Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники

УТВЕРЖДАЮ:
Директор института
_____ Галкин А. А.
«_26_» августа 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

направление подготовки / специальность

10.05.04 «Информационно-аналитические системы безопасности»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

Автоматизация информационно-аналитической деятельности
(направленность (профиль) подготовки))

г. Владимир

2021 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Методы и средства криптографической защиты информации» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО 3++ и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности», ознакомление студентов с основами теории двоичного кодирования, алгоритмами сжатия, помехоустойчивого кодирования. Дисциплина «Методы и средства криптографической защиты информации» рассматривается как теоретическая и прикладная дисциплина, дающая представления об основных математических и алгоритмических подходах, применяемых для хранения, передачи, исправления информации, представленной в двоичных кодах. Дисциплина посвящена изучению основ криптографии и криптографического анализа, применяемых к защите информации в информационных системах Обучаемые знакомятся с понятием шифров, симметричной и асимметричной криптографии, электронной подписью, хешированием и другими математическими объектами криптографии. Изучаются соответствующие криптографические стандарты, применяемые сегодня в защите информации в России и за рубежом. Подробно рассматриваются: стандарты RSA, DES, GOST1989, и другие. Также уделено внимание перспективным направлениям в криптографии: криптографические протоколы с разглашением и без разглашения, теория алгоритмической сложности и односторонних функций, схемы разделения секрета и некоторые их приложения в задачах идентификации и аутентификации

Задачами курса дисциплины являются: ознакомление с основами математической теории криптологии; приобретение навыков в практическом использовании, постановке и решении задач шифрования информации; понимание сути информационных процессов в криптографических системах; применение компьютеров для решения задач шифрования и дешифрования; разработка и использование математических и вычислительных моделей процессов шифрования информации, их оптимизация и выработка направлений совершенствования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части образовательной программы, код Б1.О.14 специальности 10.05.04 «Информационно-аналитические системы безопасности». В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора*	Результаты обучения по дисциплине	
ОПК-3 Способен на основании совокупности существующих математических методов	ОПК-3.1.1	Знать основные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды)	Тестовые вопросы
	ОПК-3.1.2	Знать понятие пропускной способности канала связи, прямую и обратную теоремы кодирования (без доказательства)	

разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1.3	Знать основные методы оптимального кодирования источников информации (код Хаффмана) и помехоустойчивого кодирования каналов связи (линейные коды, циклические коды, код Хэмминга)	
	ОПК-3.2.1	Уметь вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность)	
	ОПК-3.3.1	Владеть общими проблемы криптологии, в сфере применения соответствующих задач, возникающих при построении информационных систем различного назначения, а также критерии информационных оценок функционирования этих систем	
ОПК-9 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-9.1.1	Знать основные понятия и задачи криптографии, математические модели криптографических систем	
	ОПК-9.1.2	Знать основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы	
	ОПК-9.1.3	Знать национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения	
	ОПК-9.1.4	Знать основные положения (основополагающие теоремы) криптологии, вытекающие из теории симметричных и ассиметричных криптографических подходов, а также информационные критерии оценок функционирования криптографических систем	
	ОПК-9.1.5	Знать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	
	ОПК-9.2.1	Уметь разрабатывать и рассчитать характеристики криптографической защиты информационных систем в зависимости от назначения этих систем (количество информации, скорость передачи информации, пропускную способность каналов связи, требуемый объём памяти и др.)	
	ОПК-9.2.2	Уметь применять современные технологии криптографии в задачах обработки информации	
	ОПК-9.2.3	Уметь применять математические модели для оценки стойкости СКЗИ	
	ОПК-9.2.4	Уметь использовать СКЗИ в автоматизированных системах	
	ОПК-9.31	Владеть общими проблемы криптологии, в сфере применения соответствующих задач, возникающих при построении информационных систем различного назначения, а также критерии информационных оценок функционирования этих систем	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Криптографические протоколы.	7	1-2	4	4	4		5	
2	Протокол анонимных вычислений.	7	3-4	4	4	4		5	
3	Криптография на эллиптических кривых	7	5-6	4	4	4		5	Рейтинг-контроль №1
4	Электронная подпись.	7	7-8	4	4	4		5	
5	Функция Эйлера. RSA.	7	9-10	4	4	4		5	
6	Задачи факторизации и дискретного логарифма.	7	11-12	4	4	4		5	Рейтинг-контроль №2
7	Схемы разделения секрета	7	13-14	4	4	4		5	
8	Принцип Керкхоффса	7	15-16	4	4	4		5	
9	Примеры шифров. Шифр Цезаря, Полибия	7	17-18	4	4	4		5	Рейтинг-контроль №3
Всего за 6 семестр		**180**		**36**	**36**	**36**		**45**	**Экзамен (27)**
Наличие в дисциплине КП/КР		**нет**							
Итого по дисциплине		**180**		**36**	**36**	**36**		**45**	**Экзамен (27)**

Содержание лекционных занятий по дисциплине

Раздел 1. Введение. Стандарты и функции криптографии

Тема 1. *Криптографические протоколы.* Криптографический протокол (англ. Cryptographic protocol) — это абстрактный или конкретный протокол, включающий набор криптографических алгоритмов. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.

