И.Н. Васильева, Д.Ю. Федоров. – СПб. : Изд-во СПбГЭУ, 2020.%– 119 с. ISBN 978-5-7310-4986-3. Режим доступа: https://infosec.spb.ru/wp-content/uploads/2020/12/intellektualnye-sistemy-zashhity-informaczii.pdf

3. Терентьев А.И. Основы информационной безопасности. Методы и средства защиты компьютерной информации [Текст] : учебное пособие / А.И. Терентьев. – М. : ИД Академии Жуковского, 2020. – 84 с. ISBN 978-5-907275-59-1. — URL: http://storage.mstuca.ru/xmlui/handle/123456789/8842

в) методическая литература:

1. Карчевский В.П., Волков А.П., Чёрная Е.С., Авершина М.В., Тимошенко Д.С., Ганзенко И.В., Труфанова М.К., Владарский И.В. Исследование тенденций развития и инноваций в образовании с использованием искусственного интеллекта: учебное пособие для дополнительного изучения информационных технологий, робототехники и искусственного интеллекта в инженерно-педагогическом образовании для студентов очной и заочной форм обучения направления подготовки «Профессиональное обучение. Информационные технологии и системы» / В.П. Карчевский, А.П. Волков, Е.С. Чёрная, М.В. Авершина, Д.С. Тимошенко, И.В. Ганзенко, М.К. Труфанова, И.В. Владарский; под общ. редакцией В.П. Карчевского. – Луганск: СИПИМ ЛГУ им. В.ДАЛЯ, 2021. – 1024 с.

г) интернет-ресурсы:

Министерство науки и высшего образования РФ – https://minobrnauki.gov.ru/

Федеральная служба по надзору в сфере образования и науки – http://obrnadzor.gov.ru/

Портал Федеральных государственных образовательных стандартов высшего образования – http://fgosvo.ru

Федеральный портал «Российское образование» – http://www.edu.ru/

Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru/

Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru/

Электронные библиотечные системы и ресурсы

1. Электронно-библиотечная система «Консультант студента» – http://www.studentlibrary.ru/cgi-bin/mb4x

2. Электронная библиотека ФГБОУ ВО «ЮРГПУ (НПИ) имени М.И. Платова» «МегаПро» https://libweb.srspu.ru/MegaProWeb/Web.

Информационный ресурс библиотеки образовательной организации

3. Научная библиотека имени А. Н. Коняева – http://biblio.dahluniver.ru/

7. Материально-техническое и программное обеспечение дисциплины

Освоение дисциплины «Информационная безопасность экономической деятельности» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

Программное обеспечение:

Функциональное назначение	**Бесплатное программное обеспечение**	**Ссылки**
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплейер	VLC	http://www.videolan.org/vlc/

8. Оценочные средства по дисциплине

Паспорт
оценочных средств по учебной дисциплине
«Информационная безопасность экономической деятельности»

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины (модуля) или практики

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине	Контролируемые темы учебной дисциплины, практики	Этапы формирования (семестр изучения)
1	ОПК-6	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-6.1. Знает современные информационные технологии и программные средства, методы обработки информации ОПК-6.2. Умеет использовать методы и средства решения задач экономического характера с использованием информационных технологий и программных средств ОПК-6.3. Владеет навыками	Тема 1. Информационная безопасность: основные определения и положения. Тема 2. Понятие информационных угроз и их виды. Тема 3. Программное обеспечение средств защиты информации. Тема 4. Правовая база регулирования информационной	6

			использования офисных программных продуктов, правовых информационных систем, поиска информации в интернет, статистической обработки информации	безопасности. Тема 5. Методы и средства обеспечения информационной безопасности. Тема 6. Организация системы защиты информации. Тема 7. Защита информации в Интернет. Тема 8. Информационная безопасность в профессиональной деятельности. Тема 9. Перспективные технологии в информационной безопасности экономической деятельности.	
2	ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7.1. Знает перспективы развития информационных технологий и ресурсов, основные принципы работы современных информационных технологий в сетях различного уровня, принципы организации различных сервисов сети Internet ОПК-7.2. Умеет работать с различными информационными ресурсами и технологиями; использует программное обеспечение для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) ОПК-7.3. Применяет основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации при решении профессиональных задач ОПК-7.4. Владеет навыками работы в корпоративных информационных системах и глобальных компьютерных сетях; навыками использования в профессиональной деятельности сетевых средств поиска и обмена информацией	Тема 1. Информационная безопасность: основные определения и положения. Тема 2. Понятие информационных угроз и их виды. Тема 3. Программное обеспечение средств защиты информации. Тема 4. Правовая база регулирования информационной безопасности. Тема 5. Методы и средства обеспечения информационной безопасности. Тема 6. Организация системы защиты информации. Тема 7. Защита информации в Интернет. Тема 8. Информационная безопасность в профессиональной деятельности. Тема 9. Перспективные технологии в информационной безопасности экономической деятельности.	6

