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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.08.01 Информационная безопасность

для программы бакалавриата
по направлению подготовки 01.03.02 «Прикладная математика и информатика»
Направленность (профиль) программы: Системное программирование и компьютерные технологии

Форма обучения: очная

Автор(ы): Похорукова М.Ю., к.т.н., доцент кафедры МиИ, maria.pokhorukova@gmail.com

РЕКОМЕНДОВАНО	ОДОБРЕНО	ПРОВЕРЕНО
Заведующий кафедрой разработчика МиИ _____ / Самохина В.М. протокол № 10 от «05» 05 2023 г.	Заведующий выпускающей кафедрой МиИ _____ / Самохина В.М. протокол № 10 от «05» 05 2023 г.	Нормоконтроль в составе ОПОП пройден Специалист УМО B.Julia / Кравчук К.А. «15» 05 2023 г.
Рекомендовано к утверждению в составе ОПОП Председатель УМС _____ / Ядреева Л.Д. протокол УМС № 10 от «18» 05 2023 г.		Зав. библиотекой _____ / Бочкова ОН «15» 05 2023 г.

Нерюнгри 2023

1. АННОТАЦИЯ
к рабочей программе дисциплины
Б1.В.ДВ.08.01 Информационная безопасность

Трудоемкость 3 з.е.

1.1. Цель освоения и краткое содержание дисциплины

Цель освоения дисциплины: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи дисциплины:

- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартам шифрования;
- изучение математических основ защиты информации; а также методов, средств и инструментов шифрования, применяемых в сфере информационных технологий;
- привитие навыков работы с методами шифрования и криптоанализа.

Краткое содержание дисциплины: Информационная безопасность и уровни ее обеспечения. Компьютерные вирусы и защита от них. Информационная безопасность вычислительных систем. Механизмы обеспечения «информационной безопасности».

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Планируемые результаты освоения программы (код и содержание компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине	Оценочные средства
Профессиональные компетенции	**ПК-3:** способен осуществлять алгоритмизацию поставленных задач и применять выбранные языки программирования для написания программного кода.	ПК-3.1: Способен выполнять формализацию и алгоритмизацию поставленных задач в соответствии с требованиями технического задания ПК-3.2: Способен написать программный код с использованием языков программирования, использовать выбранную среду программирования и средства системы управления базами данных, стандартные библиотеки языка программирования ПК-3.3: Способен применять методы и приемы отладки программного кода, интерпретировать со-	**знать:** основные понятия и уровни обеспечения информационной безопасности; особенности компьютерных вирусов и способы защиты от них; механизмы обеспечения информационной безопасности. **уметь:** написать программный код для решения задач профессиональной деятельности с учетом основных требований информационной безопасности. **владеть:** навыками выбора методов и приемов отладки программного кода на ос-	Лабораторные работы, СРС, контрольная работа

		общения об ошибках, применять современные компиляторы, отладчики программного кода	нове теоретических знаний в области информационной безопасности.	

1.3. Место дисциплины в структуре образовательной программы

Индекс	Наименование дисциплины (модуля), практики	Семестр изучения	Индексы и наименования учебных дисциплин (модулей), практик	
			на которые опирается содержание данной дисциплины (модуля)	для которых содержание данной дисциплины (модуля) выступает опорой
Б1.В.ДВ.08.01	Информационная безопасность	8	Б1.О.22 Проектирование информационных систем Б1.О.07 Основы права Б1.В.02 Разработка и сопровождение программного обеспечения Б2.В.01(П) Производственная II технологическая практика	Б2.В.02(П) Проектно-технологическая практика Б3.01(Д) Выполнение и защита выпускной квалификационной работы

1.4. Язык преподавания: русский.

2. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Выписка из учебного плана (гр. Б-ПМ-23):

Код и название дисциплины по учебному плану	Б1.В.ДВ.08.01 Информационная безопасность	
Курс изучения	4	
Семестр(ы) изучения	8	
Форма промежуточной аттестации (зачет/экзамен)	зачет	
Контрольная работа, семестр выполнения	8	
Трудоемкость (в ЗЕТ)	3 ЗЕТ	
Трудоемкость (в часах) (сумма строк №1,2,3), в т.ч.:	108	
№1. Контактная работа обучающихся с преподавателем (КР), в часах:	Объем аудиторной работы, в часах	В т.ч. с применением ДОТ или ЭО, в часах
Объем работы (в часах) (1.1.+1.2.+1.3.):	38	-
1.1. Занятия лекционного типа (лекции)	12	-
1.2. Занятия семинарского типа, всего, в т.ч.:	-	-
- семинары (практические занятия, коллоквиумы и т.п.)	-	-
- лабораторные работы	24	-
- практикумы	-	-
1.3. КСР (контроль самостоятельной работы, консультации)	2	-
№2. Самостоятельная работа обучающихся (СРС) (в часах)	70	
№3. Количество часов на зачет	-	

3. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

3.1. Распределение часов по разделам и видам учебных занятий

Раздел	Всего часов	Контактная работа, в часах									Часы СРС
		Лекции	из них с применением ЭО и ДОТ	Семинары (практические занятия, коллоквиумы)	из них с применением ЭО и ДОТ	Лабораторные работы	из них с применением ЭО и ДОТ	Практикумы	из них с применением ЭО и ДОТ	КСР (консультации)	
Информационная безопасность и уровни ее обеспечения.	11	2	-	-	-	2	-	-	-	-	2 (ЛР) 5 (Т)
Компьютерные вирусы и защита от них.	15	2	-	-	-	4	-	-	-	-	4 (ЛР) 5 (Т)
Информационная безопасность вычислительных систем.	31	4	-	-	-	8	-	-	-	1	8 (ЛР) 10 (СРС)
Механизмы обеспечения «информационной безопасности».	51	4	-	-	-	10	-	-	-	1	10 (ЛР) 10 (СРС) 16 (К)
Итого	108	12	-	-	-	24	-	-	-	2	70

Примечание: ЛР-подготовка к лабораторным занятиям, К – написание контрольной работы, СРС – выполнение самостоятельной работы, Т - тестирование.

3.2. Содержание тем программы дисциплины

Тема 1. Информационная безопасность и уровни ее обеспечения.

Понятие «информационная безопасность». Составляющие информационной безопасности. Система формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ. Стандарты информационной безопасности. Административный уровень обеспечения информационной безопасности. Классификация угроз «информационной безопасности».

Тема 2. Компьютерные вирусы и защита от них.

Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристика «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.

Тема 3. Информационная безопасность вычислительных систем.

Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые

удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.

Тема 4. Механизмы обеспечения «информационной безопасности».

Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).

3.3. Формы и методы проведения занятий, применяемые учебные технологии

В процессе преподавания дисциплины используются традиционные технологии, наряду с активными и интерактивными технологиями.

Активные/интерактивные технологии, используемые в образовательном процессе

Раздел	Семестр	Используемые активные/интерактивные образовательные технологии	Количество часов
Информационная безопасность и уровни ее обеспечения.		Лекция-визуализация, презентация, проблемный метод, тестирование	
Компьютерные вирусы и защита от них.		Лекция-визуализация, презентация, проблемный метод, тестирование	
Информационная безопасность вычислительных систем.		Лекция-визуализация, презентация, проблемный метод, тестирование	
Механизмы обеспечения «информационной безопасности».		Лекция-визуализация, презентация, проблемный метод, тестирование	
		Итого:	