Тема 2. *Протокол анонимных вычислений.* SSL (англ. *Secure Sockets Layer* — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко использовался для обмена мгновенными сообщениями и передачи голоса через IP (англ. *Voice over IP* — VoIP) в таких приложениях, как электронная почта, интернет-факс и др. В 2014 году правительство США сообщило об уязвимости в текущей версии протокола[1]. SSL должен быть исключён из работы в пользу TLS (см. CVE-2014-3566). SSL изначально разработан

компанией *Netscape Communications* для добавления протокола HTTPS в свой веб-браузер Netscape Navigator. Впоследствии на основании протокола SSL 3.0 был разработан и принят стандарт RFC, получивший имя TLS.

Тема 3. *Криптография на эллиптических кривых.* Эллиптическая криптография — раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. ... Использование эллиптических кривых для создания криптосистем было независимо друг от друга предложено Нилом Коблицем и Виктором Миллером в 1985 году.

Тема 4. *Задачи факторизации и дискретного логарифма*. Дискретное логарифмирование (DLOG) — задача обращения функции в некоторой конечной мультипликативной группе. Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны.

Тема 5. *Схемы разделения секрета*. Схема разделения секрета - криптографическая схема, позволяющая разделить секрет между участниками группы, при этом каждый участник получает долю секрета, а исходный секрет стирается. Воссоздать **секрет** может определенная коалиция участников

Раздел 2. Виды шифрования и протоколов.

Тема 1. *Принцип Керкхоффса.* При́нцип Керкго́ффса — правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым. Другими словами, при оценке надёжности шифрования необходимо предполагать, что противник знает об используемой системе шифрования всё, кроме применяемых ключей. Широко применяется в криптографии. Впервые данный принцип сформулировал в XIX веке голландский криптограф Огюст Керкгоффс

Тема 2. *Примеры щифров. Шифр Цезаря, Полибия.* Шифр Цезаря -- это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется буквой, находящейся на некоторое постоянное число позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3, А была бы заменена на Г, Б станет Д, и так далее. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами. Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все еще имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

Содержание лабораторных занятий по дисциплине

Темы лабораторных работ:

Лабораторная работа №1. Тема 1: Хэш-функция. Электронная подпись.

Лабораторная работа №2. Тема 2: Генератор псевдослучайных последовательностей.

Лабораторная работа №3. Тема 3: Генерация ключей.

Лабораторная работа №4. Тема 4: Арифметика с длинными целыми.

Темы практических занятий

- Классы сложности алгоритмов и задач.
- Одностороннии функции. Задачи-кандидаты в одностороннии функции.
- Функции Эйлера и ее свойства. Теорема Эйлера и теорема Ферма.
- Факторизация целого числа.
- Дискретный логарифм в конечных полях. Протокол Диффи-Хеллмана.

- RSA.
- Электронная подпись в ассиметричных схемах и ее свойства. С хеш функциями и без.
- Хеш функции и их свойства. Криптографические хеш-функции.
- Криптографические протоколы.
- Интераполяция многочленами. Теорема о существовании и единственности многочлена. Схема разделения секрета Шамира.
- Электронные деньги. Неотслеживаемость. Схема Шаума-Педерсана.
- Стандарты DES и ГОСТ Блочных шифров. Архитектурный и сравнительный анализ шифров.
- Блочные шифры. Режимы работ блочных шифров.
- Потоковые шифры.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Вопросы рейтинг-контроля №1

- Понятие электронной подписи. Необходимость электронной подписи в криптосистемах с открытым ключом.
- Математическая теория групп как основа современных криптосистем.
- Дискретные отображения и признаки хаотичности числовых рядов.
- Аннулирующие многочлены.

Вопросы рейтинг-контроля №2

- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Конструкция конечного поля из pn элементов.
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.

Вопросы рейтинг-контроля №3

- Оценки и критерии сложности алгоритмов криптографии.
- Криптоанализ и алгоритмические неразрешимые проблемы.
- Особенности хаотических систем.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.

5.2. Промежуточная аттестация по итогам освоения дисциплины

Примерный перечень вопросов к экзамену

- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.
- Дискретные отображения и признаки хаотичности числовых рядов.

