



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение
высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Факультет бизнес-коммуникаций и информатики

Кафедра естественнонаучных дисциплин

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине Б1.О.22 Информационная безопасность

направление подготовки 09.03.03 Прикладная информатика

направленность (профиль) Прикладная информатика

Одобрено
УМК факультета бизнес-коммуникаций
и информатики

Разработан в соответствии с ФГОС ВО

с учетом требований проф. стандарта

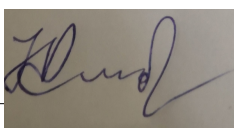
Председатель УМК

М.Г. Синчурина

ФИО, должность, ученая степень, звание

подпись, печать

Разработчики:



профессор

(занимаемая должность)

Н.В. Амбросов

(инициалы, фамилия)

Цель фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Б1.О.22 Информационная безопасность». Перечень видов оценочных средств соответствует рабочей программе дисциплины.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля (в следующих формах: тест, устный опрос, конспект лекций) и промежуточной аттестации в форме вопросов и заданий к экзамену.

Структура и содержание заданий – задания разработаны в соответствии с рабочей программой дисциплины «Б1.О.22 Информационная безопасность».

1. Паспорт фонда оценочных средств

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.2	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3	Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1	Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
	ОПК-4.2	Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
	ОПК-4.3	Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы

2. Показатели и критерии оценивания компетенций, шкалы оценивания

2.1. Показатели и критерии оценивания компетенций

№ п/п	Раздел, тема	Код индикатора компетенции	Наименование ОС	
			ТК	ПА
1	Введение в безопасность информационных систем.	ОПК-3.1, ОПК-3.2, ОПК-3.3	Тест, УО	Тест, КЛ
2	Угрозы безопасности информационных систем и их реализация.	ОПК-3.1, ОПК-3.2, ОПК-3.3	Тест, УО	Тест, КЛ
3	Криптографические системы защиты информации.	ОПК-3.1, ОПК-3.2, ОПК-3.3	Тест, УО	Тест, КЛ
4	Программно-технические средства защиты информации.	ОПК-3.1, ОПК-3.2, ОПК-3.3	Тест, УО	Тест, КЛ

2.2. Критерии оценивания результатов обучения для текущего контроля успеваемости и промежуточной аттестации

Оценочное средство	Критерии оценивания	Шкала оценивания
Тест	Студентом даны правильные ответы на 91-100% заданий	Отлично
	Студентом даны правильные ответы на 81-90% заданий	Хорошо
	Студентом даны правильные ответы на 71-80% заданий	Удовлетворительно
	Студентом даны правильные ответы менее чем на 70% заданий	Неудовлетворительно

Оценочное средство	Критерии оценивания	Шкала оценивания
Устный опрос	Ответ соответствует поставленной теме и содержит ответы на поставленные задачи, имеет четкую структуру, логически сопоставляемую с поставленными вопросами. Ответ демонстрирует способность анализировать и обобщать информацию, опираясь на знания, полученные в ходе изучения темы, а также демонстрировать самостоятельность автора в решении поставленных задач. Ответ содержит качественную речь и аргументацию, которая убедительно подтверждает выводы и ответы на поставленные вопросы	Отлично
	Ответ должен быть направлен на ответ на поставленные вопросы и соответствовать поставленной теме, иметь логическую цепочку рассуждений и четко демонстрировать связь между поставленными вопросами. Ответ выдержан в четкой форме, быть грамотно и без ошибок озвучен, выделены ключевые термины. Ответ должен демонстрировать способность анализировать и критически оценивать информацию, выбирая ключевые аспекты и выделяя главные выводы	Хорошо
	Ответ должен соответствовать поставленной теме и содержать ответы на поставленные вопросы, должен содержать существенную информацию, ясно передавать ответы и идеи. Ответ должен содержать достаточное количество аргументов и примеров, связанных с темой работы и позволяющих изложить свою точку зрения. Ответ должен быть грамотно сформулирован	Удовлетворительно
	Ответ не соответствует поставленной теме или не содержит ответов на поставленные задачи, содержит недостаточно аргументации и примеров, которые подтверждают высказанные в ответе идеи и выводы. Ответ не соответствует логической цепочке рассуждений и не выполняет требования логической последовательности высказывания, затрудняющей понимание ответа. Ответ содержит грубые ошибки, что затрудняет понимание высказывания	Неудовлетворительно

