МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ЧЕЧЕНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ ФИЗИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

КАФЕДРА ПРИКЛАДНОЙ ИНФОРМАТИКИ

Утверждаю:
Зав.каф.: Юшаев С-Э.С-М.
Протокол № 8 заседания
кафедры от 24 апреля 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Оценка и обеспечение информационной безопасности
(наименование дисциплины (модуля))

Направление подготовки

09.04.03 «Прикладная информатика»
(код и направление подготовки)

Профиль(и) подготовки
«Прикладная информатика в экономике»

Квалификация
Магистр

Форма обучения
очная/заочная

Год набора - 2023

Грозный, 2023

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ

1.1. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Оценка и обеспечение информационной безопасности» относится к обязательной части подготовки магистра. Курс базируется на предварительном усвоении таких дисциплин как: «Методы и средства проектирования информационных систем и технологий», «Проектирование информационных систем управления», «Администрирование информационных систем управления».

1.2. Цель освоения дисциплины (модуля)

Целью освоения учебной дисциплины «Оценка и обеспечение информационной безопасности» является формирование у магистрантов компетенций, необходимых для использования изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.3. Планируемые результаты обучения по дисциплине (модулю)

Достижение цели освоения дисциплины (модуля) обеспечивается через формирование следующих компетенций *(с указанием шифра компетенции):*

Таблица 1

Код и наименование компетенции	Код и наименование индикатора достижения компетенций, которые формирует дисциплина (модуль)	Планируемые результаты обучения
ПК-4	Способен распределять полномочия в ИТ проекте и вести управление документацией на всех стадиях жизненного цикла проекта.	Знает: способы управления проектами по информатизации. Умеет: определять стратегию информатизации прикладных задач; моделировать и проектировать прикладные и информационные процессы на основе современных технологий; разрабатывать проекты информатизации предприятий и организаций в прикладной области. Владеет: навыками управления проектами по информатизации прикладных задач и созданию ИС предприятий и организаций.
ПК-5	Способность управлять информационными ресурсами и ИС	Знает: методы и модели управления информационными ресурсами и информационными системами Умеет: определять вид программного средства для моделирования экономических и управленческих процессов; использовать передовые методы управления проектами по информатизации. Владеет: навыками и умениями для решения профессиональных задач.
ПК-6	Способность управлять проектами по информатизации прикладных задач и созданию ИС предприятий и организаций	Знает: методы системного и критического анализа; методики

		разработки стратегии действий для выявления и решения проблемной ситуации; стандарты и методики управления проектами различных типов; методы оценки ИТ-проектов и результатов ИТ-проектов. Умеет: разрабатывать сервисы на основе аналитики больших данных. Владеет: приемами обеспечения защиты и конфиденциальности данных.

1.4. Объем дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет очно 6 з.е, заочно 6 з.е. (академ. часов)

Таблица 2

Вид учебной работы	**Количество академ. часов**	
	Очно	**Заочно**
4.1. Объем контактной работы обучающихся с преподавателем	**40+149**	**14+193**
4.1.1. аудиторная работа	**40**	**14**
в том числе:		
лекции	16	4
практические занятия, семинары, в том числе практическая подготовка	24	10
лабораторные занятия		
4.1.2. внеаудиторная работа	**27**	**9**
в том числе:		
индивидуальная работа обучающихся с преподавателем		
курсовое проектирование/работа		
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем	27	9
4.2. Объем самостоятельной работы обучающихся	149	193
в том числе часов, выделенных на подготовку к экзамену	2	1

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Тематическое планирование дисциплины (модуля):

Таблица 3

№ п/п	**Наименование темы (раздела) дисциплины (модуля)**	**Общая трудоёмкость в акад.часах**		**Трудоёмкость по видам учебных занятий (в акад.часах)**							
				Лекции		**Практ. занятия**		**Лаб. занятия**		**Сам. работа**	
		Очно	Заочн.	Очно	Заочн.	Очно	Заочн.	Очно	Заочн.	Очно	Заочн.
1.	**Модуль 1. Основополагающие положения информационной безопасности**	**20**	**8**	**8**	**2**	**12**	**6**	**-**	**-**	**88**	**96**

