Министерство науки и высшего образования
Российской Федерации
Министерство науки, высшего образования и инноваций
Кыргызской Республики

Государственное образовательное учреждение
высшего профессионального образования
Кыргызско-Российский Славянский университет имени
первого президента Российской Федерации Б.Н. Ельцина
Естественно-технический факультет

Кафедра Информационных и вычислительных технологий

Фонд
оценочных средств

по дисциплине «Информационная безопасность открытых систем»

Уровень высшего образования

МАГИСТРАТУРА

Направление подготовки

09.04.04 - РФ, 710400 - КР Программная инженерия

(код и наименование направления подготовки)

Разработка программно-информационных систем

(профиля) образовательной программы)

Квалификация

магистр

Фонд оценочных средств предназначен для контроля знаний обучающихся по направлению подготовки 09.04.04 – РФ, 710400 - КР «Программная инженерия» по дисциплине *« Информационная безопасность открытых систем»*.

Фонд оценочных средств рассмотрен и утвержден на заседании кафедры Информационных и вычислительных технологий

Заведующий кафедрой
д.т.н., проф. Лыченко Н.М.

Исполнители (разработчики):
к.т.н., доцент кафедры ИВТ, Демиденко А.П.;
ст.преп. кафедры ИВТ, Беляев А.А.

СОГЛАСОВАНО:
И.О. декана ЕТФ

Комарцов Н.М.

Раздел 1. Перечень компетенций, с указанием этапов их формирования в процессе освоения дисциплины/практики

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Виды оценочных средств/ шифр раздела в данном документе
ОПК-7: Способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях	**Знать:** особенности построения открытых систем и системы защиты информации для них.	**Блок А –** задания репродуктивного уровня - Тесты - Контрольная работа.
	Уметь: применять методы и средства обеспечения информационной безопасности открытых систем	**Блок В** – задания реконструктивного уровня - Практические работы - Контрольная работа
	Владеть: навыками аудита открытых систем	**Блок С** – задания практико-ориентированного и/или исследовательского уровня Практические работы

Раздел 2. Технологическая карта дисциплины
Информационная безопасность открытых систем

Курс 2, семестр 3, Количество ЗЕ -4, Отчетность – зачет с оценкой

Название модулей дисциплины согласно РПД	Контроль	Форма контроля	зачетный минимум	зачетный максимум	График контроля
1. Стандартизация и модельное представление открытых информационных систем	текущий	Тест	3	5	4
	рубежный	Защита практической работы.	7	10	
2 Атаки на открытые системы	текущий	Тест	3	5	11
	рубежный	Защита практической работы	7	10	
3 Аутентификация субъектов и объектов взаимодействия в открытых системах. Межсетевые экраны	текущий	Тест	3	5	14
	рубежный	Защита практической работы. Контрольная работа.	7	15	
4 Криптографическая защита в открытых системах	текущий	Тест	3	5	17
	рубежный	Защита практической работы.	7	15	
ВСЕГО за семестр			40	70	

Промежуточный контроль (Зачет с оценкой)	20	30	
Семестровый рейтинг по дисциплине	60	100	

Раздел 3. Типовые контрольные задания и иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (оценочные средства)

Блок А

Вопросы теста

Тест. Модуль 1

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

Тест. Модуль 2

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
- Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания

Тест. Модуль 3
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных
тест_20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
- Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальность

Тест. Модуль 4
23) Угроза информационной системе (компьютерной сети) – это:

- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
- Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:- -
Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

Контрольная работа. Пример вопросов

1. Шифрование с открытым ключом. Как реализовать аутентификацию, цифровую подпись и конфиденциальность.
2. Алгоритм RSA. Для каких целей применяется. Подробно

Блоки В и С

Практические задания

Практическая работа 1 Построение модели открытых систем

- Исследовать функции физического уровня модели OSI;
- Реализовать канальный уровень модели OSI:
- Исследовать корректность передачи каждого кадра.

Практическая работа 2 Защищенность сетей передачи данных

- Исследовать защищенность сетей передачи данных.

Практическая работа 3 Разработка политик безопасности.

- Проверить политику безопасности и других документов в области информационной безопасности конкретного предприятия.
- Разработать политику безопасности (Предмет политики. Описание позиции организации. Применимость)

Практическая работа №4 Выбор реализации межсетевых экранов.

