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.24 Информационная безопасность

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

Форма обучения: заочная

Нерюнгри 2026

УТВЕРЖДЕНО на заседании
выпускающей кафедры МиИ
«19» марта 2026 г., протокол № 8
Заведующий кафедрой _____ / Самохина В.М.
«19» марта 2026 г.

УТВЕРЖДЕНО на заседании
обеспечивающей кафедры МиИ
«19» марта 2026 г., протокол № 8
Заведующий кафедрой _____ / Самохина В.М.
«19» марта 2026 г.

СОГЛАСОВАНО:
Эксперты[1]:

Зарипова М.Ю., ст. преподаватель кафедры МиИ, ТИ(ф)СВФУ _____
Ф.И.О., должность, организация подпись

Самохина В.М., к.п.н, доцент кафедры МиИ, ТИ(ф)СВФУ _____
Ф.И.О., должность, организация подпись

СОСТАВИТЕЛЬ (И):

Похорукова М.Ю., к.т.н., доцент кафедры МиИ, ТИ(ф)СВФУ _____
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
по дисциплине (модулю) Б1.О.24 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

№	Контролируемые разделы (темы)	Код контролируемой компетенции (или ее части)	Индикаторы компетенций	Требования к уровню усвоения компетенции	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 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;	УК-2.3 Предлагает и обосновывает способы решения поставленных задач УК-2.5 Разрабатывает план на основе имеющихся ресурсов в рамках действующих правовых норм 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	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 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	Лабораторные работы, СРС, реферат, тестирование
2	Компьютерные вирусы и защита от них.				
3	Информационная безопасность вычислительных систем.				
4	Механизмы				

	обеспечения «информационной безопасности».	Способен разрабатывать алгоритмы и программы, пригодные для практического применения.	навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности ОПК-7:1: Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий ОПК-7.2: Умеет 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 ОПК-7.3: Владеет навыками программирования, отладки и тестирования прототипов программно-технических комплексов задач.	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 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	

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.

1-2 балл – демонстрирует, лишь поверхностный уровень выполнения работы, в содержании выполнения задания допущены принципиальные ошибки.

3-4 балла – ставится тогда, когда студент выполнил самостоятельную работу, но дает не точные ответы на заданные вопросы.

5 баллов – ставится тогда, когда студент выполнил самостоятельную работу, показан высокий уровень освоения студентом учебного материала, содержание выполнения задания не содержит ошибок.

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

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:

0 баллов - ставится, если студент не выполнил лабораторную работу.

1-2 балла - ставится, если студент обнаруживает знание и понимание основных положений лабораторной работы, но при выполнении заданий допущены ошибки или задание выполнено на 40-50%; оформление работы выполнено недостаточно последовательно (отсутствуют цель/листинг/результаты/выводы).

3-4 балла - ставится, если студентом при выполнении заданий допущены неточности или задание выполнено на 60-80%; оформление работы выполнено с ошибками (отсутствуют цель/выводы).

5 баллов - 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

Реферат

Реферат проверяет теоретические и практические знания студентов по изученным разделам дисциплины.

Темы рефератов

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

1. Основная масса угроз информационной безопасности приходится
на:

а) Троянские программы
б) Шпионские программы
в) Черви

2. Под какие системы распространение вирусов происходит наиболее
динамично:

а) Windows
б) Mac OS
в) Android

3. Какие угрозы безопасности информации являются
преднамеренными:

а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ

4. Системой криптографической защиты информации является:

а) BFox Pro
б) CAudit Pro

в) Крипто Про
5. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви
6. Под информационной безопасностью понимается:
а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) нет верного ответа
7. Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации
8. Конфиденциальностью называется:
а) защита от несанкционированного доступа к информации
б) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
в) описание процедур
9. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники
10. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
а) уровень доверия, обеспечиваемый механизмом безопасности
б) внедрение управления механизмами безопасности
в) классификацию данных после внедрения механизмов безопасности
11. Основными рисками информационной безопасности являются:
А) Искажение, уменьшение объема, перекодировка информации
Б) Техническое вмешательство, выведение из строя оборудования сети
В) Потеря, искажение, утечка информации
12. Основные типы компьютерных вирусов:
а) Аппаратные, программные, загрузочные.
б) Программные, загрузочные, макровирусы.
в) Файловые, программные, макровирусы.
13. В чем заключается размножение программного вируса?
а) Программа-вирус один раз копируется в теле другой программы.
б) Вирусный код неоднократно копируется в теле другой программы.
в) Программа-вирус один раз выполняется и удаляется из программы.
14. Какие существуют методы реализации антивирусной защиты?
а) Аппаратные и программные.
б) Программные и административные.
в) Только программные.
15. Какие существуют вспомогательные средства защиты?