2.	Тема 1.1. Международные стандарты информационного обмена	2	2	2	2			-	-	10	12
3.	Тема 1.2. Понятие угрозы	4	2	2		2	2	-	-	12	10
4.	Тема 1.3 Информационная безопасность в условиях функционирования в России	2		2				-	-	10	12
5.	Тема 1.4. Понятие о видах вирусов	2	2			2	2	-	-	10	10
6.	Тема 1.5. Три вида возможных нарушений информационной системы	2		2				-	-	10	8
7.	Тема 1.6. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	2				2		-	-	8	10
8.	Тема 1.7. Основные положения теории информационной безопасности	2				2		-	-	10	12
9.	Тема 1.8. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	2	2			2	2	-	-	10	10
10.	Тема 1.9. Модели безопасности и их применение	2				2		-	-	8	12
11.	**Модуль 2. Защита информации**	**20**	**6**	**8**	**2**	**12**	**4**	**-**	**-**	**61**	**97**
12.	Тема 2.1. Использование защищенных компьютерных систем	2		2				-	-	5	12
13.	Тема 2.2. Методы криптографии	2	2			2	2	-	-	10	10
14.	Тема 2.3. Основные технологии построения защищенных систем	2				2		-	-	10	12
15.	Тема 2.4 Место информационной безопасности экономических систем в национальной безопасности страны	2	2	2	2			-	-	6	10
16.	Тема 2.5. Защита экономических систем	2	2			2	2	-	-	4	9
17.	Тема 2.6. Обмен конфиденциальной информацией	4		2		2		-	-	10	10
18.	Тема 2.7. Структура банковских информационных систем в области защиты информации	2				2		-	-	2	12
19.	Тема 2.8. Важность защиты экономических систем	2		2				-	-	10	10
20.	Тема 2.9. Концепция информационной безопасности	2				2		-	-	4	12
	Курсовое проектирование/работа		*4*					-	-		
	Подготовка к экзамену (зачету)	*1*	*1*					-	-		
	Итого:	40	14					-	-	149	193

Часы, отведенные на лабораторные занятия, все считаются как практическая подготовка. Из часов практических занятий через косую линию указываются часы, отведенные на практическую подготовку.

2.2. Содержание разделов дисциплины (модуля):

Таблица 4

№ п/п	Наименование темы (раздела) дисциплины	Содержание дисциплины (дидактические единицы) *(для педагогических профилей наполняется с учетом ФГОС основного общего и среднего общего образования)*
1	**Модуль 1. Основополагающие положения информационной безопасности**	Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.
2	Тема 1.1. Международные стандарты информационного обмена	Международные стандарты информационного обмена. Протоколы (protocols) — это набор правил и процедур, регулирующих порядок осуществления некоторой связи.
3	Тема 1.2. Понятие угрозы	Понятие угрозы. Угроза в отношении человека в настоящее время трактуется, в первую очередь, с позиций уголовного права.
4	Тема 1.3 Информационная безопасность в условиях функционирования в России глобальных сетей	Информационная безопасность в условиях функционирования в России глобальных сетей. Главной целью создания сети Интернет было обеспечение функциональности при выходе из строя одного или нескольких ее узлов, цель в общем со-стояла в обеспечение безопасности.
5	Тема 1.4. Понятие о видах вирусов	Понятия о видах вирусов. Вирус, как программа, состоит из двух частей: механизма размножения и начинки.
6	Тема 1.5. Три вида возможных нарушений информационной системы	Понятие угрозы. Три вида возможных нарушений информационной системы. Под угрозой понимается потенциально возможные события, процесс или явление, которое может привести к уничтожению информации или утрате целостности, конфиденциальности или доступности информации.
7	Тема 1.6. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные	Нормативно-справочные документы содержат нормы и нормативы, необходимые при решении задач организации и планирования труда в сфере материального производства и управления.
8	Тема 1.7. Основные положения теории информационной безопасности	Изложены основные понятия теории информационной безопасности, методология построения систем защиты автоматизированных информационных систем (АС), раскрывается понятие формальных политик безопасности.
9	Тема 1.8. Назначение и задачи в сфере обеспечения информационной безопасности	Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
10	Тема 1.9. Модели безопасности и их применение	Модели безопасности и их применение. Метод формальной разработки системы опирается на модель безопасности (модель управления доступом, модель политики безопасности).
11	**Модуль 2. Защита информации**	Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
15	Тема 2.1. Использование защищенных компьютерных систем	Использование защищенных компьютерных систем. Межсетевой экран – инструмент реализации политики безопасности.
16	Тема 2.2. Методы криптографии	Что такое криптография. Криптография — наука, которая изучает методы обеспечения конфиденциальности, безопасности и аутентичности информации.
17	Тема 2.3. Основные технологии построения защищенных систем	Основные технологии построения защищённых. Экономические информационные системы. Общие принципы построения защищенных систем. Средства разработки и правила их реализации.
18	Тема 2.4 Место информационной безопасности экономических систем в национальной	Место информационной безопасности экономических систем в национальной безопасности страны. Internet и информационная безопасность несовместны по самой природе Internet.