Оценочное средство	Критерии оценивания	Шкала оценивания
Конспект лекций	Все темы, предложенные для конспектирования были проработаны обучающимся, прочитан материал источников, выбрано главное и второстепенное, установлена логическая связь между элементами темы, выделены ключевые слова и понятия, конспект написан лаконично с применением системы условных сокращений	Отлично
	Все темы, предложенные для конспектирования были проработаны обучающимся, прочитан материал источников, выбрано главное и второстепенное, установлена логическая связь между элементами темы, выделены ключевые слова и понятия, конспект написан лаконично с применением системы условных сокращений	Хорошо
	Текст конспекта оформлен аккуратно, обучающимся выбрано главное и второстепенное, выделены ключевые слова и понятия	Удовлетворительно
	Текст конспекта не соответствует теме или не отражает ключевых положений изучаемой темы	Неудовлетворительно

2.3. Оценочные средства для текущего контроля (примеры)

2.3.1. Материалы для компьютерного тестирования обучающихся

Общие критерии оценивания

Процент правильных ответов	Оценка
91% – 100%	5 (отлично)
81% – 90%	4 (хорошо)
71% – 80%	3 (удовлетворительно)
Менее 70%	2 (неудовлетворительно)

Соответствие вопросов теста индикаторам формируемых и оцениваемых компетенций

№ вопроса в тесте	Код индикатора компетенции
1	ОПК-3.1, ОПК-3.2, ОПК-3.3
2	ОПК-3.1, ОПК-3.2, ОПК-3.3
3	ОПК-3.1, ОПК-3.2, ОПК-3.3
4	ОПК-3.1, ОПК-3.2, ОПК-3.3
5	ОПК-3.1, ОПК-3.2, ОПК-3.3
6	ОПК-3.1, ОПК-3.2, ОПК-3.3
7	ОПК-3.1, ОПК-3.2, ОПК-3.3
8	ОПК-3.1, ОПК-3.2, ОПК-3.3
9	ОПК-3.1, ОПК-3.2, ОПК-3.3

№ вопроса в тесте	Код индикатора компетенции
10	ОПК-3.1, ОПК-3.2, ОПК-3.3
11	ОПК-3.1, ОПК-3.2, ОПК-3.3
12	ОПК-3.1, ОПК-3.2, ОПК-3.3
13	ОПК-3.1, ОПК-3.2, ОПК-3.3
14	ОПК-3.1, ОПК-3.2, ОПК-3.3
15	ОПК-3.1, ОПК-3.2, ОПК-3.3
16	ОПК-3.1, ОПК-3.2, ОПК-3.3
17	ОПК-3.1, ОПК-3.2, ОПК-3.3
18	ОПК-3.1, ОПК-3.2, ОПК-3.3
19	ОПК-3.1, ОПК-3.2, ОПК-3.3
20	ОПК-3.1, ОПК-3.2, ОПК-3.3
21	ОПК-3.1, ОПК-3.2, ОПК-3.3

Ключ ответов

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
1	перебор
2	сети
3	поведение
4	a, b, c
5	внешние
6	сфере
7	b
8	доступностью
9	информации
10	полномочий
11	конфиденциальность
12	a, b, c
13	трудно
14	доступа
15	безопасностью
16	безопасности
17	три
18	оружию
19	роль
20	a, b, c
21	целостность

Перечень тестовых вопросов

№ 1. Задание открытой формы. Введите ответ.

Метод грубой атаки при дешифровке использует полный

№ 2. Задание открытой формы. Введите ответ.

Межсетевые фильтры обеспечивают защиту от распространения вредоносных воздействий по всей

№ 3. Задание открытой формы. Введите ответ.

Ментальное воздействие влияет на

№ 4. Задание с множественным выбором. Выберите 3 правильных ответа.

Основные аспекты безопасности информации

- а. конфиденциальность
- б. целостность
- с. доступность

№ 5. Задание открытой формы. Введите ответ.

Различают угрозы ИБ внутренние и

№ 6. Задание открытой формы. Введите ответ.

