

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**ФАКУЛЬТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ**

**КАФЕДРА «ЦИФРОВАЯ И ОТРАСЛЕВАЯ ЭКОНОМИКА»**

**СОГЛАСОВАНО**

Руководитель образовательной программы

\_\_\_\_\_/доц.М.А.Орцханова\_\_\_\_\_  
от « 21 » \_\_\_\_\_ мая \_\_\_\_\_ 2024г.

**УТВЕРЖДАЮ**

И.о.декана факультета экономики и  
управления

\_\_\_\_\_/\_\_\_\_М.Ш.Мержо\_\_\_\_\_  
от « 22 » \_\_\_\_\_ мая \_\_\_\_\_ 2024г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

**Б1.В.ДВ.09.01 «Информационная безопасность в цифровой  
экономике»**

**38.03.01 Экономика**

(код и наименование направления подготовки/специальности)

**Цифровая экономика**

(наименование профиля подготовки (при наличии))

**Квалификация выпускника**

бакалавр

**Форма обучения**

очная, очно-заочная, ускоренная

**МАГАС, 2024 г.**

## Паспорт фонда оценочных средств

№ п п	Контролируемые темы дисциплины	Контролируемые компетенции (их части)	Другие оценочные средства	
			Вид	Наименование
1	Стратегические решения в области информационной безопасности	УК-2, ПК-4	Тест, опрос	Тесты, задания, коллоквиум, семинары
2	Управление информационной безопасностью	УК-2, ПК-4	Тест, опрос	Доклады, эссе, семинары
3	Угрозы информационной безопасности в цифровой экономике	УК-2, ПК-4	Тест, задача, опрос	Задания, тесты, семинары, доклады
4	Современное состояние средств защиты технологий цифровой экономики в информационных системах и технологиях управления бизнес-процессами в России.	УК-2, ПК-4	Опрос	Коллоквиум, семинары

**Типовые контрольные задания или иные материалы, необходимые для оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

**Тестовые задания по дисциплине**

**1.К правовым методам, обеспечивающим информационную безопасность, относятся:**

- а. разработка аппаратных средств обеспечения правовых данных
- б. разработка и установка во всех компьютерных правовых сетях журналов учета действий
- с. разработка и конкретизация правовых нормативных актов обеспечения безопасности

**2.Основными источниками угроз информационной безопасности являются все указанное в списке:**

- а. Хищение жестких дисков, подключение к сети, инсайдерство
- б. Перехват данных, хищение данных, изменение архитектуры системы
- с. Хищение данных, подкуп системных администраторов, нарушение регламента работы

**3.Виды информационной безопасности:**

- а. Персональная, корпоративная, государственная
- б. Клиентская, серверная, сетевая
- с. Локальная, глобальная, смешанная

**4.Цели информационной безопасности – своевременное обнаружение, предупреждение:**

- а. несанкционированного доступа, воздействия в сети
- б. инсайдерства в организации
- с. чрезвычайных ситуаций

**5.Основные объекты информационной безопасности:**

- a. Компьютерные сети, базы данных
  - b. Информационные системы, психологическое состояние пользователей
  - c. Бизнес-ориентированные, коммерческие системы
- 6.Основными рисками информационной безопасности являются:**
- a. Искажение, уменьшение объема, перекодировка информации
  - b. Техническое вмешательство, выведение из строя оборудования сети
  - c. Потеря, искажение, утечка информации
- 7.К основным принципам обеспечения информационной безопасности относится:**
- a. Экономической эффективности системы безопасности
  - b. Многоплатформенной реализации системы
  - c. Усиления защищенности всех звеньев системы
- 8.Основными субъектами информационной безопасности являются:**
- a. руководители, менеджеры, администраторы компаний
  - b. органы права, государства, бизнеса
  - c. сетевые базы данных, фаерволлы
- 9.К основным функциям системы безопасности можно отнести все перечисленное:**
- a. Установление регламента, аудит системы, выявление рисков
  - b. Установка новых офисных приложений, смена хостинг-компаний
  - c. Внедрение аутентификации, проверки контактных данных пользователей
- 10.Принципом информационной безопасности является принцип недопущения:**
- a. Неоправданных ограничений при работе в сети (системе)
  - b. Рисков безопасности сети, системы
  - c. Презумпции секретности
- 11.Принципом политики информационной безопасности является принцип:**
- a. Невозможности миновать защитные средства сети (системы)
  - b. Усиления основного звена сети, системы
  - c. Полного блокирования доступа при риск-ситуациях
- 12.Принципом политики информационной безопасности является принцип:**
- a. Усиления защищенности самого незащищенного звена сети (системы)
  - b. Перехода в безопасное состояние работы сети, системы
  - c. Полного доступа пользователей ко всем ресурсам сети, системы
- 13.Принципом политики информационной безопасности является принцип:**
- a. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
  - b. Одноуровневой защиты сети, системы
  - c. Совместимых, однотипных программно-технических средств сети, системы
- 14.К основным типам средств воздействия на компьютерную сеть относится:**
- a. Компьютерный сбой
  - b. Логические закладки («мины»)
  - c. Аварийное отключение питания
- 15.Когда получен спам по e-mail с приложенным файлом, следует:**
- a. Прочитать приложение, если оно не содержит ничего ценного – удалить
  - b. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
  - c. Удалить письмо с приложением, не раскрывая (не читая) его
- 16.Принцип Кирхгофа:**
- a. Секретность ключа определена секретностью открытого сообщения
  - b. Секретность информации определена скоростью передачи данных
  - c. Секретность закрытого сообщения определяется секретностью ключа
- 17.ЭЦП – это:**
- a. Электронно-цифровой преобразователь
  - b. Электронно-цифровая подпись
  - c. Электронно-цифровой процессор