а) Аппаратные средства.
б) Программные средства.
в) Административные методы и антивирусные программы.
16. Какие программы относятся к антивирусным
а) AVP, DrWeb, Norton AntiVirus.
б) MS-DOS, MS Word, AVP.
в) MS Word, MS Excel, Norton Commander.
17. Деятельность клавиатурных шпионов
а) находясь в оперативной памяти следят за вводимой информацией. Как только пользователь вводит некое кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором
б) находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают своему хозяину
в) находясь в оперативной памяти следят за вводимой пользователем информацией и по команде хозяина производят нужную ему замену одних символов (или групп символов) другими
г) передают хозяину марку и тип используемой пользователем клавиатуры
18. Брандмауэр (firewall) – это программа, …
а) которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил
б) которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл подробную статистику сетевой активности
в) на основе которой строится система кэширования загружаемых веб страниц
г) реализующая простейший антивирус для скриптов и прочих использующихся в Интернет активных элементов
19. Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет
а) трудности с регулярным автоматическим получением новых антивирусных баз
б) невозможность использовать антиспамовую программу в режиме реального времени
в) ложные срабатывания в работе персонального брандмауэра
г) невозможность запуска антивирусной проверки в режиме реального времени
20. Заражение компьютерными вирусами может произойти в процессе ...
а) работы с файлами
б) выключения компьютера
в) форматирования диска
г) печати на принтере
21. Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...
а) Сетевой червь
б) Файловый вирус
в) Загрузочный вирус
г) Макровирус
д) Троян
22. Сетевые черви - это...
а) Вирусы, которые проникнув на компьютер, блокируют работу сети
б) Хакерские утилиты управляющие удаленным доступом компьютера
в) Вредоносные программы, устанавливающие скрытно от пользователя

другие вредоносные программы и утилиты
г) Вирусы, которые внедряются в документы под видом макросов
д) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей
Тест по Информатике. «Информационная безопасность»
«Компьютерные вирусы»: Вариант __
1. Какой вид идентификации и аутентификации получил наибольшее распространение:
а) системы PKI
б) постоянные пароли
в) одноразовые пароли
2. Заключительным этапом построения системы защиты является:
а) сопровождение
б) планирование
в) анализ уязвимых мест
3. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви
4. Защита информации:
а) небольшая программа для выполнения определенной задачи
б) комплекс мероприятий, направленных на обеспечение информационной безопасности
в) процесс разработки структуры базы данных в соответствии с требованиями пользователей
5. Конфиденциальностью называется:
а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
б) описание процедур
в) защита от несанкционированного доступа к информации
6. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники
7. Основные объекты информационной безопасности:
а) Информационные системы, психологическое состояние пользователей
б) Бизнес-ориентированные, коммерческие системы
в) Компьютерные сети, базы данных
8. Эффективная программа безопасности требует сбалансированного применения:
а) контрмер и защитных механизмов
б) процедур безопасности и шифрования
в) технических и нетехнических методов
9. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
а) уровень доверия, обеспечиваемый механизмом безопасности
б) внедрение управления механизмами безопасности
в) классификацию данных после внедрения механизмов безопасности
10. Виды информационной безопасности:
А) Персональная, корпоративная, государственная

Б) Клиентская, серверная, сетевая
В) Локальная, глобальная, смешанная
11. ЭЦП – это:
А) Электронно-цифровой преобразователь
Б) Электронно-цифровая подпись
В) Электронно-цифровой процессор
12. Что такое компьютерный вирус?
а) Прикладная программа.
б) Системная программа.
в) Программа, выполняющая на компьютере несанкционированные действия.
г) База данных.
13. Этапы действия программного вируса:
а) Размножение, вирусная атака.
б) Запись в файл, размножение.
в) Запись в файл, размножение, уничтожение программы.
14. Что называется вирусной атакой?
а) Нарушение работы программы, уничтожение данных, форматирование жесткого диска.
б) Неоднократное копирование кода вируса в код программы.
в) Отключение компьютера в результате попадания вируса.
15. Какие существуют основные средства защиты данных?
а) Резервное копирование наиболее ценных данных.
б) Аппаратные средства.
в) Программные средства.
16. На чем основано действие антивирусной программы?
а) На ожидании начала вирусной атаки.
б) На сравнении программных кодов с известными вирусами.
в) На удалении зараженных файлов.
17. Антиспамовая программа, установленная на домашнем компьютере, служит для …
а) корректной установки и удаления прикладных программ
б) обеспечения регулярной доставки антивирусной программе новых
в) антивирусных баз
г) защиты компьютера от хакерских атак
д) защиты компьютера от нежелательной и/или незапрошенной корреспонденции
18. К классу условно опасных относятся программы …
а) о которых нельзя однозначно сказать, что они вредоносны
б) последствия выполнения которых нельзя предугадать
в) которые можно выполнять только при наличии установленного антивирусного программного обеспечения
г) характеризующиеся способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов. В остальное время они безвредны
19. Антивирусные базы можно обновить на компьютере, не подключенном к Интернет.
а) да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы
б) да, позвонив в службу технической поддержки компании

производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором
в) нет
20. Как обнаруживает вирус программа-ревизор?
А) периодически проверяет все имеющиеся на дисках файлы
Б) контролирует важные функции компьютера и пути возможного заражения
В) отслеживает изменения загрузочных секторов дисков
Г) при открытии файла подсчитывает контрольные суммы и сравнивает их с данными, хранящимися в базе данных
21. Руткит - это...
а) вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю
б) разновидность межсетевого экрана
программа использующая для распространения Рунет (Российскую часть Интернета)
в) программа для скрытого взятия под контроль взломанной системы
г) вредоносная программа, маскирующаяся под макрокоманду
22. К биометрической системе защиты относятся:
а) Антивирусная защита
б) Защита паролем
в) Физическая защита данных
г) Идентификация по отпечаткам пальцев

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