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.
«01» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защищенные информационные системы
(наименование дисциплины)

направление подготовки / специальность

10.03.01 «Информационная безопасность»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

**Безопасность автоматизированных систем
(по отраслям или в сфере профессиональной деятельности)**
(направленность (профиль) подготовки))

г. Владимир

2023 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защищенные информационные системы» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность». Целью освоения дисциплины является ознакомление специалистов с современным теоретическим аппаратом информационной безопасности, представление сведений о базовых моделях и алгоритмах, используемых в управлении информационной безопасностью в информационных системах, а также о процессе теоретико-методологического анализа различных механизмов и сервисов защиты информации.

Задачей освоения курса является изучение аппарата управления информационной безопасностью в информационных системах, освоение методов анализа программно-технических сервисов информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защищенные информационные системы» относится к части, формируемой участниками образовательных отношений, код Б1.В.01 учебного плана направления подготовки 10.03.01 «Информационная безопасность». 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	
ПК-1 Способен осуществлять анализ уязвимостей внедряемой системы защиты информации	ПК-1.1.1	Знать содержание эксплуатационной документации автоматизированной системы	Тестовые вопросы
	ПК-1.2.1	Уметь классифицировать и оценивать угрозы безопасности информации автоматизированной системы	
	ПК-1.2.2	Уметь проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств	
	ПК-1.3.1	Владеть навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных систем	
	ПК-1.3.2	Владеть навыками анализа уязвимости программных и программно- аппаратных средств системы защиты информации автоматизированной системы	

ПК-3 Способен осуществлять аудит защищенности информации в автоматизированных системах	ПК-3.1.1	Знать содержание эксплуатационной документации автоматизированной системы	Тестовые вопросы
	ПК-3.2.1	Уметь разрабатывать политики безопасности информации автоматизированных систем	
	ПК-3.2.2	Уметь применять инструментальные средства контроля защищенности информации в автоматизированных системах	
	ПК-3.3.1	Владеть навыками оценки информационных рисков	
	ПК-3.3.2	Владеть навыками обоснования и контроля результатов управленческих решений в области безопасности информации автоматизированных систем	
	ПК-3.3.3	Владеть навыками оценки состояния защищенности информации автоматизированных систем	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 2 зачетных единиц, 72 часа

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	Информационные технологии и информационные системы.	8	1-2	2		2		1	
2	Примеры информационных технологий и информационных систем	8	3-4	2		2		1	
3	Проектирование и разработка защищенных информационных технологий	8	5-6	2		2	2	1	Рейтинг-контроль №1
4	Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении	8	7-8	2		2		1	
5	Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».	8	9-10	2		2	2	1	
6	Содержание классов защищенности.	8	11-12	2		2		1	Рейтинг-контроль №2

7	Функциональные требования.	8	13-14	2		2		1	
8	Вопросы гарантий и эффективности в европейском стандарте ITSEC.	8	15-16	2		2		1	
9	Подход к безопасности компьютерных систем в СС и базовые концепции.	8	17-18	2		2	2	1	Рейтинг-контроль №3
Всего за 8 семестр:		**72**		**18**		**18**		**9**	**Экзамен(27)**
Наличие в дисциплине КП/КР		**нет**							
Итого по дисциплине		**72**		**18**		**18**		**9**	**Экзамен(27)**

Содержание лекционных занятий по дисциплине

Раздел 1. Информационные технологии и информационные системы

Тема 1. Информационные технологии и информационные системы.
Примеры информационных технологий и информационных систем. Типы компьютерных систем, как элементов информационных технологий.

Тема 2. Основные принципы успешного функционирования информационной (компьютерной) системы.
Цель принимаемых руководством предприятия и должност-ными лицами мер по поддержке информационных технологий принятия решений. Основные принципы и методы защиты информационных процессов в компьютерных системах.

Тема 3. Проектирование и разработка защищенных информационных технологий.
Понятие защищенной информационной технологии. Основные подходы, используемые при проектировании защищенных информационных технологий.

Тема 4. Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.
Государственные стандарты на разработку и создание информационных систем в защищенном исполнении. CASE-технологии создания информационных систем. Стандарт ITIL.

Тема 5. Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
Американский стандарт по защите информации «Оранжевая книга». Понятие гарантии защиты. Критерии оценки защищенности баз данных.

Раздел 2. Требования к защите информации

Тема 1. Содержание классов защищенности.
Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.

Тема 2. Функциональные требования.
Вопросы гарантий и эффективности в европейском стандарте ITSEC. Европейский стандарт по защите информации ITSEC.

Тема 3. Понятие гарантии защиты в соответствии с европейским стандартом.
Критерии оценки защищенности. Содержание классов защищенности. Функциональные требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения защищенных информационных систем.

Тема 4. Подход к безопасности компьютерных систем в СС и базовые концепции.
Понятие профиля защиты. Функции поддержки политики безопасности.