**18. Наиболее распространены угрозы информационной безопасности корпоративной системы:**

- a. Покупка нелегального ПО
- b. Ошибки эксплуатации и неумышленного изменения режима работы системы
- c. Сознательного внедрения сетевых вирусов

**19. Наиболее распространены угрозы информационной безопасности сети:**

- a. Распределенный доступ клиент, отказ оборудования
- b. Моральный износ сети, инсайдерство
- c. Сбой (отказ) оборудования, нелегальное копирование данных

**20. Наиболее распространены средства воздействия на сеть офиса:**

- a. Слабый трафик, информационный обман, вирусы в интернет
- b. Вирусы в сети, логические мины (закладки), информационный перехват
- c. Компьютерные сбои, изменение администрирования, топологии

**21. Утечкой информации в системе называется ситуация, характеризующаяся:**

- a. Потерей данных в системе
- b. Изменением формы информации
- c. Изменением содержания информации

**22. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

- a. Целостность
- b. Доступность
- c. Актуальность

**23. Угроза информационной системе (компьютерной сети) – это:**

- a. Вероятное событие
- b. Детерминированное (всегда определенное) событие
- c. Событие, происходящее периодически

**24. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:**

- a. Регламентированной
- b. Правовой
- c. Защищаемой

**25. Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:**

- a. Программные, технические, организационные, технологические
- b. Серверные, клиентские, спутниковые, наземные
- c. Личные, корпоративные, социальные, национальные

### **Требования к выполнению тестового задания**

Тестирование является одним из основных средств формального контроля качества обучения. Это метод, основанный на стандартизированных заданиях, которые позволяют измерить психофизиологические и личностные характеристики, а также знания, умения и навыки испытуемого.

Основные принципы тестирования, следующие:

связь с целями обучения – цели тестирования должны отвечать критериям социальной полезности и значимости, научной корректности и общественной поддержки;

объективность – использование в педагогических измерениях этого принципа призвано не допустить субъективизма и предвзятости в процессе этих измерений;

справедливость и гласность – одинаково доброжелательное отношение ко всем обучающимся, открытость всех этапов процесса измерений, своевременность ознакомления обучающихся с результатами измерений;

систематичность – систематичность тестирований и самопроверок каждого учебного модуля, раздела и каждой темы; важным аспектом данного принципа является требование репрезентативного представления содержания учебного курса в содержании теста;

– гуманность и этичность – тестовые задания и процедура тестирования должны исключать нанесение какого-либо вреда обучающимся, не допускать ущемления их по национальному, этническому, материальному, расовому, территориальному, культурному и другим признакам;

Важнейшим является принцип, в соответствии с которым тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

закрытая форма – является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Например, обучающемуся задается вопрос, требующий альтернативного ответа «да» или «нет», «является» или «не является»,

«относится» или «не относится» и т.п. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя один или несколько правильных ответов и иногда называется выборочным заданием. Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде. Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

а) открытая форма – вопрос в открытой форме представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие – части слова или буквы, условные обозначения, линии или изображения элементов схемы и графика. Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

б) установление соответствия – в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

в) установление последовательности – предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

#### **а) критерии оценки тестовых заданий**

За тест студент может получить оценки «удовлетворительно», «хорошо» либо «отлично».

#### **б) описание шкалы оценивания**

Оценка «удовлетворительно» ставится, если студент дал верных ответов от 40 % до 70 %, оценка «хорошо» – если количество верных ответов от 70 % до 90 %, оценка «отлично» – не менее 90 %.

### **Текущий контроль успеваемости**

#### **Оценочные средства для текущего контроля знаний**

#### **Защита и презентация реферата на темы.**

1. Информационная безопасность бизнеса
2. Развитие службы информационной безопасности
3. Международная практика защиты информации
4. Модель Symantec LifeCycle Security
5. Постановка задачи анализа рисков
6. Модель Gartner Group
7. Модель Carnegie Mellon University
8. Различные взгляды на защиту информации
9. Национальные особенности защиты информации
10. Особенности отечественных нормативных документов
11. Учет остаточных рисков
12. Разработка корпоративной методики анализа рисков
13. Аудит информационной системы: рекомендации COBIT 3rd Edition
14. Методики и методологии выявления инсайдера в информационных системах

Критерии оценки реферата:

Изложенное понимание реферата как целостного авторского текста определяет критерии его оценки: новизна текста; обоснованность выбора источника; степень раскрытия сущности вопроса; соблюдения требований к оформлению.

