

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Рукович Александр Владимирович

Должность: Директор

Дата подписания: 01.03.2019

Уникальный программный ключ:

f45eb7c44954caac05ea7d4f32eb8d7d6b3cb96ae6d9b4bda094afddaffb705f

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.08.02 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

для программы бакалавриата

по направлению подготовки

01.03.02 Прикладная математика и информатика

Направленность программы: Системное программирование и компьютерные технологии

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 <u>И.В. Чумаченко</u> Заведующий кафедрой МиИ <u>В.М. Самохина</u> протокол № 10 от «07» мая 2019 г.	ОДОБРЕНО Представитель кафедры МиИ <u>И.В. Чумаченко</u> Заведующий кафедрой МиИ <u>В.М. Самохина</u> протокол № 10 от «07» мая 2019 г.	ПРОВЕРЕНО Нормоконтроль в составе ОПОП пройден Специалист УМО <u>С.П. Санникова</u> « 16 » 05 2019 г.
Рекомендовано к утверждению в составе ОП Председатель УМО протокол УМО № 08 от « 08 » 05 2019 г.	/ Л.А. Яковлева 05 2019 г.	Зав. библиотекой <u>О.В. Сокольникова</u> « 13 » 05 2019 г.

Нерюнгри 2019

1. АННОТАЦИЯ
к рабочей программе дисциплины
Б1.В.ДВ.08.02 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)	Наименование индикатора достижения компетенций	Планируемые результаты обучения по дисциплине
ПК-3: способен осуществлять алгоритмизацию поставленных задач и применять выбранные языки программирования для написания программного кода	<p>ПК-3.1: Способен выполнять формализацию и алгоритмизацию поставленных задач в соответствии с требованиями технического задания</p> <p>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</p> <p>ПК-3.3: Способен применять методы и приемы отладки программного кода, интерпретировать сообщения об ошибках, применять современные компиляторы, отладчики программного кода</p>	<p>знать: основные требования информационной безопасности.</p> <p>уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий.</p> <p>владеть: методиками решений стандартных задач профессиональной деятельности, практическими навыками использования коммуникационных технологий.</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.08.02	Методы и средства защиты компьютерной информации	8	Б1.О.23 Проектирование информационных систем	Б2.В.02(Пд) Проектно-технологическая практика (стационарная)

			Б1.О.07 Основы права Б1.В.02 Разработка и сопровождение программного обеспечения Б2.В.01(П) II Технологическая практика (стационарная)	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-ПМ-19):

Код и название дисциплины по учебному плану	Б1.В.ДВ.08.02 Методы и средства защиты компьютерной информации	
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 ¹ , в часах
Объем работы (в часах) (1.1.+1.2.+1.3.):	62	-
1.1. Занятия лекционного типа (лекции)	24	-
1.2. Занятия семинарского типа, всего, в т.ч.:	-	-
- семинары (практические занятия, коллоквиумы и т.п.)	-	-
- лабораторные работы	36	-
- практикумы	-	-
1.3. КСР (контроль самостоятельной работы, консультации)	2	-
№2. Самостоятельная работа обучающихся (СРС) (в часах)	46	
№3. Количество часов на экзамен (при наличии экзамена в учебном плане)	-	

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	Лабораторные занятия	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)	
8 семестр											
Основные понятия информационной безопасности и защиты информации	29,5	8	-	10	-	-	-	-	-	-	7,5 (ЛБ) 4 (СРС)
Криптография и криптосистемы.	34	8	-	12	-	-	-	-	-	1	9 (ЛБ) 4 (СРС)
Электронная цифровая подпись. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.	44,5	8	-	14	-	-	-	-	-	1	10,5 (ЛБ) 11 (К)
Итого:	108	24	-	36	-	-	-	-	-	2	46

Примечание: ЛБ - подготовка к лабораторным занятиям, СРС – выполнение самостоятельных работ, К – написание контрольной 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. 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. Электронная цифровая подпись

3.3. Формы и методы проведения занятий, применяемые учебные технологии

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

Учебные технологии, используемые в образовательном процессе

Раздел дисциплины	Семестр	Используемые активные/интерактивные образовательные технологии	Количество часов
Основные понятия информационной безопасности и защиты информации	8	Лекция-визуализация, презентация, проблемное обучение	4
Криптография и криптосистемы.		Дискуссионные методы, case-study (анализ конкретных, практических ситуаций).	4
Электронная цифровая подпись. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.		Дискуссионные методы, case-study (анализ конкретных, практических ситуаций).	6
Итого:			14

При *проблемном обучении* под руководством преподавателя формулируется проблемный вопрос, создаются проблемные ситуации, в результате чего активизируется самостоятельная деятельность студентов, происходит овладение профессиональными компетенциями.

Дискуссионные методы могут быть реализованы в виде диалога участников или групп участников, групповой дискуссии, анализа конкретной ситуации или других.

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
8 семестр				
1	Основные понятия информационной безопасности и защиты информации	Подготовка к лабораторным занятиям СРС	7,5ч 4ч	Анализ теоретического материала, выполнение практических заданий. Выполнение задания СРС (ауд. СРС)
2	Криптография и криптосистемы.	Подготовка к лабораторным занятиям СРС	9ч 4ч	Анализ теоретического материала, выполнение практических заданий. Выполнение задания СРС (ауд. СРС)
3	Электронная цифровая подпись.	Подготовка к лабораторным	10,5ч	Анализ теоретического материала, 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).

Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.	занятиям Выполнение контрольной работы	11ч	практических заданий. Выполнение контрольной работы
Итого:		46ч	

Лабораторная работа

В период освоения дисциплины студенты посещают лекционные занятия, самостоятельно изучают дополнительный теоретический материал к лабораторным занятиям. Критериями оценки работы на лабораторных занятиях является: полнота и правильность выполненного задания; степень осознанности, понимания изученного; оформление задания.

Темы лабораторных работ

Тема 1. Основные понятия информационной безопасности и защиты информации.

Тема 2. Криптография и криптосистемы.

Тема 3. Электронная цифровая подпись. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.

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

Критерии оценки:

0 баллов - ставится, если студент не готов к лабораторной работе.

1 балл - ставится, если студент обнаруживает знание и понимание основных положений обсуждаемой темы, но при выполнении заданий допущены неточности или задание выполнено на 50-60%; оформление работы выполнено недостаточно последовательно, допущены ошибки в языковом оформлении материала.

2 балла - ставится, если студент обнаруживает знание и понимание основных положений обсуждаемой темы, но при выполнении заданий допущены неточности или задание выполнено на 70-80%; слабо владеет навыками исследовательского анализа по данной теме; оформление работы выполнено недостаточно правильно.

3 балла - ставится, если студент полностью выполнил задание, но допустил единичные ошибки в изложении материала, знает теоретический материал, самостоятельно поправляет ошибки и погрешности после замечаний преподавателя:

- задание выполнено правильно или, в случае недочётов, скорректировано студентом самостоятельно;
- студент обладает необходимыми навыками научно-исследовательского анализа по данной теме и обнаруживает полное понимание материала, может обосновать свои суждения;
- оформление задания выполнено последовательно и полно, правильно использована соответствующая терминология.

Самостоятельная работа студента

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

Темы заданий для самостоятельной работы студентов

СРС.1. Принципы засекречивания сведений и отнесения их к государственной тайне

СРС 2. Порядок отнесения информации к коммерческой тайне и способы ее получения

Критерии оценки:

№	Критерий	26	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	86		

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

Контрольная работа

Контрольная работа предполагает выполнение письменной работы с обязательными практическими примерами по одной из тем.

Тематика 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	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.

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	18ЛР*1,5ч=27ч	18ЛР*26=366	18ЛР*36=546	Теоретическое изучение материала, решение задач
2	Выполнение контрольной работы	11ч	156	306	в письменном виде, по вариантам
3	Выполнение самостоятельной работы	2СР*4ч=8ч	96	2СРС*86=166	в письменном виде, по вариантам
	Итого:	46ч	606	1006	

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
ПК-3: способен осуществлять алгоритмизацию поставленных задач и применять выбранные языки программирования для написания программного кода	знать: основные требования информационной безопасности. уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий. владеть: методиками решений стандартных задач профессиональной деятельности, практическими навыками использования коммуникационных технологий.	Освоено	Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения нестандартных заданий с использованием инструментария современных ИТ. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения в условиях своей профессиональной деятельности	зачтено
		Освоено	Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые были разобраны на практических занятиях с преподавателем. Обучаемый владеет терминологией, знаниями, умениями и навыками в применении информационных технологий в своей профессиональной деятельности.	зачтено
		Освоено	Обучаемый	зачтено

			<p>демонстрирует самостоятельность в применении знаний, умений и навыков к решению практических и теоретических заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем.</p> <p>Имеются ошибки в раскрытии понятий, употреблении терминов. Обучаемый не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи.</p>	
		Не освоены	<p>Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.</p> <p>Отсутствие самостоятельности в применении умения к использованию инструментария ИТ для решения задач в профессиональной деятельности и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу.</p>	незачтено

6.2. Методические материалы, определяющие процедуры оценивания

Характеристики процедуры	
Вид процедуры	зачет
Цель процедуры	выявить степень сформированности компетенций ПК-3
Локальные акты вуза, регламентирующие	Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся СВФУ, версия 2.0,

проведение процедуры	утверждено ректором СВФУ 15.03.2016 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	10 компьютеров
Требования к банку оценочных средств	-
Описание проведения процедуры	В соответствии с п. 5.13 Положения о балльно-рейтинговой системе в СВФУ, зачет «ставится при наборе 60 баллов». Таким образом, процедура зачета не предусмотрена.
Шкалы оценивания результатов	-
Результаты процедуры	В результате сдачи всех заданий студенту необходимо набрать не менее 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		18
2	Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ;			biblioclub.ru/index.php?page=book&id=428605	18
Дополнительная литература					
3	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			//biblioclub.ru/index.php?page=book&id=90539	18
4	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			//biblioclub.ru/index.php?page=book&id=90790	18
Периодические издания					
1	Автоматизация и производство				
2	Вестник компьютерных и информационных технологий				
3	Известия Вузов. Электроника				
4	Информационные технологии				

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).

5	Прикладная информатика
6	Программные продукты
7	Программирование на языке C++

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

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 дисциплине⁵

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

- ОС Windows, MS Visual Studio Open Office.

10.3. Перечень информационных справочных систем

Не используются.

⁵В перечне могут быть указаны такие информационные технологии, как использование на занятиях электронных изданий (чтение лекций с использованием слайд-презентаций, электронного курса лекций, графических объектов, видео- аудио- материалов (через Интернет), виртуальных лабораторий, практикумов), специализированных и офисных программ, информационных (справочных) систем, баз данных, организация взаимодействия с обучающимися посредством электронной почты, форумов, Интернет-групп, скайп, чаты, видеоконференцсвязь, компьютерное тестирование, дистанционные занятия (олимпиады, конференции), вебинар (семинар, организованный через Интернет), подготовка проектов с использованием электронного офиса или оболочки) и т.п.

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.ДВ.08.02 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

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.