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Содержание СРС

№	Наименование раздела (темы) дисциплины	Вид СРС	Трудоемкость (в часах)	Формы и методы контроля
8 семестр				
1	Информационная безопасность и уровни ее обеспечения.	Подготовка к лабораторным занятиям Тестирование	2 (ЛР) 5 (Т)	Выполнение заданий на практических занятиях Выполнение теста
2	Компьютерные вирусы и защита от них.	Подготовка к лабораторным занятиям Тестирование	4 (ЛР) 5 (Т)	Выполнение заданий на практических занятиях Выполнение теста
3	Информационная безопасность вычислительных систем.	Подготовка к лабораторным занятиям Самостоятельная работа	8 (ЛР) 10 (СРС)	Выполнение заданий на практических занятиях Выполнение самостоятельной работы
4	Механизмы обеспечения	Подготовка к лабораторным занятиям	10 (ЛР) 10 (СРС)	Выполнение заданий на практических

	«информационной безопасности».	Самостоятельная работа Контрольная работа	16 (К)	занятиях Выполнение самостоятельной работы Выполнение контрольной работы
	Всего часов		70	

Работа на лабораторном занятии

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

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 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).

Самостоятельная работа

Тема 1. Принципы засекречивания сведений и отнесения их к государственной тайне
Тема 2. Порядок отнесения информации к коммерческой тайне и способы ее получения
0 баллов – самостоятельная работа не выполнена.
1 балл – демонстрирует, лишь поверхностный уровень выполнения работы, в содержании выполнения задания допущены принципиальные ошибки.
2 балла – ставится тогда, когда студент выполнил самостоятельную работу, но дает не точные ответы на заданные вопросы.
3 балла – ставится тогда, когда студент выполнил самостоятельную работу, показан высокий уровень освоения студентом учебного материала, содержание выполнения задания не содержит ошибок.

Тестирование

Образцы тестовых заданий:

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, Webmoney 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

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

Контрольная работа

Контрольная работа поверяет теоретические и практические знания студентов по изученным разделам дисциплины.

Образец контрольных заданий

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

Соответствие критерию: полностью соответствует – 2 балла; частично – 1 балл; не соответствует – 0 баллов.

5. Методические указания для обучающихся по освоению дисциплины

Методические указания для помощи обучающимся в успешном освоении дисциплины в соответствии с запланированными видами учебной и самостоятельной работы обучающихся размещены в СДО Moodle http://moodle.nfygu.ru/course/view.php?id=13348

Рейтинговый регламент по дисциплине:

№	**Вид выполняемой учебной работы (контролирующие материалы)**		Количество баллов (min)	Количество баллов (max)	*Примечание*
	Испытания / Формы СРС	*Время, час*			
	Подготовка к лабораторным заданиям	12ЛР*2б=24б	12ЛР*2б=24б	12ЛР*3б=36б	Теоретическое изучение материла, решение задач
2	Выполнение контрольной работы	16	10	20	в письменном виде, по вариантам
3	Выполнение самостоятельной работы	10СРС*2=20	8СРС*2=16	8СРС*3=24	в письменном виде, по вариантам
4	Тестирование	2Т*5=10	2Т*5=10	2Т*10=20	
	Итого:	70	60б	100б	

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Показатели, критерии и шкала оценивания

Коды оцениваемых компетенций	Показатель оценивания (по п.1.2.РПД)	Уровни освоения	Критерии оценивания (дескрипторы)	Оценка
ПК-3: способен осуществлять алгоритмизацию поставленных задач и применять выбранные языки программирования для написания программного	**знать:** основные понятия и уровни обеспечения информационной безопасности; особенности компьютерных вирусов и способы защиты от них; механизмы	Освоено	Обучаемый показал полное знание учебно-программного материала, успешно выполнил предусмотренные рабочей программой задания, показал систематический характер знаний по дисциплине и спосо-	Зачтено