Информационная безопасность РФ - состояние защищенности национальных интересов в информационной

№ 7. Задание с единичным выбором. Выберите один правильный ответ.

Электронная подпись подтверждает личность

- а. автора криптографической системы
- б. автора письма

№ 8. Задание открытой формы. Введите ответ.

Свойство информации, позволяющее получать информацию субъектом с правом доступа называют

№ 9. Задание открытой формы. Введите ответ.

Стеганография обеспечивает сокрытие факта передачи

№ 10. Задание открытой формы. Введите ответ.

Мандатный метод доступа использует фиксированный набор

№ 11. Задание открытой формы. Введите ответ.

Доступ к информации только для тех, кто имеет право доступа называют

№ 12. Задание с множественным выбором. Выберите 3 правильных ответа.

Должны соблюдаться в информационной сфере интересы

- а. государства
- б. личности
- с. общества
- д. противника

№ 13. Задание открытой формы. Введите ответ.

Односторонняя функция в криптографии вычисляется в прямом направлении легко, а в обратном

№ 14. Задание открытой формы. Введите ответ.

Дискреционный метод управления доступом основан на использовании матрицы

№ 15. Задание открытой формы. Введите ответ.

Состояние защищенности национальных интересов в информационной сфере

называют информационной

№ 16. Задание открытой формы. Введите ответ.

Доктрина информационной безопасности РФ определяет правила и направления обеспечения информационной

№ 17. Задание открытой формы. Введите ответ.

В шифре Цезаря используется сдвиг на

№ 18. Задание открытой формы. Введите ответ.

Компьютерные вирусы, логические бомбы относят к информационному

№ 19. Задание открытой формы. Введите ответ.

Ролевой метод управления доступом вводит новую сущность

№ 20. Задание с множественным выбором. Выберите 3 правильных ответа.

Основные процедуры при входе в компьютерную систему

- a. авторизация
- b. аутентификация
- c. идентификация

№ 21. Задание открытой формы. Введите ответ.

Сохранение информации без искажений

2.3.2. Вопросы для коллоквиумов, собеседования для оценки компетенции

«ОПК-3.1»

№ 1. Геополитическое информационное противоборство.

№ 2. Выявление атак и защита при когнитивном воздействии.

№ 3. Поточковые методы шифрования.

№ 4. Популярные средства защиты информации.

2.3.3. Вопросы для коллоквиумов, собеседования для оценки компетенции

«ОПК-3.2»

№ 5. Геополитическое информационное противоборство.

№ 6. Выявление атак и защита при когнитивном воздействии.

№ 7. Поточковые методы шифрования.

№ 8. Популярные средства защиты информации.

2.3.4. Вопросы для коллоквиумов, собеседования для оценки компетенции

«ОПК-3.3»

№ 9. Выявление атак и защита при когнитивном воздействии.

№ 10. Поточковые методы шифрования.

№ 11. Популярные средства защиты информации.

3. Промежуточная аттестация

3.1. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и опыта деятельности

Экзамен является заключительным этапом процесса формирования компетенций обучающегося при изучении дисциплины и имеет целью проверку и оценку знаний обучающегося по теории, и применению полученных знаний, умений и навыков при решении практических задач.

Экзамен проводится по расписанию, сформированному учебно-методическим управлением, в сроки, предусмотренные календарным учебным графиком. Экзамен принимается преподавателем, ведущим лекционные занятия.

Экзамен проводится только при предъявлении обучающимся зачетной книжки и при условии выполнения всех контрольных мероприятий, предусмотренных учебным планом и рабочей программой дисциплины. Обучающимся на экзамене представляется право выбрать один из билетов. Время подготовки к ответу составляет 30 минут. По истечении установленного времени обучающийся должен ответить на вопросы экзаменационного билета. Результаты экзамена оцениваются по четырехбалльной системе и заносятся в зачетно-экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки. Подписанный преподавателем экземпляр ведомости сдается не позднее следующего дня в деканат.

В случае неявки обучающегося на экзамен в зачетно-экзаменационную ведомость делается отметка «не явка». Обучающиеся, не прошедшие промежуточную аттестацию по дисциплине, должны ликвидировать академическую задолженность в установленном локальными нормативными актами порядке.