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код контроли-руемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов	Контроли-руемые темы учебной дисциплины	Наименование оценочного средства
1	ОПК-6	ОПК-6.1. Знает современные информационные технологии и программные средства, методы обработки информации ОПК-6.2. Умеет использовать методы и средства решения задач экономического характера с использованием информационных технологий и программных средств	Знать: виды угроз компьютерной информации; программные методы защиты информации; законодательное регулирование информационной безопасности; основные понятия и задачи информационной безопасности; виды угроз компьютерной информации; теоретические основы информационных технологий по применению ЭВМ в расчётах; понятия и определения, используемые в сфере информационной безопасности. Уметь: применять методы защиты компьютерной информации в различных	Тема 1; Тема 2; Тема 3; Тема 4; Тема 5 Тема 6; Тема 7; Тема 8; Тема 9.	Вопросы и задания к практическим работам, вопросы к контрольным работам, вопросы к зачету

		ОПК-6.3. Владеет навыками использования офисных программных продуктов, правовых информационных систем, поиска информации в интернет, статистической обработки информации	предметных областях; работать с различными видами информации с помощью компьютера и других средств информационных и коммуникационных технологий (ИКТ); организовывать собственную информационную деятельность и планировать ее результаты. Владеть: методами использования основных положений теории информационной безопасности в различных информационных системах; навыками формирование общих требований к организации безопасности локальных сетей с учетом анализа угроз и различных групп нарушителей; навыками принятия решений.		
2	ОПК-7	ОПК-7.1. Знает перспективы развития информационных технологий и ресурсов, основные принципы работы современных информационных технологий в сетях различного уровня, принципы организации различных сервисов сети Internet ОПК-7.2. Умеет работать с различными информационными ресурсами и технологиями; использует программное обеспечение для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) ОПК-7.3. Применяет основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации при решении профессиональных задач ОПК-7.4. Владеет навыками работы в корпоративных информационных системах и глобальных компьютерных сетях; навыками использования в профессиональной деятельности сетевых средств поиска и обмена информацией	Знать: методы и средства обеспечения информационной безопасности компьютерных систем; основные угрозы безопасности информации и возможные способы их реализации, а также методы и средства противодействия этим угрозам; основные понятия и направления в защите компьютерной информации, принципы защиты информации; принципы классификации и примеры угроз безопасности компьютерным системам. Уметь: устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; настраивать инструменты резервного копирования и восстановления информации. Владеть: эксплуатации технических и программных средств информационных сетей; навыками постановки и решения задачи обеспечения информационной безопасности компьютерных систем и сетей; методами системного анализа информационных систем.	Тема 1; Тема 2; Тема 3; Тема 4; Тема 5 Тема 6; Тема 7; Тема 8; Тема 9.	Вопросы и задания к практическим работам, вопросы к контрольным работам, вопросы к зачету

Оценочные средства по дисциплине «Информационная безопасность экономической деятельности»

Вопросы для обсуждения (в виде докладов и сообщений):

1. Свойства информации. Виды защищаемой информации. Источники угроз.
2. Компьютерные сети: основные понятия и виды угроз.
3. Принципы защиты информации в компьютерных сетях.
4. Программы для обеспечения информационной безопасности сети.
5. Основные понятия и определения в области информационной безопасности.
6. Утечки информации: источники, правовые и технологические аспекты борьбы.
7. Безопасность Web-браузеров.
8. Безопасность беспроводных технологий.
9. Виртуальные частные сети (VPN) - технологии и средства организации.
10. Биометрические системы аутентификации: принципы, технологии и перспективы.
11. Средства взлома парольных систем и противодействие им.
12. Спам: способы распространения, принципы и средства противодействия
13. Защита персональных данных, типовые решения.
14. Понятие политики безопасности.
15. Методы поиска уязвимостей в информационных системах.
16. Управление программным обеспечением, как аспект обеспечения информационной безопасности. Структура, требования, задачи.
17. Безопасность современных сетевых технологий. Протоколы аутентификации.
18. Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.

