

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Рукович Александр Владимирович

Должность: Директор

Дата подписания: 16.10.2018 16:13:03

Уникальный программный ключ:

f45eb7c44954caac05ea7d4f32eb8d7d6b3cb96ae6d9b4bda094afddaffb705f

Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

СЕВЕРНО-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.09.02 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

для программы бакалавриата

по направлению подготовки

09.03.03 Прикладная информатика

Направленность программы: Прикладная информатика в менеджменте

Форма обучения: очная

Автор: Похорукова М.Ю., к.т.н., доцент кафедры математики и информатики, e-mail: maria.pokhorukova@gmail.com

РЕКОМЕНДОВАНО Представитель кафедры Мии <i>Ашмарина М.В.</i> Заведующий кафедрой Мии <i>Самохина В.М.</i> протокол № 10 от «20» апреля 2018 г.	ОДОБРЕНО Представитель кафедры Мии <i>Ашмарина М.В.</i> Заведующий кафедрой Мии <i>Самохина В.М.</i> протокол № 10 от «20» апреля 2018 г.	ПРОВЕРЕНО Нормоконтроль в составе ОПОП пройден Специалист УМО <i>Санникова С.Р.</i> «23» 04 2018 г.
Рекомендовано к утверждению в составе ОП Председатель УМС <i>Л.А. Яковлева</i> протокол УМС № <i>04</i> от «20» 04 2018 г.		Зав. библиотекой <i>Гошанская И.С.</i> «10» 04 2018 г.

Нерюнгри 2018

1. АННОТАЦИЯ
к рабочей программе дисциплины
Б1.В.ДВ.09.02 Методы и средства защиты компьютерной информации
Трудоемкость 3 з.е.

1.1. Цель освоения и краткое содержание дисциплины

Цель освоения дисциплины: формирование профессиональной компетентности системных программистов в области применения современных методов и средств защиты информации при разработке систем автоматизированного проектирования и при работе с системами автоматизации конструкторского и технологического проектирования приборов различного назначения.

Краткое содержание дисциплины: Постановка задачи по предотвращению угроз информационной безопасности. Меры по защите баз данных.

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

Планируемые результаты освоения программы (содержание и коды компетенций)	Планируемые результаты обучения по дисциплине
<p>ОПК-1: владеет способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий.</p> <p>ПК-24: владеет способностью готовить обзоры научной литературы и электронных информационно-образовательных ресурсов для профессиональной деятельности.</p>	<p>Знать: основные требования информационной безопасности; методы целенаправленного поиска информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет") и в других источниках.</p> <p>Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий; осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно телекоммуникационной сети "Интернет" (далее – сеть "Интернет") и в других источниках.</p> <p>Владеть: (методиками) решений стандартных задач профессиональной деятельности; практическими навыками использования коммуникационных технологий; навыками целенаправленного поиска информации о новейших научных и технологических достижениях в информационно телекоммуникационной сети "Интернет" (далее – сеть "Интернет") и в других источниках.</p>

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.09.02	Методы и средства защиты компьютерной информации	7	Б1.Б.12 Информатика и программирование Б1.Б.13 Языки программирования и методы трансляции Б1.В.03 Объектно-ориентированное программирование	Б2.В.04(Пд) Производственная преддипломная практика для выполнения выпускной квалификационной работы Б3.Б.01(Д) Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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-18):

Код и название дисциплины по учебному плану	Б1.В.ДВ.09.02 Методы и средства защиты компьютерной информации	
Курс изучения	4	
Семестр(ы) изучения	7	
Форма промежуточной аттестации (зачет/экзамен)	зачет	
Реферат	7	
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.):	45	-
1.1. Занятия лекционного типа (лекции)	14	-
1.2. Занятия семинарского типа, всего, в т.ч.:	-	-
- семинары (практические занятия, коллоквиумы и т.п.)	-	-
- лабораторные работы	28	-
- практикумы	-	-
1.3. КСР (контроль самостоятельной работы, консультации)	3	-
№2. Самостоятельная работа обучающихся (СРС) (в часах)	63	
№3. Количество часов на зачет	-	

¹Указывается, 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)	
Основные понятия информационной безопасности и защиты информации	12	2	-	-	-	4	-	-	-	-	4 (ЛР) 2 (СРС)
Криптография и криптосистемы.	25	4	-	-	-	8	-	-	-	1	8 (ЛР) 4 (СРС)
Электронная цифровая подпись.	25	4	-	-	-	8	-	-	-	1	8 (ЛР) 4(СРС)
Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.	46	4	-	-	-	8	-	-	-	1	8 (ЛР) 4 (СРС) 21(Р)
Итого	108	14	-	-	-	28	-	-	-	3	63

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

3.2. Содержание тем программы дисциплины

Тема 1. Основные понятия информационной безопасности и защиты информации.

