Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Филологический факультет

УТВЕРЖДЕНО:
Декан
И. В. Тубалова

Оценочные материалы по дисциплине

Основы информационной безопасности

по направлению подготовки

45.04.03 Фундаментальная и прикладная лингвистика

Направленность (профиль) подготовки:
Компьютерная и когнитивная лингвистика

Форма обучения
Очная

Квалификация
Магистр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
З.И. Резанова

Председатель УМК
Ю.А. Тихомирова

Томск – 2025

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-3 Способен выбирать оптимальные подходы и методы решения конкретных научных и прикладных задач в области лингвистики и информационных технологий.

ОПК-6 Способен осуществлять эффективное управление разработкой программных средств информационных проектов в сфере своей профессиональной деятельности.

ПК-4 Способен разрабатывать проекты прикладной направленности в области когнитивной и компьютерной лингвистики с применением современных технических средств и информационных технологий, в том числе в области искусственного интеллекта.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-3.3 Способен решать конкретные научные и прикладные задачи в области лингвистики и информационных технологий на основе самостоятельного выбора оптимальных подходов и методов их решения

ИОПК-6.2 Разрабатывает алгоритмы и программы для решения лингвистических и междисциплинарных задач в том числе с применением высокопроизводительных вычислительных технологий

ИОПК-6.3 Разрабатывает и отлаживает программный код, направленный на решение лингвистических и междисциплинарных задач с применением современных языков программирования

ИПК-4.2 Разрабатывает программу действий по решению задач проекта в области когнитивной и компьютерной лингвистики с учетом имеющихся технических средств и информационных технологий, в том числе в области искусственного интеллекта

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– тесты;

– устные или письменные вопросы;

Пример тестового задания

Тест (ОПК-3, ОПК-6, ПК-4, ИОПК-3.3., ИОПК-6.2, ИОПК-6.3, ИПК-4.2)

1. Наукой, изучающей математические методы защиты информации путем ее преобразования, является
   A. криптоанализ
   B. криптология
   C. стеганография
   D. криптография
2. Конечное множество используемых для кодирования информации знаков называется
   A. шифром
   B. кодом
   C. алфавитом
   D. ключом
3. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет
   A. криптология
   B. стеганография
   C. криптоанализ
   D. криптография

Критерии оценивания: тест считается пройденным, если обучающий ответил правильно как минимум на половину вопросов.

Примерный перечень теоретических вопросов (ИОПК-3.3., ИОПК-6.2, ИОПК-6.3, ИПК-4.2)

1. Информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
2. Классификация угроз информационной безопасности и их сравнительный анализ.
3. Информационная безопасность в современных условиях хозяйствования. Общегосударственные цели, задачи и методы обеспечения информационной безопасности.
4. Понятия о видах вирусов. Классификация вирусов и угрозы для информационной инфраструктуры хозяйствующих субъектов.
5. Виды возможных нарушений информационной безопасности в сфере финансовой деятельности.
6. Отечественные и международные стандарты обеспечения информационной безопасности.
7. Особенности современной нормативно-правовой и методологической базы обеспечения информационной безопасности.
8. Основные нормативные руководящие документы, касающиеся конфиденциальной информации и государственной тайны, нормативно-справочные документы по обеспечению информационной безопасности применяемые в финансовой деятельности.
9. Общие критерии оценки безопасности информационных систем и технологий ГОСТ 15408, как основа определения требований к обеспечению информационной безопасности.
10. Место информационной безопасности экономических систем в национальной безопасности страны.
11. Цели и задачи обеспечения национальной безопасности. Система целеполагания в структуре государственного и муниципального управления при обеспечении информационной безопасности.
12. Основные положения концепции информационной безопасности. Сравнительная таблица.
13. Государственные информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
14. Взаимосвязь государственных и коммерческих информационных ресурсов (конфиденциальной информации и государственной тайны).
15. Модели безопасности, и их применение.

Критерии оценивания:

Результаты контрольной работы определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если даны правильные ответы на все теоретические вопросы и все задачи решены без ошибок.

Оценка «хорошо» выставляется, если частично даны правильные ответы на все теоретические вопросы и все задачи решены без ошибок.

Оценка «удовлетворительно» выставляется, если частично даны правильные ответы на все теоретические вопросы и все задачи решены с ошибками.

Оценка «не удовлетворительно» выставляется, если нет правильных ответов на все теоретические вопросы и все задачи решены с ошибками.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

В этом разделе следует описать форму и структуру промежуточной аттестации, перечислить вопросы, задачи или задания, выносимые на зачет или экзамен, описать критерии оценивания ответов.

Структура экзамена должна соответствовать компетентностной структуре дисциплины. При описании системы оценивания итогового контроля по дисциплине необходимо продемонстрировать достижение всех запланированных индикаторов – результатов обучения.