Критерии и шкала оценивания по оценочному средству «доклад, сообщение»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Доклад (сообщение) представлен(о) на высоком уровне (студентв полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Доклад (сообщение) представлен(о) на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)

3	Доклад (сообщение) представлен(о) на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Доклад (сообщение) представлен(о) на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

Вопросы к контрольным работам

1. Понятие атрибутов доступа к файлам. Защита сетевого файлового ресурса на примерах организации доступа в различных операционных системах.
2. Понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
3. Современные программно-аппаратные средства защиты компьютерной информации.
4. Несанкционированное копирование программ как тип несанкционированного доступа. Юридические аспекты несанкционированного копирования программ. Способы защиты от копирования.
5. Направления по защите от враждебных воздействий на безопасность компьютерных сетей.
6. Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий.
7. Понятие атрибутов доступа к файлам. Организация доступа к файлам в различных операционных системах
8. Способы фиксации фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам
9. Организационно-правовая основа защиты информации в ФСИН России.
10. Методы и средства защиты данных от несанкционированного доступа.
11. Понятие и содержание информационной безопасности.
12. Необходимость, назначение и общее содержание организационно-правового обеспечения информационной безопасности.
13. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.
14. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки
15. Уязвимость компьютерных систем. Понятие несанкционированного доступа (НСД). Классы и виды НСД
16. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки
17. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты
18. Требования и показатели защищенности автоматизированных средств обработки информации.

19. Технические методы защиты информации.

20. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.

21. Краткий обзор современных методов защиты информации.

22. Обеспечение информационной безопасности в каналах связи.

23. Меры противодействия информационной безопасности в автоматизированных системах обработки данных.

24. Особенности проблем защиты конфиденциальной информации.

32. К каким последствиям может привести действие компьютерного вируса?

33. Какими путями распространяется компьютерный вирус?

34. Какие средства защиты от вируса вы знаете?

35. Какие утилиты используются для очистки дисков? В чем отличия в их работе?

36. Что такое архивация данных? Для чего ее необходимо выполнять?

37. Как выполняется очистка реестра?

38. Какие утилиты для работы с дисками и реестром вам известны? Каковы их возможности?

Критерии и шкала оценивания по оценочному средству «контрольная работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Контрольная работа выполнена на высоком уровне (правильные ответы даны на 90-100% вопросов/задач)
4	Контрольная работа выполнена на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3	Контрольная работа выполнена на низком уровне (правильные ответы даны на 50-74% вопросов/задач)
2	Контрольная работа выполнена на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

Задания к практическим работам
Раздел «Безопасность ввода данных в информационных системах»