**Новизна текста:** а) актуальность темы исследования; б) новизна и самостоятельность в постановке проблемы, формулирование нового аспекта известной проблемы в установлении новых связей (межпредметных, внутрипредметных, интеграционных); в) умение работать с исследованиями, критической литературой, систематизировать и структурировать материал; г) явленность авторской позиции, самостоятельность оценок и суждений; д) стилевое единство текста, единство жанровых черт.

**Степень раскрытия сущности вопроса:** а) соответствие плана теме реферата; б) соответствие содержания теме и плану реферата; в) полнота и глубина знаний по теме; г) обоснованность способов и методов работы с материалом; е) умение обобщать, делать выводы, сопоставлять различные точки зрения по одному вопросу (проблеме).

**Обоснованность выбора источников:** а) оценка использованной литературы: привлечены ли наиболее известные работы по теме исследования (в т.ч. журнальные публикации последних лет, последние статистические данные, сводки, справки и т.д.).

**Соблюдение требований к оформлению:** а) насколько верно оформлены ссылки на используемую литературу, список литературы; б) оценка грамотности и культуры изложения (в т.ч. орфографической, пунктуационной, стилистической культуры), владение терминологией; в) соблюдение требований к объёму реферата.

в) описание шкалы оценивания:

**Оценка 5(отлично)** ставится, если выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

**Оценка 4(хорошо)** – основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

**Оценка 3(удовлетворительно)** – имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

**Оценка 2(неудовлетворительно)** – тема реферата не раскрыта, обнаруживается существенное непонимание проблемы

### **Промежуточная аттестация**

#### **Форма промежуточной аттестации: зачет**

При проведении промежуточной аттестации студент должен ответить на вопросы теоретического характера и практического характера.

При оценивании ответа на вопрос теоретического характера учитывается:

- теоретическое содержание не освоено, знание материала носит фрагментарный характер, наличие грубых ошибок в ответе;
- теоретическое содержание освоено частично, допущено не более двух-трех недочетов;
- теоретическое содержание освоено почти полностью, допущено не более одного-двух недочетов, но обучающийся смог бы их исправить самостоятельно;
- теоретическое содержание освоено полностью, ответ построен по собственному плану.

При оценивании ответа на вопрос практического характера учитывается объем правильного решения.

Основой для определения оценки служит уровень усвоения студентами материала, предусмотренного рабочей программой дисциплины.

### **Примерные вопросы к зачету**

1. Базовый (Baseline) анализ рисков.
2. Полный (Full) анализ рисков
3. Классификация угроз информационной безопасности
4. Информационные угрозы, причины.
5. Последствия атаки
6. Несанкционированный доступ к данным через скрытые элементы данных.

7. Неправильное хранение носителей информации в случае аварий.
8. Риск нарушения информационной безопасности
- 9 .Анализ уязвимостей информационной системы.
- 10 .Недостатки в документировании коммуникаций.
11. Разрушение оборудования или данных в результате небрежности.
12. Опасности, связанные с увольнением или выведением персонала за штат.
13. Запрещенные действия в информационной системе.
14. Запрещенные действия системного администратора.
15. Неправильное администрирование сайта и прав доступа.
16. Смена пользователей ПК, не соответствующая внутренним правилам
17. Нарушение правил администрирования DBMS
18. Небрежность манипуляций с данными
19. Недостатки системы сегментации.
20. Уязвимости ПО или ошибки.
21. Понятие инсайдера и задача его выявления

### **Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья**

В ИнгГУ созданы специальные условия для получения высшего образования по образовательным программам обучающимися с ограниченными возможностями здоровья (ОВЗ).

Для перемещения инвалидов и лиц с ограниченными возможностями здоровья в ИнгГУ созданы специальные условия для беспрепятственного доступа в учебные помещения и другие помещения, а также их пребывания в указанных помещениях с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При получении образования обучающимся с ограниченными возможностями здоровья при необходимости предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература.

Получение доступного и качественного высшего образования лицами с ограниченными возможностями здоровья обеспечено путем создания в университете комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте университета .

Для обучения инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата обеспечиваются и совершенствуются материально-технические условия беспрепятственного доступа в учебные помещения, столовую, туалетные, другие помещения, условия их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и др.).

Для адаптации к восприятию инвалидами и лицами с ОВЗ с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой ИнгГУ по выбранной специальности, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
- тотально озвучивается; обеспечивается необходимый уровень освещенности помещений;
- предоставляется возможность использовать компьютеры во время занятий и право записи объяснения на диктофон (по желанию обучающегося).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ определяется преподавателем в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ с учетом его индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.