Содержание лабораторных занятий по дисциплине

Раздел 1. Информационные технологии и информационные системы

Тема № 1. Сравнительный анализ различных стандартов в области защиты информационных технологий с точки зрения эффективности достижения цели построения защищенных информационных систем.

Изучить следующие стандарты и провести их сравнительный анализ: Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»). Европейские критерии безопасности информационных технологий. Руководящие документы ФСТЭК в области построения защищенных систем обработки информации. Федеральные критерии безопасности информационных технологий. Обзор серии стандартов ИСО/МЭК 27000. Сравнительный анализ стандартов в области защиты информационных систем.

Тема № 2. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев

Опишите уровень A (класс безопасности) в системе общих критериев?
Опишите уровень B (класс безопасности) в системе общих критериев?
Опишите уровень C (класс безопасности) в системе общих критериев?
Опишите уровень D (класс безопасности) в системе общих критериев?

Тема № 3. Анализ рисков для информационной системы предприятия (организации) и построение модели угроз безопасности

Изучить следующие документы: Классификация и характеристика угроз информационной безопасности ИС. Методики и программный инструментарий для анализа и оценки рисков информационной безопасности. Программные комплексы *MSAT* и ГРИФ. Методология *COBIT* и программный инструментарий *CORAS.* Методология *OCTAVE*. Методы и программные продукты, используемые в международной практике для анализа и оценки рисков, угроз и уязвимостей информационной системы. Учет угроз и рисков при построении защищенной системы обработки информации. Особенности анализа и оценки рисков информационной безопасности в малом и среднем бизнесе. Управление инцидентами информационной безопасности.

Тема № 4. Порядок сертификации средств защиты информации для разработчика СЗИ.

Дайте определение понятию «сертификация»?
Дайте определение понятию «сертификат соответствия»?
В каком порядке проводится сертификация?
В каком порядке проводится контроль сертифицированных продуктов?
Какие средства подлежат обязательной сертификации

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

8 семестр

Вопросы рейтинг-контроля №1

- Типы компьютерных систем, как элементов информационных технологий.
- Основные принципы успешного функционирования информационной (компьютерной) системы.

- Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.
- Основные принципы и методы защиты информационных процессов в компьютерных системах.
- Понятие защищенной информационной технологии.
- Основные подходы, используемые при проектировании защищенных информационных технологий.
- Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.

Вопросы рейтинг-контроля №2

- Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.
- Вопросы гарантий и эффективности в европейском стандарте ITSEC.
- Европейский стандарт по защите информации ITSEC.
- Понятие гарантии защиты в соответствии с европейским стандартом ITSEC.
- Критерии оценки защищенности в соответствии с европейским стандартом ITSEC. Содержание классов защищенности в соответствии с европейским стандартом ITSEC.
- Функциональные требования по защите информации, предъявляемые в каждом классе защищенности в соответствии с европейским стандартом ITSEC.
- Принципы и методы построения защищенных информационных систем.

Вопросы рейтинг-контроля №3

- Подсистемы разграничения доступа.
- Подсистемы идентификации и аутентификации.
- Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы.
- Подсистемы защиты связи.
- Требования к подсистемам, предъявляемые в каждом классе защищенности.
- Гарантии безопасности компьютерных систем в системе общих критериев.
- Понятие гарантии безопасности. Уровни гарантий.
- Гарантии проектирования защищенных информационных систем.
- Принципы обеспечения гарантий безопасности. Методология анализа гарантий безопасности.

5.2. Промежуточная аттестация по итогам освоения дисциплины

Примерный перечень вопросов к экзамену 8 семестр:

- Типы компьютерных систем, как элементов информационных технологий.
- Основные принципы успешного функционирования информационной (компьютерной) системы.
- Цель принимаемых руководством предприятия и должностными лицами мер по поддержке информационных технологий принятия решений.
- Основные принципы и методы защиты информационных процессов в компьютерных системах.
- Понятие защищенной информационной технологии.
- Основные подходы, используемые при проектировании защищенных информационных технологий.
- Требования, предъявляемые к информационным (компьютерным) системам в защищенном исполнении.