19	Тема 2.5. Защита экономических систем	Защита экономической системы - это взаимосвязанный комплекс мер в политической, экономической, здравоохранительной, социальной, военной и правовой сферах.
20	Тема 2.6. Обмен конфиденциальной информацией	Конфиденциальная информация — это сведения, доступ к которым ограничен законом, а их разглашение наказуемо.
21	Тема 2.7. Структура банковских информационных систем в области защиты информации	Компания SearchInform – российский разработчик средств информационной безопасности и инструментов для защиты информации.
22	Тема 2.8. Важность защиты экономических систем	Защита экономической системы – это взаимоувязанный комплекс мероприятий в области политики, экономики, здравоохранения, социальной защиты, военной, правовой сферы.
23	Тема 2.9. Концепция информационной безопасности	Шаблоны типовых документов по информационной безопасности. Концепция обеспечения информационной безопасности предприятия.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

3.1. Учебно-методическое обеспечение самостоятельной работы обучающихся

Таблица 5

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы обучающихся
1.	Угрозы информационной безопасности	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
2.	Современные средства защиты информации	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
3.	Современные системы компьютерной безопасности	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
4.	Современные криптографические системы	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
5.	Криптоанализ, современное состояние	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов
6.	Правовые основы защиты информации	Изучение и конспектирование основной и дополнительной литературы, подготовка рефератов

3.1 Учебно-методическое и информационное обеспечение программы дисциплины (модуля)

3.1.1. Основная и дополнительная литература

Таблица 6

Виды литературы	Автор, название литературы, город, издательство, год	Количество часов, обеспеченных указанной литературой Аудит./самост.	Количество обучающихся	Количество экземпляров в библиотеке университета	Режим доступа ЭБС/ электронный носитель (CD,DVD)	Обеспеченность обучающихся литературой, (5гр./4гр.)х100%))
1	2	3	4	5	6	7

	Основная литература					
1	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный //	40+149 14+192	50		ЭБС Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837	100%
2	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный //	40+149 14+192	50		ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/530927	100%
3	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный //	40+149 14+192	50		ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/531084	100%
	Дополнительная литература					
1	Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный //	40+149 14+192	50		ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/512268	100%
2	Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный //	40+149 14+192	50		ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/515435	100%
3	Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный //	40+149 14+192	50		ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/519079	100%

3.1.2. Интернет-ресурсы

1. Электронно-библиотечная система IPRbooks (www.iprbookshop.ru)
2. Образовательная платформа «ЮРАЙТ» https://urait.ru/)
3. Электронно-библиотечная система «Лань» (https://e.lanbook.com/)
4. МЭБ (Межвузовская электронная библиотека) НГПУ. (https://icdlib.nspu.ru/)
5. НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU (https://www.elibrary.ru/)
6. СПС «КонсультантПлюс» (http://www.consultant.ru/

3.2. Материально-техническое обеспечение дисциплины

Для осуществления образовательного процесса по дисциплине необходима следующая материально-техническая база:

Таблица 7

Помещения для осуществления образовательного процесса	**Перечень основного оборудования (с указанием кол-ва посадочных мест)**	**Адрес (местоположение)**
Аудитория для проведения лекционных занятий		
5-04	- стандартно оборудованные лекционные аудитории с видеопроектором и настенным экраном - персональный компьютер или ноутбук под управлением MS Windows, пакет Microsoft Office с возможностью подключения проектора 40 посадочных мест	Чеченская Республика г. Грозный, ул. Ляпидевского, 9. Учебный корпус №
Аудитории для проведения практических занятий, контроля успеваемости		
3-18	- класс персональных компьютеров под управлением MS Windows, включенных в корпоративную сеть университета 25 посадочных мест	Чеченская Республика г. Грозный, ул. Ляпидевского, 9. Учебный корпус №
Помещения для самостоятельной работы		
Компьютерный центр	Компьютерная мебель на 52 посадочных мест, 52 компьютеров с выходом в Интернет, системный блок (52 шт.), клавиатура (52 штук), мышь (52 штук)	Чеченская Республика г. Грозный, ул. Субры Кишиевой, № 33