3.2. Вопросы к экзамену

№	Вопрос	Код компетенции
1.	Информационная безопасность	ОПК-3.1, ОПК-3.2
2.	Геополитическое информационное противоборство	ОПК-3.1, ОПК-3.2, ОПК-3.3
3.	Доктрина информационной безопасности РФ	ОПК-3.1, ОПК-3.2
4.	Угрозы информационной безопасности	ОПК-3.1, ОПК-3.2, ОПК-3.3
5.	Угрозы безопасности информации	ОПК-3.1, ОПК-3.2, ОПК-3.3
6.	Угрозы информационной безопасности РФ	ОПК-3.1, ОПК-3.2, ОПК-3.3
7.	Источники угроз информационной безопасности РФ	ОПК-3.1, ОПК-3.2, ОПК-3.3
8.	Информационное оружие и информационные войны	ОПК-3.1, ОПК-3.2, ОПК-3.3
9.	Способы сокрытия информации	ОПК-3.1, ОПК-3.2, ОПК-3.3
10.	Развитие криптографических методов	ОПК-3.1, ОПК-3.2, ОПК-3.3
11.	Система Диффи-Хеллмана	ОПК-3.1, ОПК-3.2, ОПК-3.3
12.	Система Эль Гамала	ОПК-3.1, ОПК-3.2, ОПК-3.3
13.	Система RSA	ОПК-3.1, ОПК-3.2, ОПК-3.3
14.	Электронная подпись	ОПК-3.1, ОПК-3.2, ОПК-3.3
15.	Комплексный подход к ИБ предприятия	ОПК-3.1, ОПК-3.2, ОПК-3.3
16.	Методы и средства обеспечения ИБ на предприятии	ОПК-3.1, ОПК-3.2, ОПК-3.3
17.	Управление доступом	ОПК-3.1, ОПК-3.2, ОПК-3.3
18.	Технические средства защиты информации	ОПК-3.1, ОПК-3.2, ОПК-3.3
19.	Программно-аппаратные средства защиты информации	ОПК-3.1, ОПК-3.2, ОПК-3.3

3.3. Тематика курсовых работ

По данной дисциплине выполнение курсовых проектов (работ) не предусматривается.

3.4. Материалы для компьютерного тестирования обучающихся

Общие критерии оценивания

Процент правильных ответов	Оценка
91% – 100%	5 (отлично)
81% – 90%	4 (хорошо)
71% – 80%	3 (удовлетворительно)
Менее 70%	2 (неудовлетворительно)

Соответствие вопросов теста индикаторам формируемых и оцениваемых компетенций

№ вопроса в тесте	Код индикатора компетенции
1	ОПК-3.1, ОПК-3.2, ОПК-3.3
2	ОПК-3.1, ОПК-3.2, ОПК-3.3
3	ОПК-3.1, ОПК-3.2, ОПК-3.3
4	ОПК-3.1, ОПК-3.2, ОПК-3.3
5	ОПК-3.1, ОПК-3.2, ОПК-3.3
6	ОПК-3.1, ОПК-3.2, ОПК-3.3
7	ОПК-3.1, ОПК-3.2, ОПК-3.3
8	ОПК-3.1, ОПК-3.2, ОПК-3.3
9	ОПК-3.1, ОПК-3.2, ОПК-3.3
10	ОПК-3.1, ОПК-3.2, ОПК-3.3
11	ОПК-3.1, ОПК-3.2, ОПК-3.3
12	ОПК-3.1, ОПК-3.2, ОПК-3.3
13	ОПК-3.1, ОПК-3.2, ОПК-3.3
14	ОПК-3.1, ОПК-3.2, ОПК-3.3
15	ОПК-3.1, ОПК-3.2, ОПК-3.3
16	ОПК-3.1, ОПК-3.2, ОПК-3.3
17	ОПК-3.1, ОПК-3.2, ОПК-3.3
18	ОПК-3.1, ОПК-3.2, ОПК-3.3
19	ОПК-3.1, ОПК-3.2, ОПК-3.3
20	ОПК-3.1, ОПК-3.2, ОПК-3.3
21	ОПК-3.1, ОПК-3.2, ОПК-3.3

Ключ ответов

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
1	перебор
2	сети
3	поведение
4	a, b, c
5	внешние
6	сфере
7	b

№ вопроса в тесте	Номер ответа (или ответ, или соответствие)
8	доступностью
9	информации
10	полномочий
11	конфиденциальность
12	a, b, c
13	трудно
14	доступа
15	безопасностью
16	безопасности
17	три
18	оружию
19	роль
20	a, b, c
21	целостность

Перечень тестовых вопросов

№ 1. Задание открытой формы. Введите ответ.