- Выбрать одну из реализаций межсетевых экранов
- Оценить критерии реализации межсетевых экранов.

Практическая работа №5 Система PGP.

- Установить PGP и исследовать его возможности.
- Установить Mozilla Thunderbird.

- Установить Enigmail.

Контрольная работа. *Пример заданий*
Используя задачу о рюкзаке, зашифруйте слово “ШИФР”

Блок D (промежуточный контроль)

Вопросы для проверки уровня обученности ЗНАТЬ

1. Концепция безопасности.
2. Сетевые и системные угрозы (атаки).
4. Аудит сетевых систем.
5. Брандмауэры.
6. Обнаружение попыток взлома.
7. Криптография.
8. SSL.
9. Уровни безопасности компьютеров.
10. Решение проблем безопасности в Windows NT.
11. Политики безопасности.
12. Управление правами доступа.
13. Матричная модель доступа (модель Харрисона-Руззо-Ульмана).
14. Многоуровневая модель доступа (модель Белла-Лападулы).
15. Защита информации от несанкционированного доступа.
16. Защита от несанкционированного копиро-вания.
17. Аутентификация сообщений. Типы функций аутентификации.
18. Традиционное шифрование и аутентификация.
19. Шифрование с открытым ключом. Аутентификация и цифровая подпись.
20. Шифрование с открытым ключом. Аутентификация, цифровая подпись и конфиденциальность.
21. Код аутентичности сообщений (MAC).
22. Код аутентичности сообщений на основе DES.
23. Защита от разрушающих программных воздействий.
24. Вредоносные программы и их классификация.
26. Проблемы обеспечения безопасности при удаленном доступе.
27. Персональные и межсетевые защитные средства.

Задания для проверки уровня обученности УМЕТЬ

1 Реализовать авторизацию в доменах Windows.
2. Выполнить защиту от несанкционированного копирования.
3.Показать на примере борьбу с сетевыми атаками.
4. Показать на примере методы обнаружения и удаления вирусов и восстановления программного обеспечения.

Навыки для проверки уровня обученности ВЛАДЕТЬ

1. Используйте классические алгоритмы шифрования.
2. Примените алгоритмы шифрования с открытым ключом для обеспечения конфиденциальности, аутентификации и цифровой подписи.
3. Продемонстрируйте умение владеть приемами использования MAC.

Пример

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ № ___

1. Вопросы для проверки уровня обученности ЗНАТЬ
1.1 Управление правами доступа.
1.2. Матричная модель доступа (модель Харрисона-Руззо-Ульмана).
2. Задание для проверки уровня обученности УМЕТЬ и ВЛАДЕТЬ
1.1 Реализовать авторизацию в доменах Windows.

Раздел 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Применяемые оценочные средства:

- Тест (текущая аттестация)
- Сдача практических работ на практических занятиях в соответствии с технологической картой дисциплины (рубежная аттестация),
- Написание контрольной работы (рубежная аттестация)
- Письменный опрос по экзаменационным билетам (промежуточная аттестация - зачет с оценкой),

Все виды оценочных средств оцениваются в соответствии со шкалами оценивания.

ШКАЛА ОЦЕНИВАНИЯ ТЕСТА (текущий контроль)

1. В одном тестовом задании некоторое количество закрытых вопросов.
2. К заданиям даются готовые ответы на выбор, один правильный и остальные неправильные.
3. Обучающемуся необходимо помнить: в каждом задании с выбором одного правильного ответа правильный ответ должен быть.
4. За каждый правильно ответ – 5 баллов
5. Определяется сумма набранных баллов.
6. Вычисляется отношение набранных баллов к максимально возможным за тест. Отметка выражается в %.

ШКАЛА ОЦЕНИВАНИЯ ПРАКТИЧЕСКИХ (ЛАБОРАТОРНЫХ) РАБОТ (текущий/рубежный контроль)

- 85-100 % - Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию, выполнены.
- 70-84 % - Демонстрирует значительное понимание проблемы. Все требования, предъявляемые к заданию, выполнены.
- 60-69 % - Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых к заданию выполнены.
- 31-60 % - Демонстрирует небольшое понимание проблемы. Многие требования, предъявляемые к заданию не выполнены.
- 0-30 % - Демонстрирует непонимание проблемы и даже не было попытки решить задачу.