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ / МОДУЛЯ

4.1. Характеристика оценочных средств

Контроль и оценка результатов освоения дисциплины / модуля осуществляется преподавателем в процессе проведения практических и лабораторных занятий, контрольных работ, а также выполнения обучающимися индивидуальных заданий, проектов, исследований и т.д.

Таблица 8

№ п/п	Наименование темы (раздела) с контролируемым	Код и наименование проверяемых	Оценочные средства	
	содержанием	**компетенций**	**текущий контроль**	**промежуточная аттестация**
1.	Защита экономических систем Литература: основная. 1, 2,3, дополнительная 1,2,3	ПК-4	Подготовка и защита презентации по темам раздела	Вопросы для подготовки к экзамену
2.	Структура банковских информационных систем в области защиты информации Литература: основная. 1, 2,3, дополнительная 1,2,3	ПК-5	Подготовка и защита реферата по темам раздела	Вопросы для подготовки к экзамену
3.	Обмен конфиденциальной информацией Литература: основная. 1, 2,3, дополнительная 1,2,3		Тестирование	Вопросы для подготовки к экзамену
4.	Концепция информационной безопасности Литература: основная. 1, 2,3, дополнительная 1,2,3	ПК-6	Выполнение индивидуальных заданий	Вопросы для подготовки к экзамену

4.2. Оценочные средства для проведения текущего контроля успеваемости

4.2.1. Наименование оценочного средства: *тест*

Примерные вопросы для тестирования

Тест №1

1. Программа, которая может размножаться, присоединяя свой код к другой программе, Называется. Выберите один ответ.

a. Компилятор

b. Интернет-черви

c. Вирус

2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется. Выберите один ответ.

a. Воздействием (влиянием)

b. Потерей

c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется. Выберите один ответ.

a. Троянской программой

b. Червем

c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата, называется

Выберите один ответ.

a. Устойчивостью

b. Терпимостью по отношению к риску

c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд. Выберите один ответ.

a. Две

b. Одну

c. Сколько зададут

6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:

Выберите один ответ.

a. Статическими алгоритмами

b. Алгоритмы RMS

c. Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:

Выберите один ответ.

a. Каталоги

b. Символьные файлы

c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются

Выберите один ответ.

a. Вирусами

b. Руткитами

c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:

Выберите один ответ.

a. Правилами безопасности

b. Требованием безопасности

c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

Выберите один ответ.

a. Управление риском

b. Предупреждением рисков

c. Анализом рисков

11. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется. Выберите один ответ.

a. Мультипроцессоры типа «хозяин-подчиненный»

b. Симметричный мультипроцессор

c. Мультипроцессор с общей памятью

Тест №2

1. Назовите центральный блок ПК.

a. системная шина;

b. видеомонитор;

c. память;

d. микропроцессор.

2. Комплекс различных устройств, поддерживающий работу системы, управляющий внутренними связями и взаимодействующий с внешними устройствами – это:

a. системная шина;
b. процессор;
c. материнская плата;
d. контроллер.

3. Для подключения микросхем памяти на материнской плате имеется:

a. контроллер;
b. слот;
c. порт;
d. шина.

4. Обработку графических функций производит:

a. графический контроллер;
b. видеопамять;
c. буфер кадра;
d. интерфейсная шина.

5. Разрешение монитора определяется:

a. скоростью видеопамяти;
b. количеством пикселов на линии и количеством самих линий;
c. скоростью графического контроллера;
d. количеством цветов, из которых можно выбирать при создании изображения.

6. Общее время доступа к информации определяется:

a. количеством пластин в корпусе жесткого диска;
b. увеличением плотности записи информации;
c. скоростью вращения пластин;
d. временем поиска нужной дорожки на диске и временем позиционирования внутри этой дорожки.