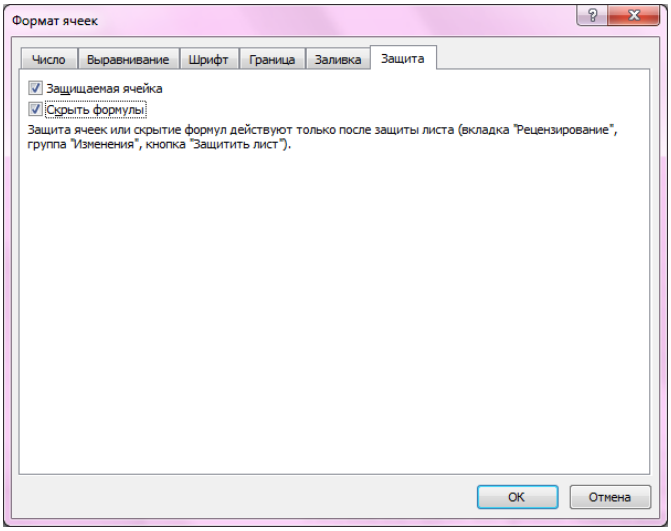
Защита листа или книги паролем

Защита элементов листа от всех пользователей

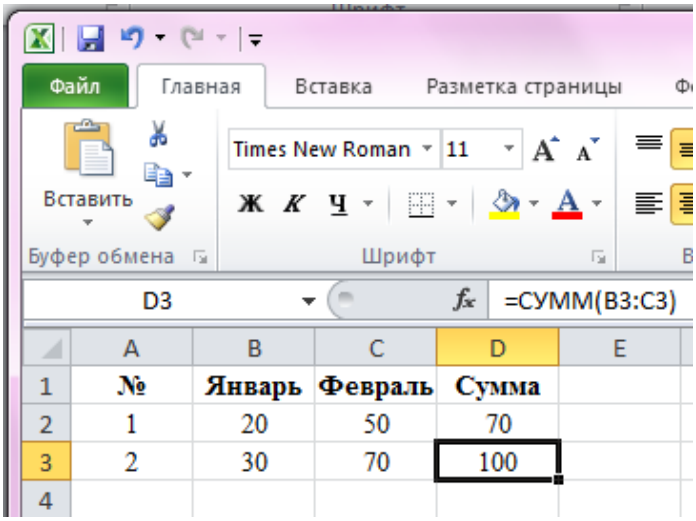
Откройте лист, который требуется защитить.

Разблокируйте все ячейки, которые должны быть доступны пользователям для изменения: выделите каждую ячейку или диапазон, выберите в меню Формат команду Ячейки, откройте вкладку Защита , а затем снимите флажок Защищаемая ячейка .

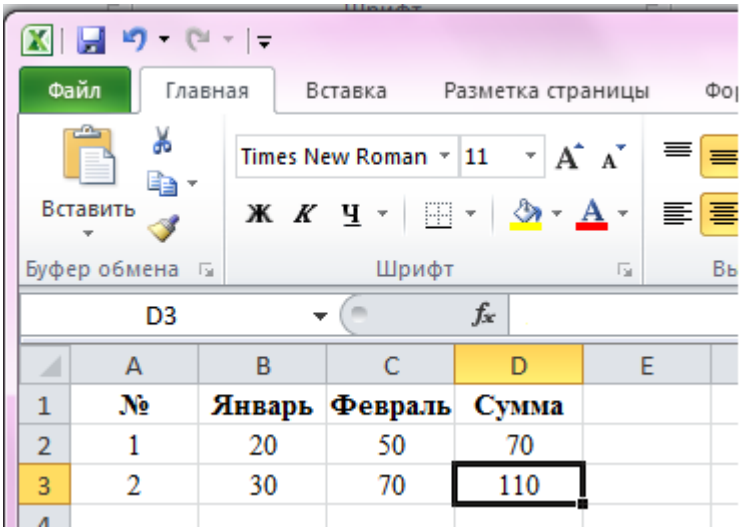
Скройте все формулы, которые не должны отображаться: выделите ячейки с этими формулами, выберите в меню **Формат** команду **Ячейки**, откройте вкладку **Защита** , а затем установите флажок **Скрыть формулы**.



Окно настройки защита ячеек и скрытие формул.

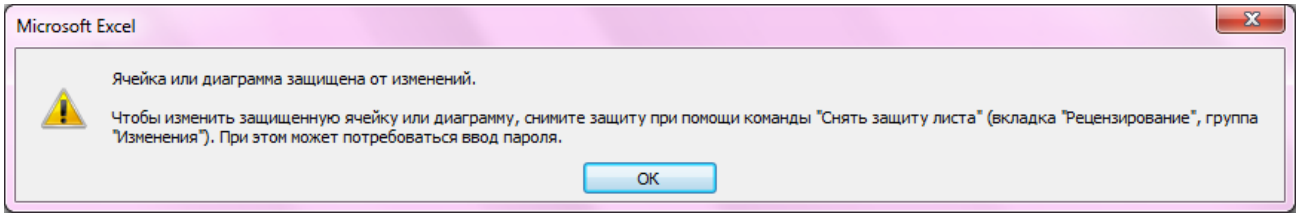


Лист без применения настройки «Скрыть формулы».



Лист с применением настройки «Скрыть формулы».

При попытке доступа к защищенным ячейкам появится сообщение.



Окно сообщения о защищенности объекта.

Разблокируйте все графические объекты, которые должны быть доступны пользователям для изменения.

Нет необходимости разблокировать кнопки и элементы, пользователи в любом случае смогут использовать их. Следует разблокировать внедренные диаграммы, надписи и другие рисованные объекты, которые должны быть доступны пользователям для изменения. Чтобы найти на листе графические объекты, выберите в меню **Правка** команду **Перейти**, нажмите кнопку **Выделить**, а затем установите переключатель в положение **объекты**.

- Удерживая нажатой клавишу **CTRL**, последовательно щелкните все объекты, которые требуется разблокировать.

