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.О.26 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

для программы бакалавриата
по направлению подготовки 09.03.03 «Прикладная информатика»
Направленность программы: Прикладная информатика в менеджменте
Форма обучения: заочная

Автор: Юданова В.В., ст. преподаватель кафедры МиИ, e-mail: udanov_sb@mail.ru

РЕКОМЕНДОВАНО Представитель кафедры МиИ _____/Е.О. Агабабян И.о. заведующего кафедрой МиИ _____/В.М. Самохина протокол № 10 от «14» 05 2021г.	ОДОБРЕНО Представитель кафедры МиИ _____/Е.О. Агабабян И.о. заведующего кафедрой МиИ _____/В.М. Самохина протокол № 10 от «14» 06 2021г.	ПРОВЕРЕНО Нормоконтроль в составе ОПОП пройден Специалист УМО _____/_____ «24» 05 2021 г.
Рекомендовано к утверждению в составе ОПОП Председатель УМС _____/ Л.А. Яковлева протокол УМС № 8 от «27» мая 2021 г.		Зав. библиотекой _____/ Булгалова Н.С. «24» 05 2021 г.

Нерюнгри 2021

1. АННОТАЦИЯ
к рабочей программе дисциплины
Б1.О.26 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

Планируемые результаты освоения программы (содержание и коды компетенций)	Наименование индикатора достижения компетенций	Планируемые результаты обучения по дисциплине
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 ОПК-7: Способен разрабатывать алгоритмы и программы,	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 навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом тре-	**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 основе теоретических знаний в области информационной безопасности.

пригодные для практического применения	бований 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	

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.О.26	Информационная безопасность	9	Б1.О.18 Информатика и программирование Б1.О.19 Языки и методы программирования Б1.В.03 Объектно-ориентированное программирование	Б2.В.02(П) Производственная 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. БА-ПИ-21(5)):

Код и название дисциплины по учебному плану	Б1.О.26 Информационная безопасность	
Курс изучения	5	
Семестр(ы) изучения	9	
Форма промежуточной аттестации (зачет/экзамен)	зачет	
Контрольная работа, семестр выполнения (по плану есть)	9	
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[1], в часах
Объем работы (в часах) (1.1.+1.2.+1.3.):	18	-
1.1. Занятия лекционного типа (лекции)	6	-
1.2. Занятия семинарского типа, всего, в т.ч.:	-	-
- семинары (практические занятия, коллоквиумы и т.п.)	-	-
- лабораторные работы	8	-
- практикумы	-	-
1.3. КСР (контроль самостоятельной работы, консультации)	4	-
№2. Самостоятельная работа обучающихся (СРС) (в часах)	86	
№3. Количество часов на зачет	4	

[1]Указывается, если в аннотации образовательной программы по позиции «Сведения о применении дистанционных технологий и электронного обучения» указан ответ «да».

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.	19	1	-	-	-	2	-	-	-	1	6 (ЛР) 4(СРС) 5(Т)
Компьютерные вирусы и защита от них.	25	1	-	-	-	2	-	-	-	1	12 (ЛР) 4(СРС) 5(Т)
Информационная безопасность вычислительных систем.	26	2	-	-	-	2	-	-	-	1	12 (ЛР) 4(СРС) 5(Т)
Механизмы обеспечения «информационной безопасности».	34	2	-	-	-	2	-	-	-	1	12 (ЛР) 17(КР)
Зачет	4										
Итого	108	6	-	-	-	8	-	-	-	4	86+4

Примечание: ЛР-подготовка к лабораторным занятиям, СРС – выполнение самостоятельной работы.

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.

Раздел	Семестр	Используемые активные/интерактивные образовательные технологии	Количество часов
Информационная безопасность и уровни ее обеспечения.		Лекция-визуализация, презентация, проблемный метод	
Компьютерные вирусы и защита от них.		Дискуссия, проблемный метод, тестирование	2
Информационная безопасность вычислительных систем.		Дискуссия, проблемный метод, тестирование	
		Итого:	

Учебные технологии, используемые в образовательном процессе:

традиционное обучение (классно-урочная система),

*проблемное обучение (*Case-study (анализ конкретных ситуаций, ситуационный анализ*)* под руководством преподавателя формулируется проблемный вопрос, создаются проблемные ситуации, в результате чего активизируется самостоятельная деятельность студентов, происходит овладение профессиональными компетенциями.

дискуссионные методы (диалог; групповая дискуссия; разбор ситуаций из практики) могут быть реализованы в виде диалога участников или групп участников, групповой дискуссии, анализа конкретной ситуации или других.