7. Дорожки винчестеров представляют собой:

a. концентрические окружности;
b. прямые линии;
c. прерывающуюся спираль;
d. нет правильного ответа.

8. Все клавиатуры делятся на три вида:

a. полные, неполные и планшетные;
b. полные, мультимедийные и неполные;
c. полные, мультимедийные и роликовые;
d. полные, неполные и проекционные.

9. В процессе оцифровки изображение разбивается на элементарные частицы:

a. пикселы;
b. кванты;
c. графы;
d. нет правильного ответа.

10. Наиболее дешевым кабельным соединением является:

a. соединение Cheapernet-кабель;
b. витое проводное соединение;
c. оптоволоконные линии;
d. коаксиальный кабель.

Критерии оценивания результатов тестирования

Таблица 9

Уровень освоения	*Критерии*	*Баллы*
Максимальный уровень	*Выполнены правильно все задания теста (тест зачтен)*	*2*
Средний уровень	*Выполнено правильно больше половины заданий (тест зачтен)*	*1*
Минимальный уровень	*Выполнено правильно меньше половины заданий (тест не зачтен)*	*0*

4.2.2. Наименование оценочного средства: ***практико-ориентированное задание***

Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки.

Примерные практико-ориентированные задания

Задание №1. Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля:
В качестве информационного ресурса использовать любой файл или приложение.

Задание №2. Практическая работа состоит из двух частей:
Часть 1 – применение одного из алгоритмов симметричного шифрования;
Часть 2 – шифрование с использованием алгоритма RSA.

Задание №3. Сформировать ЭЦП к сообщению M' (см. вариант) и произвести проверку целостности принятого сообщения.
Порядок выполнения работы:
Разделить лист на две части: слева – сторона отправителя сообщения, справа – получателя.

Задание №4. Разработать программу, имитирующую некоторые (см. вариант) действия вируса или другой вредоносной программы и подготовить отчет о проделанной работе.

Критерии оценивания результатов выполнения практико-ориентированного задания

Таблица 10

Уровень освоения	*Критерии*	*Баллы*
Максимальный уровень	*Задание выполнено правильно: выводы аргументированы, основаны на знании материала, владении категориальным аппаратом*	*3*
Средний уровень	*Задание выполнено в целом правильно: но допущены ошибки в аргументации, обнаружено поверхностное владение терминологическим аппаратом*	*2*
Минимальный уровень	*Задание выполнено с ошибками в формулировке тезисов и аргументации, обнаружено слабое владение терминологическим аппаратом*	*1*
Минимальный уровень не достигнут	*Задание не выполнено или выполнено с серьёзными ошибками*	*0*

4.2.3. Наименование оценочного средства: ***доклад/сообщение***

Темы докладов:

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними

2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы
6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ

Критерии и шкалы оценивания доклада/сообщения (в форме презентации):

Таблица 11

Уровень освоения	***Критерии***	***Баллы***
Максимальный уровень	*– продемонстрировано умение выступать перед аудиторией;* *– содержание выступления даёт полную информацию о теме;* *– продемонстрировано умение выделять ключевые идеи;* *– умение самостоятельно делать выводы, использовать актуальную научную литературу;* *– высокая степень информативности, компактность слайдов*	*3*
Средний уровень	*– продемонстрирована общая ориентация в материале;* *– достаточно полная информация о теме;* *– продемонстрировано умение выделять ключевые идеи, но нет самостоятельных выводов;* *– невысокая степень информативности слайдов;* *– ошибки в структуре доклада;* *– недостаточное использование научной литературы*	*2*
Минимальный уровень	*– продемонстрирована слабая (с фактическими ошибками) ориентация в материале;* *– ошибки в структуре доклада;* *– научная литература не привлечена*	*1*
Минимальный уровень не достигнут	*– выступление не содержит достаточной информации по теме;* *– продемонстрировано неумение выделять ключевые идеи;* *– неумение самостоятельно делать выводы, использовать актуальную научную литературу.*	*0*

4.2.4. Наименование оценочного средства: ***контрольная работа***

Примерное задание для контрольной работы:

Задание. Дайте ответы на контрольные вопросы:

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?