- Государственные стандарты на разработку и создание информационных систем в защищенном исполнении.
- CASE-технологии создания информационных систем.
- Стандарт ITIL.
- Построение гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга».
- Американский стандарт по защите информации «Оранжевая книга».
- Понятие гарантии защиты.
- Критерии оценки защищенности баз данных.
- Содержание классов защищенности.
- Требования по защите информации, предъявляемые в каждом классе защищенности. Принципы и методы построения гарантированно защищенных информационных систем.
- Вопросы гарантий и эффективности в европейском стандарте ITSEC.
- Европейский стандарт по защите информации ITSEC.
- Понятие гарантии защиты в соответствии с европейским стандартом ITSEC.
- Критерии оценки защищенности в соответствии с европейским стандартом ITSEC. Содержание классов защищенности в соответствии с европейским стандартом ITSEC.
- Функциональные требования по защите информации, предъявляемые в каждом классе защищенности в соответствии с европейским стандартом ITSEC.
- Принципы и методы построения защищенных информационных систем.
- Подход к безопасности компьютерных систем в СС и базовые концепции. Понятие профиля защиты.
- Функции поддержки политики безопасности. Гарантии безопасности.
- Требования по безопасности информационных технологий. Классы защищенности.
- Компоненты подсистем поддержки политики безопасности.
- Содержание типовой политики безопасности.
- Классы защищенности в системе общих критериев. Понятие аудита политики безопасности.
- Требования к подсистемам аудита.

5.3. Самостоятельная работа обучающегося.

Примерные вопросы и задания для самостоятельной работы студентов

- ITIL – Компонент «Поддержка услуг».
- ITIL – Компонент «Предоставление услуг».
- ITIL — основа концепции управления ИТ-службами.
- Service Desk — цели, возможности, реализации.
- Аудит инфраструктуры РИС/КАС.
- Аутсорсинг.
- Методология Penetration Testing. Open Source Security Testing Methodology Manual (OSSTMM).
- Методология Penetration Testing. Information Systems Security Assessment Framework (ISSAF).
- Методология Penetration Testing. Open Web Application Security Project (OWASP).
- Методология Penetration Testing. Web Application Security Consortium Threat Classification (WASC-TC).
- Стандарт Penetration Testing. Penetration Testing Execution Standard (PTES).
- Footprinting. Цели, задачи Footprinting. Этапы Footprinting и Reconnaissance.
- Footprinting. Открытые источники и пассивный сбор информации.
- Footprinting. Активный сбор информации.

- Footprinting. Программные инструменты Footprinting и Reconnaissance.
- Сканирование сети. Обнаружение узлов сети. Методы и программные средства.
- Сканирование сети. Обнаружение открытых портов узла сети. Методы и программные средства.
- Сканирование сети. Типы сканирования (Full Open Scan, Half-open Scan, Xmas Tree Scan). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (FIN Scan, NULL Scan, ACK Scanning). Особенности использования рассматриваемых типов сканирования.
- Сканирование сети. Типы сканирования (UDP Scanning, ARP Scan). Особенности использования рассматриваемых типов сканирования.

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		
Технологии обеспечения безопасности информационных систем: учебное пособие: [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва; Берлин: Директ-Медиа, 2021. – 210 с.– ISBN 978-5-4499-1671-6. – DOI 10.23681/598988	2021	https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 18.09.2021)
Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем: курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. – Томск: ТУСУР, 2016. – 396 с.	2016	https://biblioclub.ru/index.php?page=book&id=480796 (дата обращения: 18.09.2021)
Мэйволд, Э. Безопасность сетей: учебное пособие: [16+] / Э. Мэйволд. – 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с.	2016	https://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 18.09.2021)
Бова, В. В. Основы проектирования информационных систем и технологий: учебное пособие: [16+] / В. В. Бова, Ю. А. Кравченко. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 106 с.– ISBN 978-5-9275-2717-5	2018	https://biblioclub.ru/index.php?page=book&id=499515 (дата обращения: 18.09.2021)
Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие: [16+] / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с.	2017	https://biblioclub.ru/index.php?page=book&id=467139 (дата обращения: 18.09.2021)
Дополнительная литература		
Методологические основы построения защищенных автоматизированных систем: учебное пособие / А. В. Душкин, О. В. Ланкин, С. В. Потехецкий и др.; Воронежский государственный университет инженерных технологий. – Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 258 с. – ISBN 978-5-89448-981-0	2013	https://biblioclub.ru/index.php?page=book&id=255851 (дата обращения: 18.09.2021)

Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие: [16+] / А. М. Голиков; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск, 2015. – 284 с.	2015	https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 18.09.2021)
Организация безопасной работы информационных систем: учебное пособие / Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако и др.; Тамбовский государственный технический университет. – Тамбов, 2014. – 132 с..	2014	https://biblioclub.ru/index.php?page=book&id=277794 (дата обращения: 18.09.2021)

6.2. Периодические издания

- Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
- Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
- Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.
- «Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;
- Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

6.3. Интернет-ресурсы

- Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
- Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
- Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.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: заведующий кафедрой ИЗИ
д.т.н. Монахов М.Ю.____

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

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 13 от 12.05.23 года
Заведующий кафедрой д.т.н., профессор__________________________/М.Ю. Монахов/____

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность»

Протокол № 13 от 12.05.23 года
Председатель комиссии д.т.н., профессор__________________________/М.Ю. Монахов/____

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

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)

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

Защищенные информационные системы

образовательной программы направления подготовки *10.03.01. Информационная безопасность*

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*