4. Перечень учебно-методического обеспечения для самостоятельной работы[2] обучающихся по дисциплине

Содержание СРС

№	Наименование раздела (темы) дисциплины	Вид СРС	Трудоемкость (в часах)	Формы и методы контроля
9 семестр				
1	Информационная безопасность и уровни ее обеспечения.	Подготовка к лабораторным занятиям Самостоятельная работа Тестирование	6 (ЛР) 4(СРС) 5(Т)	Выполнение практических заданий Выполнение самостоятельной работы Выполнение теста (внеауд. СРС)
2	Компьютерные вирусы и защита от них.	Подготовка к лабораторным занятиям Самостоятельная работа	12 (ЛР) 4(СРС)	Выполнение практических заданий Выполнение

[2] Самостоятельная работа студента может быть внеаудиторной (выполняется студентом самостоятельно без участия преподавателя – например, подготовка конспектов, выполнение письменных работ и др.) и аудиторной (выполняется студентом в аудитории самостоятельно под руководством преподавателя – например, лабораторная или практическая работа).

		Тестирование	5(Т)	самостоятельной работы Выполнение теста (внеауд. СРС)
3	Информационная безопасность вычислительных систем.	Подготовка к лабораторным занятиям Самостоятельная работа Тестирование	12 (ЛР) 4(СРС) 5(Т)	Выполнение практических заданий Выполнение самостоятельной работы Выполнение теста (внеауд. СРС)
4	Механизмы обеспечения «информационной безопасности».	Подготовка к лабораторным занятиям Контрольная работа	12 (ЛР) 17(КР)	Выполнение практических заданий Выполнение контрольной работы
	Всего часов		86+4	

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

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 или все задания выполнены неправильно.
1 балл – в содержании выполнения задания допущены принципиальные ошибки, правильных ответов на контрольные вопросы менее 30%.
2 балла – в содержании выполнения задания допущены ошибки, правильных ответов на контрольные вопросы менее 70%.
3 балла – ставится тогда, когда студент полностью и правильно выполнил самостоятельную работу, ошибок вы выполнении нет.

Контрольная работа

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

Темы контрольных работ

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
2.	Логичность и последовательность в изложении материала	1б
3.	Способность к работе с литературными источниками, Интернет-ресурсами, справочной и энциклопедической литературой	1б
4.	Способность к выполнению практических заданий по заданной тематике	1б
5.	Использование соответствующих компьютерных программ при выполнении практических заданий	1б
6.	Анализ полученных результатов, наличие вывода о проделанной работе	1б
7.	Правильность оформления (наличие всех структурных частей, структурная упорядоченность, ссылки на литературу, цитаты, таблицы, рисунки и т.д.);	1б
8.	Соответствие оформления правилам компьютерного набора текста (соблюдение объема, шрифтов, интервалов, выравнивания текста на страницах, нумерация страниц и т.д.);	1б
9.	Наличие презентационного материала	1б
10.	Правильность ответов на заданные вопросы по заявленной теме	1б
	Итого	10

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=11098

Рейтинговый регламент по дисциплине:

№	**Вид выполняемой учебной работы (контролирующие материалы)**		Количество баллов (min)	Количество баллов (max)	*Примечание*
	Испытания / Формы СРС	*Время, час*			
1	Подготовка к лабораторным заданиям	14ЛР*3=42	14ЛР*2=28	14ЛР*3=42	Теоретическое изучение материла, решение задач
2	Выполнение контрольной работы	17	5	10	Выполнение контрольной работы по выбранной теме
3	Выполнение самостоятельной работы	6СРС*2=12	6СРС*2=12	6СРС*3=18	в письменном виде, по вариантам
4	Тестирование	3Т*5=15	3Т*5=15	3Т*10=20	Выполнение теста
	Итого:	86+4	60	100	

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
УК-2 ОПК-3 ОПК-7	**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 основе теоретических	Освоено	Обучаемый показал полное знание учебно-программного материала, успешно выполнил предусмотренные рабочей программой задания, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе профессиональной деятельности.	Зачтено
		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 про-	Не зачтено

	знаний в области информационной безопасности.		фессиональной деятельности.	

6.2. Методические материалы, определяющие процедуры оценивания

Характеристики процедуры	
Вид процедуры	зачет
Цель процедуры	выявить степень сформированности компетенции УК-2, ОПК-3,7
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[3]

№	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[4]					
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		17
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	17
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	17
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	17

[3] Для удобства проведения ежегодного обновления перечня основной и дополнительной учебной литературы рекомендуется размещать раздел 7 на отдельном листе,с обязательной отметкой в Учебной библиотеке.
[4] 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

Свободно распространяемое ПО: Open Office

10.3. Перечень информационных справочных систем

-

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.О.26 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.