Критерии оценивания результатов контрольной работы

Таблица 12

Балл (интервал баллов)	***Уровень освоения***	***Критерии оценивания уровня освоения компетенций****
10	*Максимальный уровень (интервал)*	*Контрольная работа оформлена в соответствии с предъявляемыми требованиями, содержит 1-2 мелких ошибки; ответы студента правильные, четкие, содержат 1-2 неточности*
[6-8]	*Средний уровень (интервал)*	*Контрольная работа содержит одну принципиальную или 3 или более недочетов; ответы студента правильные, но их формулирование затруднено и требует наводящих вопросов от преподавателя*
[3-5]	*Минимальный уровень (интервал)*	*Контрольная работа оформлена в соответствии с предъявляемыми требованиями, неполное раскрытие темы в теоретической части и/или в практической части контрольной работы; ответы студенты формально правильны, но поверхностны, плохо сформулированы, содержат более одной принципиальной ошибки*
Менее 3	*Минимальный уровень (интервал) не достигнут.*	*Контрольная работа содержит более одной принципиальной ошибки моделей решения задачи; контрольная работа оформлена не в соответствии с предъявляемыми требованиями; ответы студента путанные, нечеткие, содержат множество ошибок, или ответов нет совсем; несоответствие варианту.*

4.3. Оценочные средства для промежуточной аттестации

Представлено в приложении №1.

Автор(ы) рабочей программы дисциплины (модуля):

доцент, к.п.н Исаева Л.М.
(подпись)

Заведующий кафедрой,
к.ф.-м.н., доцент (подпись) Юшаев С.-Э.С.-М.

СОГЛАСОВАНО:
Директор библиотеки (подпись) Арсагириева Т.А.

Приложение 1

Оценочные средства
для проведения промежуточной аттестации по дисциплине

Направление подготовки
09.04.03 «ПРИКЛАДНАЯ ИНФОРМАТИКА»
(код и направление подготовки)
Профили подготовки «Прикладная информатика в экономике»
Форма обучения: очная и заочная
Год приема: 2022

1. Характеристика оценочной процедуры:
Семестр -4
Форма аттестации – экзамен

2. Оценочные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

2.1. Вопросы для промежуточной аттестации по дисциплине:

1. Основополагающие положения информационной безопасности
2. Международные стандарты информационного обмена
3. Понятие угрозы
4. Информационная безопасность в условиях функционирования в России глобальных сетей
5. Понятие о видах вирусов
6. Три вида возможных нарушений информационной системы
7. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы
8. Основные положения теории информационной безопасности
9. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства
10. Модели безопасности и их применение
11. Защита информации
12. Использование защищенных компьютерных систем
13. Методы криптографии
14. Основные технологии построения защищенных систем
15. Место информационной безопасности экономических систем в национальной безопасности страны
16. Защита экономических систем
17. Обмен конфиденциальной информацией
18. Структура банковских информационных систем в области защиты информации
19. Важность защиты экономических систем
20. Концепция информационной безопасности
21. Какие меры по устранению угрозы IP -спуфинга существуют?
22. Что включает борьба с атаками на уровне приложений?
23. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
24. В чем заключается распределенное хранение файлов?
25. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?

26. Какие уровни информационной защиты существуют, их основные составляющие?
27. В чем заключаются задачи криптографии?
28. Зачем нужны ключи?
29. Какая схема шифрования называется многоалфавитной подстановкой?
30. Какие системы шифрования вы знаете?

2.2. Структура экзаменационного билета (примерная):

1. *Теоретический вопрос: Страница Your Prezis портала PREZI.COM.*
2. *Практико-ориентированное задание: Создание комбинированной гистограммы в Google*

3. Критерии и шкала оценивания устного ответа обучающегося на экзамене (зачете)

Максимальное количество баллов на экзамене (зачете) – 30, из них:

1. Ответ на первый вопрос, содержащийся в билете – 15 баллов.
2. Ответ на второй вопрос, содержащийся в билете – 15 баллов.

