Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Технический институт (филиал) ФГАОУ ВО «СВФУ» в г. Нерюнгри

Кафедра Математики и информатики

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Б1.О.25 Информационная безопасность

для программы бакалавриата
по направлению подготовки 09.03.03 - Прикладная информатика
Направленность (профиль) программы: Прикладная информатика в менеджменте

Форма обучения: очная

Нерюнгри 2024

УТВЕРЖДЕНО на заседании
выпускающей кафедры МиИ
«24» апреля 2024 г., протокол № 10
Заведующий кафедрой _____ / Самохина В.М.
«24» апреля 2024 г.

УТВЕРЖДЕНО на заседании
обеспечивающей кафедры МиИ
«24» апреля 2024 г., протокол № 10
Заведующий кафедрой _____ / Самохина В.М.
«24» апреля 2024 г.

СОГЛАСОВАНО:
Эксперты[1]:

Самохина В.М., к.п.н, доцент кафедры МиИ _____
Ф.И.О., должность, организация подпись

Семенова Е.О., ассистент кафедры МиИ _____
Ф.И.О., должность, организация подпись

СОСТАВИТЕЛЬ (И):

Похорукова М.Ю., к.т.н., доцент кафедры МиИ _____
Ф.И.О., должность, организация подпись

[1] Эксперт первый: со стороны выпускающей кафедры (или работодатель). Эксперт второй: со стороны обеспечивающей кафедры.

Паспорт фонда оценочных средств
Б1.О.25 Информационная безопасность

№	Контролируемые разделы (темы) дисциплины	Планируемые результаты освоения программы (содержание и коды компетенций)	Планируемые результаты обучения по дисциплине	Наименование оценочного средства
1.	Информационная безопасность и уровни ее обеспечения.	**УК-2:** Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**Знать:** о правовых и экономических основах разработки и реализации проектов, действующие правовые нормы и их источники. **Уметь:** оформлять проект в виде документа в соответствии со стандартами достигать результативности проекта **Владеть:** навыками работы с правовыми и нормативными документами, применяемыми в профессиональной деятельности	Лабораторные работы, СРС, контрольная работа, тестирование
2.	Компьютерные вирусы и защита от них.	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;	**Знать:** 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 **Уметь:** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности **Владеть:** навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности	
3.	Информационная безопасность вычислительных систем.	ОПК-7: Способен разрабатывать алгоритмы и программы, пригодные для практического применения.	**Знать:** основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий **Уметь:** применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ **Владеть:** навыками программирования, отладки и тестирования прототипов программно-технических комплексов задач	
4.	**Механизмы обеспечения «информационной безопасности».**			

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Технический институт (филиал) ФГАОУ ВО «СВФУ» в г. Нерюнгри

КАФЕДРА МАТЕМАТИКИ И ИНФОРМАТИКИ

Самостоятельная работа

Включает проработку конспектов лекций, обязательной и дополнительной учебной литературы в соответствии с планом занятия. Основной формой проверки СРС является устный фронтальный опрос на занятии, письменные ответы на контрольные вопросы для проверки знаний по теме либо выполнение практических заданий по заданной теме.

СРС 1. Понятие «информационная безопасность». Составляющие информационной безопасности.
СРС 2. Классификация угроз «информационной безопасности».
СРС 3. Классификация компьютерных вирусов.
СРС 4. Антивирусные программы.
СРС 5. Особенности обеспечения информационной безопасности в компьютерных сетях.
СРС 6. Классификация удаленных угроз в вычислительных сетях.
СРС 7. Криптография и шифрование.
СРС 8. Технология виртуальных частных сетей (VPN).

Примерный перечень контрольных вопросов:

1. Каковы характерные черты компьютерных вирусов?
2. Дайте определение программного вируса.
3. Перечислите классификационные признаки компьютерных вирусов.
4. В чем особенности резидентных вирусов?
5. Перечислите деструктивные возможности компьютерных вирусов.
6. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.

Критерии оценки:

0 баллов – самостоятельная работа не выполнена.
1 балл - ставится, если студент обнаруживает знание и понимание основных положений лабораторной работы, но при выполнении заданий допущены ошибки или задание выполнено на 50%; оформление работы выполнено недостаточно последовательно (отсутствуют цель/листинг/результаты/выводы).
2 балла - ставится, если студентом при выполнении заданий допущены неточности или задание выполнено на 70%; оформление работы выполнено с ошибками (отсутствуют цель/выводы).
3 балла - ставится, если студент полностью выполнил задание, правильно ответил на теоретические вопросы преподавателя, оформление работы выполнено последовательно и полно (присутствуют цели работы, задания, листинг программ, результаты и выводы).

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Технический институт (филиал) ФГАОУ ВО «СВФУ» в г. Нерюнгри

КАФЕДРА МАТЕМАТИКИ И ИНФОРМАТИКИ

Лабораторные работы

В период освоения дисциплины студенты посещают лекционные занятия, самостоятельно изучают дополнительный теоретический материал к практическим занятиям.

Критериями для оценки результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения учебного материала;
- умение использовать теоретические знания при выполнении практических задач;
- сформированность общеучебных умений;
- обоснованность и четкость изложения ответа.

Максимальный балл, который студент может набрать на лабораторном занятии – **3 балла.**

Темы лабораторных работ

Тема 1. Информационная безопасность и уровни ее обеспечения.