- В меню **Формат** выберите команду, соответствующую выделенному объекту: Автофигура , Объект, Надпись, Рисунок, Элемент управления или Объект WordArt.

- Откройте вкладку **Защита**

- Снимите флажок **Защищаемый объект** и флажок **Скрыть текст** (если он отображается).

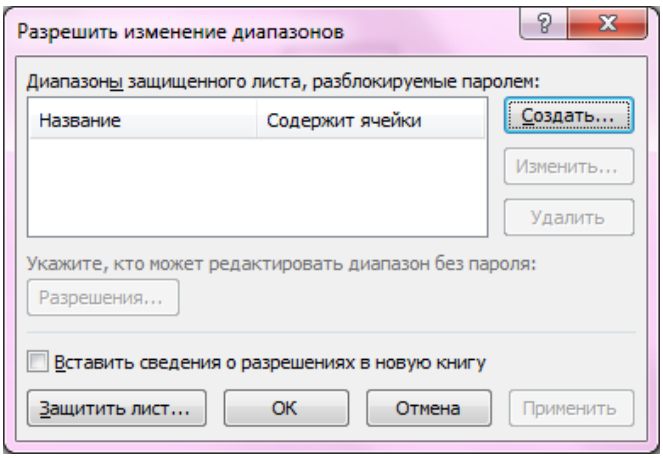
- В меню **Сервис** укажите на пункт **Защита** и выберите команду **Защитить лист**.

- Введите **пароль** для защиты листа.

Предоставление определенным пользователям доступа к защищенным диапазонам

Для предоставления определенным пользователям доступа к диапазонам ячеек требуется компьютер с операционной системой Microsoft Windows 2000 или более поздней версии, являющийся членом домена.

В меню **Сервис** укажите на пункт **Защита** , а затем выберите команду **Разрешить изменение диапазонов**. (Эта команда доступна, только если лист не защищен.)



Окно «Разрешить изменение диапазонов».

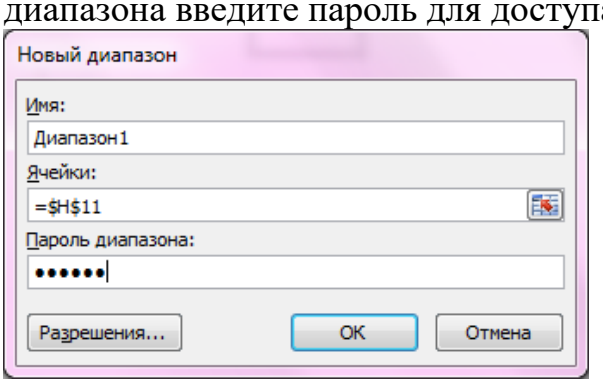
Нажмите кнопку **Создать**.

В поле **Имя** введите имя **диапазона**, доступ к которому требуется

предоставить.

В поле **Ячейки** введите знак равно (=), а затем введите ссылку или выделите диапазон ячеек.

В поле **Пароль** диапазона введите пароль для доступа к диапазону.



Окно создания диапазона.

Пароль задавать не обязательно, но если пароль не будет задан, любой пользователь сможет изменять эти ячейки.

Нажмите кнопку **Разрешения**, а затем — кнопку **Добавить.**

Найдите и выделите пользователей, которым требуется предоставить доступ. Чтобы выделить несколько пользователей, последовательно щелкните их имена, удерживая нажатой клавишу **CTRL**.

Два раза нажмите кнопку **OK** и, если будет предложено, введите пароль еще раз.

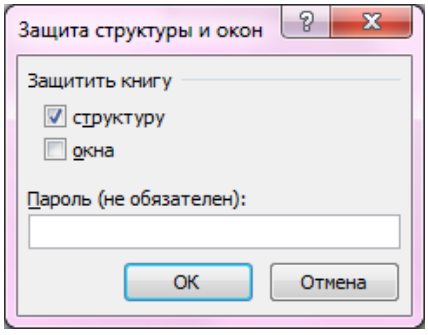
Повторите предыдущие шаги для всех диапазонов, к которым требуется предоставить доступ.

Чтобы сохранить отдельную запись диапазонов и пользователей, установите флажок Вставить сведения о разрешениях в новую книгу в диалоговом окне Разрешить изменение диапазонов.

Защитите лист: нажмите в диалоговом окне **Разрешить изменение диапазонов** кнопку **Защитить лист**.

Защита элементов книги

В меню **Сервис** укажите на пункт **Защита** , а затем выберите команду **Защитить книгу**.