Таблица 13

№ n/n	Характеристика ответа	Баллы
1.	Даны полные, развернутые ответы на поставленные вопросы; в ответах прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений.	**13-15**
2.	Даны полные, но недостаточно последовательные ответы на поставленные вопросы, но при этом показано умение выделить существенные и несущественные признаки и причинно-следственные связи.	**10-12**
3	Даны неполные ответы, логика и последовательность изложения имеют нарушения	**7-9**
4.	Отсутствует представление о предмете аттестационного испытания	**6 и менее**

Расчет итоговой рейтинговой оценки

Таблица 14

До 50 баллов включительно	«неудовлетворительно»
От 51 до 70 баллов	«удовлетворительно»
От 71 до 85 баллов	«хорошо»
От 86 до 100 баллов	«отлично»

4. Уровни сформированности компетенций по итогам освоения дисциплины (модуля)

Таблица 15

Индикаторы достижения компетенции (ИДК)	**Уровни сформированности компетенций**			
	«отлично»	**«хорошо»**	**«удовлетворительно»**	**«неудовлетворительно»**
	86-100	**71-85**	**51-70**	**Менее 51**
	«зачтено»			**«не зачтено»**
Код и наименование формируемой компетенции				
ПК-1.1	Знает	Знает	Знает	Не знает
	Умеет	Умеет	Умеет	Не умеет
	Владеет	Владеет	Владеет	Не владеет

ПК-1.2	Знает	Знает	Знает	Не знает
	Умеет	Умеет	Умеет	Не умеет
	Владеет	Владеет	Владеет	Не владеет
Код и наименование формируемой компетенции				
ОПК-8.1	Знает	Знает	Знает	Не знает
	Умеет	Умеет	Умеет	Не умеет
	Владеет	Владеет	Владеет	Не владеет
ОПК-8.2	Знает	Знает	Знает	Не знает
	Умеет	Умеет	Умеет	Не умеет
	Владеет	Владеет	Владеет	Не владеет
….				

5. Рейтинг-план изучения дисциплины

Таблица 16

I	**БАЗОВАЯ ЧАСТЬ РЕЙТИНГОВОЙ СИСТЕМЫ**		
Виды контроля	**Контрольные мероприятия**	**Мин. кол-во баллов на занятиях**	**Макс. кол-во баллов на занятиях**
Текущий контроль № 1	Тема № 1. Основополагающие положения информационной безопасности Тема № 2. Международные стандарты информационного обмена	0	10
Текущий контроль № 2	Тема № 3. Понятие угрозы	0	10
	Тема № 4. Информационная безопасность в условиях функционирования в России глобальных сетей		
Рубежный контроль: контрольная работа №1 (Темы 1-4)		0	10
Текущий контроль №3	Тема 5. Понятие о видах вирусов	0	10
	Тема 6. Три вида возможных нарушений информационной системы		
	Тема 7. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы		
Текущий	Тема 8. Основные положения теории информационной безопасности	0	10

контроль №4	Тема 9. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства			
Рубежный контроль: контрольная работа №2 (Темы 5-9)			0	10
Допуск к промежуточной аттестации			**Мин 36**	
II	**ДОПОЛНИТЕЛЬНАЯ ЧАСТЬ РЕЙТИНГОВОЙ СИСТЕМЫ**		**Мин.**	**Макс.**
1	**Поощрительные баллы**		**0-10**	**10**
	Подготовка доклада с презентацией по дисциплине		0-1	1
	Посещаемость лекций (100%)		0-2	2
	Участие в работе круглого стола, студенческой конференции		0-2	2
	Соц.-личностный рейтинг		0-3	3
	Участие в общественной, культурно-массовой и спортивной работе		0-2	2
2	**Штрафные баллы**		**0-3**	**3**
	Пропуск учебных лекций	за пропуск лекции снимается балльная стоимость лекции (2:8=0,25)	0,25 x N (N – количество пропущенных лекций	
	Несвоевременное выполнение контрольной (аттестационной) работы №1	минус 5% от максимального балла	- 0,5	
	Несвоевременное выполнение контрольной (аттестационной) работы №2	минус 5% от максимального балла	- 0,5	
III	**ИТОГОВЫЙ КОНТРОЛЬ**		**0-30**	**30**
Форма итогового контроля:	Зачет (экзамен)		0-30	**30**
ИТОГО БАЛЛОВ ЗА СЕМЕСТР:			**0-100**	

Приложение 2

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ

_____

(наименование дисциплины / модуля)

Направление подготовки _____

Профили _____

(год набора _____, форма обучения _____)

на 20___ / 20___ учебный год

В рабочую программу дисциплины / модуля вносятся следующие изменения:

№ n/n	**Раздел рабочей программы (пункт)**	**Краткая характеристика вносимых изменений**	**Основание для внесения изменений**