кода	обеспечения информационной безопасности. **уметь:** написать программный код для решения задач профессиональной деятельности с учетом основных требований информационной безопасности. **владеть:** навыками выбора методов и приемов отладки программного кода на основе теоретических знаний в области информационной безопасности.		бен к их самостоятельному пополнению и обновлению в ходе профессиональной деятельности.	
		Не освоено	Обучаемый не знает большей части основного содержания дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания при решении типовых практических задач в области профессиональной деятельности.	Не зачтено

6.2. Методические материалы, определяющие процедуры оценивания

Характеристики процедуры	
Вид процедуры	зачет
Цель процедуры	выявить степень сформированности компетенции ПК-3
Локальные акты вуза, регламентирующие проведение процедуры	Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся СВФУ, версия 3.0, утверждено ректором СВФУ 19.02.2019 г. Положение о балльно-рейтинговой системе в СВФУ, версия 4.0, утверждено 21.02.2018 г.
Субъекты, на которых направлена процедура	студенты 4 курса бакалавриата
Период проведения процедуры	летняя экзаменационная сессия
Требования к помещениям и материально-техническим средствам	-
Требования к банку оценочных средств	-
Описание проведения процедуры	В соответствии с Положением о балльно-рейтинговой системе в СВФУ (утвержденный приказом ректором СВФУ от 21.02.2018 г.), зачет «ставится при наборе 60 баллов». Таким образом, процедура зачета не предусмотрена.
Шкалы оценивания результатов	-
Результаты процедуры	В результате сдачи всех заданий для СРС студенту необходимо набрать 60 баллов, чтобы получить зачет.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№	Автор, название, место издания, издательство, год издания учебной литературы, вид и характеристика иных информационных ресурсов	Наличие грифа, вид грифа	Библиотека ТИ (ф) СВФУ, кол-во экземпляров	Электронные издания: точка доступа к ресурсу (наименование ЭБС, ЭБ СВФУ)	Количество студентов
Основная литература[1]					
1	Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студ. вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 2-е изд., стер. – Москва: Академия, 2007. – 331 с.: ил. – (Высшее профессиональное образование). – Библиогр.: с. 327-328. – ISBN 978-5-7695-4148-3 : 208?67	Гриф МО РФ	20		18
2	Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ;			http://biblioclub.ru/index.php?page=book&id=428605	18
Дополнительная литература					
3	Ковалев, Д. В. Информационная безопасность : учебное пособие : [16+] / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.			https://biblioclub.ru/index.php?page=book&id=493175	18
4	Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.			https://biblioclub.ru/index.php?page=book&id=576726	18

[1] Рекомендуется указывать не более 3-5 источников (с грифами).

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее сеть-Интернет), необходимых для освоения дисциплины

Научная электронная библиотека https://www.elibrary.ru/
Университетская библиотека ONLINE - http://biblioclub.ru/

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Виды учебных занятий*	Наименование аудиторий, кабинетов, лабораторий и пр.	Перечень оборудования
1.	Лекционные занятия	Мультимедийный кабинет	интерактивная доска, ноутбук, мультимедийный проектор
2.	Подготовка к СРС	Кабинет для СРС № 402	Компьютер, доступ к интернет
3.	Лабораторные занятия	Кабинет № 201, 207	Компьютеры, доступ к интернет

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

10.1. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

- использование на занятиях электронных изданий (чтение лекций с использованием слайд-презентаций, электронного учебного пособия), видео- и аудиоматериалов (через Интернет);
- организация взаимодействия с обучающимися посредством электронной почты и СДО Moodle.

10.2. Перечень программного обеспечения

- MS Office, MS Visual Studio.

10.3. Перечень информационных справочных систем

-

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.ДВ.08.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебный год	Внесенные изменения	Преподаватель (ФИО)	Протокол заседания выпускающей кафедры(дата, номер), ФИО зав. кафедрой, подпись

В таблице указывается только характер изменений (например, изменение темы, списка источников по теме или темам, средств промежуточного контроля) с указанием пунктов рабочей программы. Само содержание изменений оформляется приложением по сквозной нумерации.