- Методы криптографии на основе сортировки детерминировано-хаотических рядов.
- Методы криптографии на основе парных сравнений чисел в детерминировано-хаотических числовых рядах.
- Стеганография.
- Оценки и критерии сложности алгоритмов криптографии.
- Криптоанализ и алгоритмические неразрешимые проблемы.
- Особенности хаотических систем.
- Дискретный логарифм в конечных полях. Протокол Диффи-Хеллмана.
- Алгоритм RSA.
- Электронная подпись в ассиметричных схемах и ее свойства. С хеш функциями и без.
- Хеш функции и их свойства. Криптографические хеш-функции.
- Криптографические протоколы.
- Интераполяция многочленами. Теорема о существовании и единственности многочлена. Схема разделения секрета Шамира.
- Электронные деньги. Неотслеживаемость. Схема Шаума-Педерсана.
- Стандарты DES и ГОСТ Блочных шифров. Архитектурный и сравнительный анализ шифров.
- Блочные шифры. Режимы работ блочных шифров.
- Потоковые шифры.
- Криптографические модели безопасности. Модель симметричного шифрования, ассиметричного и модель Долев-Яо.

5.3. Самостоятельная работа обучающегося.

Вопросы и задания для самостоятельной работы студентов 6 семестр:

- Основные соотношения затрат памяти и времени.
- Автоматы на основе дискретного отображения Лоренца, достоинства и недостатки;
- Автоматы на основе отображений TentMap и Хенона, сопоставительный анализ.
- Сопоставительный анализ алгоритмов криптоанализа, оценки сложности;
- Перспективы криптоанализа и алгоритмически неразрешимы проблемы.

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература		
Котов, Ю. А. Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом : [16+] / Ю. А. Котов. – Новосибирск: Новосибирский государственный технический университет, 2017. – 67 с.– ISBN 978-5-7782-3411-6	2017	https://biblioclub.ru/index.php?page=book&id=574782 (дата обращения: 14.09.2021)
Майстренко, Н. В. Основы теории информации и криптографии: учебное электронное издание / Н. В. Майстренко, А. В. Майстренко. – Тамбов: Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. – ISBN 978-5-8265-1950-9	2018	https://biblioclub.ru/index.php?page=book&id=570354 (дата обращения: 14.09.2021)

Фороузан, Б. А. Математика криптографии и теория шифрования: учебное пособие: [16+] / Б. А. Фороузан. – 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 511 с. – ISBN 978-5-9963-0242-0	2016	https://biblioclub.ru/index.php?page=book&id=428998 (дата обращения: 14.09.2021)
Лапонина, О. Р. Криптографические основы безопасности: учебное пособие: [16+] / О. Р. Лапонина. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с.– ISBN 5-9556-00020-5	2016	https://biblioclub.ru/index.php?page=book&id=429092 (дата обращения: 14.09.2021)
Котов, Ю. А. Приложения шифров: криптоанализ: [16+] / Ю. А. Котов; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 76 с. – ISBN 978-5-7782-3902-9	2019	https://biblioclub.ru/index.php?page=book&id=575479 (дата обращения: 14.09.2021)
Дополнительная литература		
Кнауб, Л. В. Теоретико-численные методы в криптографии: учебное пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов; Сибирский федеральный университет. – Красноярск: Сибирский федеральный университет (СФУ), 2011. – 160 с. – ISBN 978-5-7638-2113-7	2011	https://biblioclub.ru/index.php?page=book&id=229582 (дата обращения: 14.09.2021)
Аграновский, А. В. Практическая криптография: алгоритмы и их программирование: [16+] / А. В. Аграновский, Р. А. Хади. – Москва: СОЛОН-ПРЕСС, 2009. – 256 с. – ISBN 5-98003-002-6	2009	https://biblioclub.ru/index.php?page=book&id=117663 (дата обращения: 14.09.2021)

6.2. Периодические издания

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.

6.3. Интернет-ресурсы

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
3. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045.

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4,

симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил: доцент кафедры ИЗИ к.ф-м.н. Александров А.В_____

Рецензент: Заместитель руководителя РАЦ ООО
«ИнфоЦентр» к.т.н. Вертилевский Н.В_____

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 26.08.21 года
Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/__

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии специальности 10.05.04 «Информационно-аналитические системы безопасности»

Протокол № 1 от 26.08.21 года
Председатель комиссии д.т.н., профессор_____/М.Ю. Монахов/__

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20 22 / 20 23 учебный год

Протокол заседания кафедры № 14 от 28.06.22 года

Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/__

(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/__

(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/__

(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/__

(ФИО, подпись)

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Методы и средства криптографической защиты информации

образовательной программы специальности

10.05.04 «Информационно-аналитические системы безопасности»

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/М.Ю. Монахов/__

Подпись *ФИО*