Метод грубой атаки при дешифровке использует полный

№ 2. Задание открытой формы. Введите ответ.

Межсетевые фильтры обеспечивают защиту от распространения вредоносных воздействий по всей

№ 3. Задание открытой формы. Введите ответ.

Ментальное воздействие влияет на

№ 4. Задание с множественным выбором. Выберите 3 правильных ответа.

Основные аспекты безопасности информации

a. конфиденциальность

b. целостность

c. доступность

№ 5. Задание открытой формы. Введите ответ.

Различают угрозы ИБ внутренние и

№ 6. Задание открытой формы. Введите ответ.

Информационная безопасность РФ - состояние защищенности национальных интересов в информационной

№ 7. Задание с единичным выбором. Выберите один правильный ответ.

Электронная подпись подтверждает личность

a. автора криптографической системы

b. автора письма

№ 8. Задание открытой формы. Введите ответ.

Свойство информации, позволяющее получать информацию субъектом с правом доступа называют

№ 9. Задание открытой формы. Введите ответ.

Стеганография обеспечивает сокрытие факта передачи

№ 10. Задание открытой формы. Введите ответ.

Мандатный метод доступа использует фиксированный набор

№ 11. Задание открытой формы. Введите ответ.

Доступ к информации только для тех, кто имеет право доступа называют

№ 12. Задание с множественным выбором. Выберите 3 правильных ответа.

Должны соблюдаться в информационной сфере интересы

a. государства

b. личности

c. общества

d. противника

№ 13. Задание открытой формы. Введите ответ.

Односторонняя функция в криптографии вычисляется в прямом направлении легко, а в обратном

№ 14. Задание открытой формы. Введите ответ.

Дискреционный метод управления доступом основан на использовании матрицы

№ 15. Задание открытой формы. Введите ответ.

Состояние защищенности национальных интересов в информационной сфере называют информационной

№ 16. Задание открытой формы. Введите ответ.

Доктрина информационной безопасности РФ определяет правила и направления обеспечения информационной

№ 17. Задание открытой формы. Введите ответ.

В шифре Цезаря используется сдвиг на

№ 18. Задание открытой формы. Введите ответ.

Компьютерные вирусы, логические бомбы относят к информационному

№ 19. Задание открытой формы. Введите ответ.

Ролевой метод управления доступом вводит новую сущность

№ 20. Задание с множественным выбором. Выберите 3 правильных ответа.

Основные процедуры при входе в компьютерную систему

a. авторизация

b. аутентификация

c. идентификация

№ 21. Задание открытой формы. Введите ответ.

Сохранение информации без искажений

3.5. Конспекты лекций для оценки компетенции «ОПК-3.1»

№ 1. Введение в безопасность информационных систем.

№ 2. Угрозы безопасности информационных систем и их реализация.

№ 3. Криптографические системы защиты информации.

№ 4. Программно-технические средства защиты информации.

3.6. Конспекты лекций для оценки компетенции «ОПК-3.2»

№ 5. Введение в безопасность информационных систем.

№ 6. Угрозы безопасности информационных систем и их реализация.

№ 7. Криптографические системы защиты информации.

№ 8. Программно-технические средства защиты информации.

3.7. Конспекты лекций для оценки компетенции «ОПК-4.1»

№ 9. Введение в безопасность информационных систем.

№ 10. Угрозы безопасности информационных систем и их реализация.

№ 11. Криптографические системы защиты информации.

№ 12. Программно-технические средства защиты информации.

3.8. Конспекты лекций для оценки компетенции «ОПК-3.3»

№ 13. Угрозы безопасности информационных систем и их реализация.

№ 14. Криптографические системы защиты информации.

№ 15. Программно-технические средства защиты информации.