Тема 2. Компьютерные вирусы и защита от них.

Тема 3. Информационная безопасность вычислительных систем.

Тема 4. Механизмы обеспечения «информационной безопасности».

Критерии оценки:

№	Критерий	1б	0б
1	Актуальность: конкретность и достижимость целей и задач; соответствие разработки современным подходам к рассматриваемой проблеме; соответствие целей и задач ожидаемым результатам; четкость формулировки ожидаемых результатов		
2	Содержание теоретического материала: соответствие содержания заявленной теме; отсутствие в тексте отступлений от темы; логичность и последовательность в изложении материала; способность к работе с литературными источниками, Интернет-ресурсами, справочной и энциклопедической литературой		
3	Оформление правильность оформления (наличие всех структурных частей, структурная упорядоченность, ссылки на литературу, цитаты, таблицы, рисунки и т.д.); соответствие оформления правилам компьютерного набора текста (соблюдение объема, шрифтов, интервалов, выравнивания текста на страницах, нумерация страниц и т.д.); аккуратность оформления (отсутствие помарок, работа сброшюрована и т.д.);		
4	Защита владение материалом; правильность ответов на заданные вопросы; способность к изложению собственных мыслей.		
	ИТОГО	**4б**	

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Технический институт (филиал) ФГАОУ ВО «СВФУ» в г. Нерюнгри

КАФЕДРА МАТЕМАТИКИ И ИНФОРМАТИКИ

Реферат

Проверяет теоретические и практические знания студентов по изученным разделам дисциплины.

Темы реферато

1. Угрозы и обеспечение безопасности автоматизированных ИС.
2. Криптография и криптосистемы.
3. Стандарт шифрования данных DES.
4. Алгоритм шифрования данных IDEA.
5. Электронная цифровая подпись.
6. Управление криптографическими ключами.
7. Резервное хранение информации RAID.
8. Биометрические методы защиты информации.
9. Программы с потенциально опасными последствиями.
10. Правовые аспекты информационной безопасности.
11. Методы защиты от копирования данных.

Критерии оценки:

№	Критерий		
1.	Соответствие содержания заявленной теме	1б	2б
2.	Логичность и последовательность в изложении материала	1б	2б
3.	Способность к работе с литературными источниками, Интернет-ресурсами, справочной и энциклопедической литературой	1б	2б
4.	Способность к выполнению практических заданий по заданной тематике	1б	2б
5.	Использование соответствующих компьютерных программ при выполнении практических заданий	1б	2б
6.	Анализ полученных результатов, наличие вывода о проделанной работе	1б	2б
7.	Правильность оформления (наличие всех структурных частей, структурная упорядоченность, ссылки на литературу, цитаты, таблицы, рисунки и т.д.);	1б	2б
8.	Соответствие оформления правилам компьютерного набора текста (соблюдение объема, шрифтов, интервалов, выравнивания текста на страницах, нумерация страниц и т.д.);	1б	2б
9.	Наличие презентационного материала	1б	2б
10.	Правильность ответов на заданные вопросы по заявленной теме	1б	2б
	Итого	10	20

Максимальное количество баллов – 20.

0 баллов – не соответствует критерию, 1 балл – частичное соответствие, 2 балла – полное соответствие.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Технический институт (филиал) ФГАОУ ВО «СВФУ» в г. Нерюнгри

КАФЕДРА МАТЕМАТИКИ И ИНФОРМАТИКИ

Тестирование

1. Что такое несанкционированный доступ?
a) доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
b) удаление не нужной информации
c) вход в систему без согласования с руководителем организации
2. Какой алгоритм шифрования используется в платёжных системах Яндекс.Деньги, Web-money и Cyberplat ?
a) RSA
b) ECDSA
c) DSA
3. Что НЕ относится к угрозам информационной безопасности?
a) преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)
b) классификация информации
c) сбои и отказы оборудования (технических средств)
4. Шифрование с симметричным ключом предполагает, что ... ?
a) используются два разных ключа
b) оба ключа одинаковы
c) используется один ключ
5. Что такое электронная цифровая подпись?
a) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе
b) электронный документ, достоверность которого подтверждена удостоверяющим центром
c) набор цифр персонально закрепленных за пользователями, неразрешенных к использованию любыми другими пользователями
6. К понятию информационной безопасности НЕ относятся:
a) природоохранные мероприятия
b) надежность работы компьютера
c) сохранность ценных данных
7. Что такое политика информационной безопасности организации
a) инструкции администраторам по настройке информационных систем
b) совокупность механизмов компьютерных систем
c) набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию
8. Что такое правовое обеспечение информационной безопасности?
a) нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения
b) широкое использование технических средств защиты информации
c) документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы

9. В политике безопасности НЕ должно быть:
a) разграничения прав доступа к ресурсам
b) разделение обязанностей
c) возможность перехода в небезопасное состояние
10. Какие действия НЕ относятся к реагированию на нарушение режима информационной безопасности организации?
a) судебное рассмотрение
b) выявление нарушителя
c) предупреждение повторных нарушений

Критерии оценки:

Процент выполненных тестовых заданий	**Количество набранных баллов**
91% - 100%	10
81% - 90%	9
71% - 80%	8
61% - 70%	7
51% - 60%	6
<50%	0