Также необходимо описать каким образом текущий контроль влияет на промежуточную аттестацию (студент имеет право проходить промежуточную аттестацию вне зависимости от результатов текущей успеваемости) и в каком случае ставится оценка «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

В случае применения балльно-рейтинговой системы необходимо описать механизм перевода оценки в пятибалльную шкалу. Балльно-рейтинговая система должна учитывать результаты текущего контроля и промежуточной аттестации и на промежуточную аттестацию должно отводиться не более 40% рейтинга.

Зачет состоит из двух частей.

Первая часть представляет собой тест из 5 вопросов, проверяющих ОПК-3, ОПК-6, ПК-4. Ответы на вопросы первой части даются путем выбора из списка предложенных.

Вторая часть содержит один вопрос, проверяющий ИОПК-3.3., ИОПК-6.2, ИОПК-6.3, ИПК-4. Ответ на вопрос второй части дается в развернутой форме.

Примеры тестовых заданий:

1. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

A. актуальностью информации
B. доступностью
C. качеством информации
D. целостностью
E. 2. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев
A. C
B. A
C. B
D. D

3. Организационные требования к системе защиты

A. управленческие и идентификационные
B. административные и аппаратурные
C. административные и процедурные
D. аппаратурные и физические

4. Основу политики безопасности составляет

A. программное обеспечение
B. управление риском
C. способ управления доступом
D. выбор каналов связи

5. Соответствие средств безопасности решаемым задачам характеризует

A. эффективность
B. корректность
C. адекватность
D. унификация

Примерный перечень теоретических вопросов:

1. Основные положения концепции информационной безопасности. Сравнительная таблица.
2. Государственные информационные ресурсы, подлежащие защите в сфере финансовой деятельности.
3. Взаимосвязь государственных и коммерческих информационных ресурсов (конфиденциальной информации и государственной тайны).

4. Модели безопасности, и их применение.
5. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Оценка системы защиты информации.
6. Оценка эффективности средств и механизмов обеспечения информационной безопасности.
7. Методы анализа способов нарушений информационной безопасности.
8. Программно-аппаратные комплексы криптографической защиты, их характеристики и особенности применения. Сравнительная таблица.
9. Нормативно-правовая база криптографической защиты.

Критерии оценивания:

Результаты контрольной работы определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется, если даны правильные ответы на все теоретические вопросы и все задачи решены без ошибок.

Оценка «хорошо» выставляется, если частично даны правильные ответы на все теоретические вопросы и все задачи решены без ошибок.

Оценка «удовлетворительно» выставляется, если частично даны правильные ответы на все теоретические вопросы и все задачи решены с ошибками.

Оценка «не удовлетворительно» выставляется, если нет правильных ответов на все теоретические вопросы и все задачи решены с ошибками.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Оценочные материалы для проверки остаточных знаний могут быть использованы для формирования программы ГИА (программы государственного экзамена), а также экспертом Рособрнадзора при проведении проверки диагностической работы по оценки уровня форсированности компетенций обучающихся (при контрольно-надзорной проверке). Вопросы данного раздела показывают вклад дисциплины в образовательный результат образовательной программы. Объем заданий в данном разделе зависит как от количества формируемых индикаторов достижения компетенций, так и от объема дисциплины по учебному плану.

Тест

1. Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:

а) со стороны злоумышленника;

б) со стороны законного отправителя сообщения;

в) со стороны законного получателя сообщения.

2. Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?

а) асимметричный;

б) симметричный;

в) правильного ответа нет

3. Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется:

а) шифрование;

б) дешифровка;

в) расшифровка.

4. В каких основных форматах существует симметричный алгоритм?

а) блока и строки;
б) потока и блока;
в) потока и данных
5. Открытым текстом в криптографии называют:
а) расшифрованный текст;
б) любое послание;
в) исходное послание.
6. Какой ключ известен только приемнику?
а) открытый;
б) закрытый.
7. Наука, занимающаяся защитой информации, путем преобразования этой информации это:
а) Криптография;
б) криптология;
в) криптоанализ.
Теоретические вопросы:
1. Примеры угроз доступности.
2. Вредоносное программное обеспечение.
3. Грани вредоносного ПО.
4. Основные угрозы целостности.
5. Основные угрозы конфиденциальности.
6. Что такое законодательный уровень информационной безопасности и почему он важен?
7. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
8. Закон «об информации, информатизации и защите информации» и устанавливаемые им основные определения.
9. Цели защиты информации согласно закону «об информации, информатизации и защите информации».
10. Закон "о лицензировании отдельных видов деятельности" и его определения.
11. Электронный документ, электронная цифровая подпись, владелец сертификата ключа подписи, средства электронной цифровой подписи, сертификат средств электронной цифровой подписи.
12. Закрытый ключ электронной цифровой подписи, открытый ключ электронной цифровой. подписи, сертификат ключа подписи, подтверждение подлинности электронной цифровой. подписи в электронном документе, информационная система общего пользования,
13. Корпоративная информационная система.

Информация о разработчиках

Степаненко Андрей Александрович, старший преподаватель кафедры «Общей, компьютерной и когнитивной лингвистики»