Окно настроек защиты книги

Выполните одно или несколько следующих действий.

- Чтобы защитить структуру книги для запрета перемещения, удаления, скрытия, показа или переименования, а также вставки новых листов, установите флажок Структуру.

- Чтобы блокировать окна для восстановления их размера и расположения при каждом открытии книги, установите флажок Окна .

- Чтобы никто другой не смог снять защиту с листа, введите пароль,

нажмите кнопку ОК, а затем еще раз введите этот пароль для подтверждения.

Защита общей книги

Если книга уже общая, и ее требуется защитить паролем, запретите одновременную работу с ней нескольких пользователей.

Попросите других пользователей сохранить и закрыть общую книгу. В противном случае их несохраненные данные будут утеряны.

После прекращения совместной работы над книгой журнал изменений будет удален. Чтобы сохранить копию этих сведений, напечатайте лист изменений или скопируйте его в другую книгу.

1 В меню **Сервис** укажите на пункт **Исправления** и выберите команду **Выделить исправления**.

2 В поле по времени выберите вариант **Все**.

3 Снимите флажки пользователем и в диапазоне.

4 Установите флажок Вносить изменения на отдельный лист и нажмите кнопку ОК.

5 Выполните одно или несколько следующих действий:

- чтобы напечатать лист журнала, нажмите кнопку **Печать**;

- чтобы скопировать журнал в другую книгу, выделите ячейки, которые требуется скопировать, нажмите кнопку **Копировать**, переключитесь в окно другой книги, выделите ячейку, с которой требуется начать вставку, и нажмите кнопку **Вставить**.

В меню **Сервис** выберите команду **Доступ** к книге и откройте вкладку **Правка** .

Убедитесь, что вы единственный пользователь в списке Файл открыт следующими пользователями.

Снимите флажок **Разрешить совместный доступ.**

Если этот флажок недоступен, необходимо сначала отменить общий доступ к книге, а затем снять этот флажок.

Нажмите кнопку ОК, в меню Сервис укажите на пункт Защита и выберите команду Снять защиту общей книги.

Введите пароль, если он потребуется, и нажмите кнопку ОК.

В меню **Сервис** выберите команду **Доступ** к книге и откройте вкладку **Правка** .

Если появится сообщение о влиянии на других пользователей, нажмите кнопку Да .

При необходимости установите другие типы защиты: предоставьте определенным пользователям доступ к диапазонам, защитите листы, защитите элементы книги и задайте пароли для просмотра и изменения.

В меню **Сервис** укажите на пункт Защита , а затем выберите команду **Защитить книгу** и дать общий доступ.

Установите флажок **Общий доступ с исправлениями**.

Чтобы обязать других пользователей вводить пароль для прекращения ведения журнала изменений или удаления книги из общего пользования, введите пароль в поле **Пароль**, а затем введите его еще раз для подтверждения.

Если будет предложено, сохраните книгу.

Порядок выполнения работы

1. Создайте документ Excel, произведите в нем набор некоторых

символов (заполните несколько ячеек) и после этого произведите его сохранение. Имя для сохранения пример1.xls

2. Защитить содержимое листа от изменений
3. Защитить структуру книги от изменения
4. Защитить ячейки от изменения
5. Защитить объекты листа от изменений
6. Защитить окна книги от изменения
7. Защитить ячейки, так чтобы не было видно формул
8. Защитить сценарии листа от изменений
9. Защитить ячейки от изменения
10. Оформите отчет по лабораторной работе. В отчет включите: название, цель работы и выводы по указанным пунктам с экранными копиями.

Контрольные вопросы к практическим работам

1. Для чего необходима защита информации?
2. Какие тенденции защиты информации существуют в современном мире?
3. Какие основные понятия из области информационной безопасности вам известны? В чем их сущность?
4. Какие существуют методы защиты информации, для чего они используются?
5. Какие методы защиты применяются на этапе ввода данных в информационную систему?

Критерии и шкала оценивания по оценочному средству «практическая работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Задание выполнено на высоком уровне (студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Задание выполнено на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)
3	Задание выполнено на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Задание выполнено на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

Оценочные средства для промежуточной аттестации (зачет)

Теоретические вопросы

1. Общие понятия защиты информации.
2. Основные задачи службы защиты информации предприятия.