ШКАЛА ОЦЕНИВАНИЯ КОНТРОЛЬНЫХ РАБОТ (рубежный контроль)

- 85-100 % - Демонстрирует полное понимание проблемы. Все задания выполнены.
- 70-84 % - Демонстрирует значительное понимание проблемы. Все задания выполнены, но содержат некоторые неточности.
- 60-69 % - Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых к заданию, выполнены.
- 31-60 % - Демонстрирует небольшое понимание проблемы. Многие требования, предъявляемые к заданию, не выполнены.
- 0-30 % - Демонстрирует непонимание проблемы или нет ответа и даже не было попытки решить задачу.

ШКАЛА ОЦЕНИВАНИЯ ПИСЬМЕННОГО ОПРОСА

(**промежуточный контроль** – «ЗНАТЬ»)

Отметкой (7-10- баллов) оценивается ответ, который показывает прочные знания теоретических основ дисциплины, понимание и правильное применение терминологии, правильные ответы на 75-100% вопросов

Отметкой (5-7 баллов) оценивается ответ, который показывает знание теоретических основ дисциплины, но неполное понимание и не всегда правильное применение терминологии, даны правильные ответы на 50-74% вопросов, в ответах допущено некоторое количество неточностей.

Отметкой (3-4 баллов) оценивается ответ, свидетельствующий о знакомстве с некоторыми теоретическими основами дисциплины. Даны правильные ответы на 25-49% вопросов, допущены неточности и ошибки.

Отметкой (2 балла) оценивается ответ, обнаруживающий незнание теоретических основ дисциплины. Отмечается отсутствие логичности и последовательности в ответе. Менее 25% правильных ответов. Допущены серьезные ошибки в содержании ответа.

Отметкой (0-1 балл) оценивается ответ, при котором студент демонстрирует непонимание поставленных вопросов, или нет ответа.

ШКАЛА ОЦЕНИВАНИЯ ПРАКТИЧЕСКИХ ЗАДАНИЙ

(**промежуточный контроль** – «УМЕТЬ и ВЛАДЕТЬ»)

Отметкой (8-10 баллов) оценивается ответ, при котором студент правильно отвечает на поставленные вопросы, Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию, выполнены.

Отметкой (5-7 баллов) оценивается ответ, при котором студент в основном правильно отвечает на поставленные вопросы. Демонстрирует значительное понимание проблемы. Большинство требований, предъявляемых к заданию, выполнены.

Отметкой (2-4 баллов) оценивается ответ, при котором студент в основном не правильно отвечает на поставленные вопросы. Демонстрирует частичное или небольшое понимание проблемы. Многие требования, предъявляемые к заданию, не выполнены.

Отметкой (0 -1 балл) оценивается ответ, при котором студент демонстрирует непонимание проблемы или нет ответа и даже не было попытки решить задачи.

В экзаменационный билет включены два теоретических вопроса и практическое задание, соответствующие содержанию формируемых компетенций. Зачет с оценкой проводится в письменной форме. На ответ и решение задачи студенту отводится 80 минут. За ответ на теоретические вопросы студент может получить максимально 15 баллов, за выполнение практических заданий - 15 баллов.

По итогам прохождения дисциплины и с учетом шкал оценивания все набранные в результате текущей, рубежной и промежуточной аттестаций баллы суммируются и выставляется оценка .

Перевод баллов в оценку:

85 - 100 баллов – «отлично»

70 - 84 баллов – «хорошо»

60 - 69 баллов – «удовлетворительно»

менее 60 баллов – «неудовлетворительно»

Раздел 5. Методические указания для обучающегося по освоению дисциплины и выполнению контрольных заданий

5.1. Общие рекомендации к организации самостоятельной работы

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, особое внимание, уделяя целям из задачам, структуре и содержанию курса. Работа с конспектом лекций. Необходимо просмотреть конспект сразу после занятий, отметить материал конспекта лекций, который вызывает затруднение для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось

разобраться в материале, то необходимо сформулировать вопросы и обратиться на ближайшей лекции за помощью к преподавателю. Каждую неделю нужно отводить время для повторения, пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

5.2. Подготовка к практическим занятиям

Перед посещением практического занятия изучить теорию вопроса, предполагаемого к исследованию. Оформление отчётов должно производиться по представленному образцу после окончания работы непосредственно в аудитории. Для подготовки к защите отчёта следует проанализировать экспериментальные результаты, обобщать результаты исследований в виде 2. выводов, подготовить ответы на вопросы.