Информация. Основные понятия и определения информационной безопасности и защиты информации. Закон о защите информации. Защита информации от утечки. Защита информации от несанкционированного доступа.

Тема 2. Криптография и криптосистемы.

Криптография и криптосистемы. Хеш-функции. Шифры. Аутентификация. Понятие стойкости криптографических алгоритмов. Схема шифрованной связи. Шифрование. Симметричное и несимметричное шифрование. Способы шифрования. Шифры гаммирования и генераторы псевдослучайной последовательности.

Тема 3. Электронная цифровая подпись.

Основные положения. Атаки на электронную цифровую подпись. Правовое регулирование электронной цифровой подписи в России. Средства работы с электронной цифровой подписью.

Тема 4. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.

Система биометрической аутентификации пользователя. Дактилоскопические системы аутентификации. Система аутентификации по форме ладони. Электронные идентификаторы. Идентификаторы на базе контактных смарткарт. Бесконтактные идентификаторы RFID. Методы обнаружения сетевых атак.

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
Основные понятия информационной безопасности и защиты информации		Лекция-визуализация, презентация, проблемный метод	2
Криптография и криптосистемы.		Дискуссия, проблемный метод, тестирование	
Электронная цифровая подпись.		Дискуссия, проблемный метод, тестирование	
Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.		Дискуссия, проблемный метод, тестирование	
Итого:			

4. Перечень учебно-методического обеспечения для самостоятельной работы² обучающихся по дисциплине Содержание СРС

№	Наименование раздела (темы) дисциплины	Вид СРС	Трудоемкость (в часах)	Формы и методы контроля
7 семестр				
1	Основные понятия информационной безопасности и защиты информации	Подготовка к лабораторным занятиям Самостоятельная работа	4 2	Выполнение практических заданий Выполнение самостоятельной работы
2	Криптография и криптосистемы.	Подготовка к лабораторным занятиям Самостоятельная работа	8 4	Выполнение практических заданий Выполнение самостоятельной работы
3	Электронная цифровая подпись.	Подготовка к лабораторным занятиям Самостоятельная работа	8 4	Выполнение практических заданий Выполнение самостоятельной работы
4	Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.	Подготовка к лабораторным занятиям Самостоятельная работа Реферат	8 4 21	Выполнение практических заданий Выполнение самостоятельной работы Написание реферата (по вариантам)
	Всего часов		63	

Работа на лабораторном занятии

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).

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

Темы лабораторных работ

Тема 1. Основные понятия информационной безопасности и защиты информации

Тема 2. Криптография и криптосистемы.

Тема 3. Электронная цифровая подпись.

Тема 4. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.

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

СРС 1. Понятие «информационная безопасность». Составляющие информационной безопасности.

СРС 2. Классификация угроз «информационной безопасности».

СРС 3. Принципы засекречивания сведений и отнесения их к государственной тайне

СРС 4. Криптография и криптосистемы.

СРС 5. Способы шифрования.

СРС 6. Правовое регулирование электронной цифровой подписи в России.

СРС 7. Система биометрической аутентификации пользователя.

СРС 8. Методы обнаружения сетевых атак.

Критерии оценки:

№	Критерий	16	06
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	46	

Соответствие критерию: соответствует (выполнено, реализовано) –1 балл; не соответствует – 0 баллов.

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	36	26	16	06
1	Актуальность: конкретность и достижимость целей и задач; соответствие разработки современным подходам к рассматриваемой проблеме;				
2	Актуальность: соответствие целей и задач ожидаемым результатам; четкость формулировки ожидаемых результатов				
3	Содержание теоретического материала: соответствие содержания заявленной теме; отсутствие в тексте отступлений от темы;				
4	Содержание теоретического материала: логичность и последовательность в изложении материала; способность к работе с литературными источниками, Интернет-ресурсами, справочной и энциклопедической литературой				
5	Содержание практической части: способность к анализу и обобщению информационного материала; способность к проведению расчетов, согласно заданию;				
6	Содержание практической части: использование компьютерных программ при выполнении задания; анализ полученных расчетных характеристик, обоснованность выводов				
7	Оформление правильность оформления (наличие всех структурных частей, структурная упорядоченность, ссылки на литературу, цитаты, таблицы, рисунки и т.д.);				
8	Оформление соответствие оформления правилам компьютерного набора текста (соблюдение объема, шрифтов, интервалов, выравнивания текста на страницах, нумерация страниц и т.д.);				
9	Защита владение материалом; способность к изложению собственных мыслей.				
10	Защита правильность ответов на заданные вопросы;				
	Итого	306			