3. Что такое информационная безопасность? Понятия и определения в информационной безопасности.
4. Свойства информации. Виды защищаемой информации. Источники угроз.
5. Компьютерные сети: основные понятия и виды угроз.
6. Принципы защиты информации в компьютерных сетях.
7. Программы для обеспечения информационной безопасности сети.
8. Основные понятия и определения в области информационной безопасности.
9. Утечки информации: источники, правовые и технологические аспекты борьбы.
10. Безопасность Web-браузеров.
11. Безопасность беспроводных технологий.
12. Виртуальные частные сети (VPN) - технологии и средства организации.
13. Биометрические системы аутентификации: принципы, технологии и перспективы.
14. Методы поиска уязвимостей в информационных системах.
15. Управление программным обеспечением, как аспект обеспечения информационной безопасности. Структура, требования, задачи.
16. Безопасность современных сетевых технологий. Протоколы аутентификации.
17. Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.
18. Пользователи и злоумышленники в Internet.
19. Причины уязвимости сети Internet.
20. Основные закономерности возникновения и классификация угроз информационной безопасности.
21. Пути и каналы утечки информации.
22. Удаленные атаки на интрасети.
23. Классификация "компьютерных вирусов".
24. Файловые вирусы.
25. Загрузочные вирусы.
26. Макровирусы.
27. Сетевые вирусы.
28. Источники "компьютерных вирусов".
29. Идентификация и установление подлинности объекта (субъекта).
30. Методы и средства защиты информации от случайного воздействия.
31. Методы защиты информации от аварийных ситуаций.
32. Организационные мероприятия по защите информации.
33. Законодательные меры по защите информации.
34. Обеспечение информационной безопасности в Internet.
35. Архитектура телекоммуникационных систем.
36. Модели безопасности, политика безопасности.
37. Способы хищения информации.

Практические задания

1. Рассчитайте ведомость выполнения плана товарооборота киоска №5 по форме. Выполните защиту ячеек.

№	Месяц	Отчетный год			Отклонение от плана
		план	фактически	выполнение, %	
i	Mi	Pi	Fi	Vi	Oi
1	Январь	7 800,00 р.	8 500,00 р.		
2	Февраль	3 560,00 р.	2 700,00 р.		
3	Март	8 900,00 р.	7 800,00 р.		
4	Апрель	5 460,00 р.	4 590,00 р.		
5	Май	6 570,00 р.	7 650,00 р.		
6	Июнь	6 540,00 р.	5 670,00 р.		
7	Июль	4 900,00 р.	5 430,00 р.		
8	Август	7 890,00 р.	8 700,00 р.		
9	Сентябрь	6 540,00 р.	6 500,00 р.		
10	Октябрь	6 540,00 р.	6 570,00 р.		
11	Ноябрь	6 540,00 р.	6 520,00 р.		
12	Декабрь	8 900,00 р.	10 000,00 р.		

2. Заполните таблицу по полю «дата рождения». С пмощью формулы определить возраст. Выполните защиту ячеек «возраст».

№	ФИО	Дата рождения	Возраст
1	Иванов И.И.		
2	Петров П.П.		
3	Сидоров С.С.		
…			
10	Мышкин М.М.		

3. Создайте таблицу по образцу. С пмощью формулы определить стаж работы. Выполните защиту ячеек «стаж».

ФИО	Должность	Дата приема на работу	Стаж
Иванов И.И.	Директор	01 января 2003 г.	5
Петров П.П.	Водитель	02 февраля 2002 г.	6
Сидоров С.С.	Инженер	03 июня 2001 г.	7
Кошкин К.К.	Гл. бух.	05 сентября 2006 г.	1
Мышкин М.М.	Охранник	01 августа 2008 г.	0
Мошкин М.М.	Инженер	04 декабря 2005 г.	2
Собакин С.С.	Техник	06 ноября 2007 г.	0
Лосев Л.Л.	Психолог	14 апреля 2005 г.	3
Гусев Г.Г.	Техник	25 июля 2004 г.	4
Волков В.В.	Снабженец	02 мая 2001 г.	7

Критерии и шкала оценивания по оценочному средству промежуточный контроль («зачет»)

Характеристика знания предмета и ответов	Зачеты
Студент глубоко и в полном объеме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопрос и правильно обосновывает принятые решения, хорошо владеет умениями и навыка-ми при выполнении практических задач.	зачтено
Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.	
Студент знает только основной программный материал, допускает неточности, недостаточно четкие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.	
Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы.	не зачтено

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)