Соответствие критерию: наиболее полно- 3 балла, достаточно полно – 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=9676>

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*2=28	14ЛР*2=28	14ЛР*3=42	Теоретическое изучение материала, решение задач
2	Написание реферата	21	18	30	Написание реферата по выбранной теме
3	Выполнение самостоятельной работы	7СРС*2=14	7СРС*2=14	7СРС*4=28	в письменном виде, по вариантам
	Итого:	63	60	100	

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

6.1. Показатели, критерии и шкала оценивания

В соответствии с п. 5.13 Положения 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.

Коды оцениваемых компетенций	Показатель оценивания (по п.1.2.РПД)	Уровни освоения	Критерии оценивания (дескрипторы)	Оценка
ОПК-1: владеет способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий. ПК-24: владеет способностью готовить обзоры научной литературы и электронных информационно-образовательных ресурсов для профессиональной деятельности.	Знать: основные требования информационной безопасности; методы целенаправленного поиска информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет") и в других источниках. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий; осуществлять целенаправленный поиск информации о новейших научных и технологических	Освоено	Обучаемый знает основные требования информационной безопасности; методы целенаправленного поиска информации о методах и средствах защиты компьютерной информации (ЭЦП, биометрические методы). Умеет решать стандартные задачи по обеспечению защиты информации с применением информационно-коммуникационных технологий; осуществлять целенаправленный поиск информации о методах защиты компьютерной информации и в других источниках. Владеет навыками обеспечения информационной безопасности.	зачтено
		Не освоены	Отсутствие знаний об основных требованиях информационной безопасности. Неспособность обучающегося самостоятельно осуществлять поиск информации о методах защиты компьютерной информации для решения задач обеспечения информационной	незачтено

	<p>достижения в информационно телекоммуникационной сети "Интернет" (далее – сеть "Интернет") и в других источниках. Владеть: (методиками) решений стандартных задач профессиональной деятельности; практическими навыками использования коммуникационных технологий; навыками целенаправленного поиска информации о новейших научных и технологических достижениях в информационно телекоммуникационной сети "Интернет" (далее – сеть "Интернет") и в других источниках.</p>		<p>безопасности. Отсутствие самостоятельности в применении умения к использованию знаний о средствах и методах защиты компьютерной информации в профессиональной деятельности и неспособность самостоятельно проявить навык обеспечения информационной безопасности.</p>	
--	---	--	--	--

6.2. Методические материалы, определяющие процедуры оценивания

Характеристики процедуры	
Вид процедуры	зачет
Цель процедуры	выявить степень сформированности компетенции ОПК-1, ПК-24
Локальные акты вуза, регламентирующие проведение процедуры	<p>Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся СВФУ, версия 2.0, утверждено ректором СВФУ 15.03.2016 г.</p> <p><u>Положение о балльно-рейтинговой системе в СВФУ, версия 4.0, утверждено 21.02.2018 г.</u></p>
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 дисциплины³

№	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 литература⁴					
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. ; То же [Электронный ресурс].			URL: //biblioclub.ru/index.php?page=book&id=428605	17
Дополнительная литература					
1	Башлы, П.Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. - М. : Евразийский открытый институт, 2011. - 375 с. - ISBN 978-5-374-00301-7 ; То же [Электронный ресурс]			URL: //biblioclub.ru/index.php?page=book&id=90539	17
2	Сычев, Ю.Н. Основы информационной безопасности : учебно-практическое пособие / Ю.Н. Сычев. - М. : Евразийский открытый институт, 2010. - 328 с. - ISBN 978-5-374-00381-9 ; То же [Электронный ресурс]			URL: //biblioclub.ru/index.php?page=book&id=90790	17
3	Информационная безопасность			http://www.its.ec.ru/main.php	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

1. Научная электронная библиотека, <http://elibrary.ru/>
2. Университетская библиотека ONLINE - <http://biblioclub.ru/>

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

	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 Visual Studio, MS Office, OpenOffice.

10.3. Перечень информационных справочных систем

Научная электронная библиотека, <http://elibrary.ru/>

