Министерство науки и высшего образования Российской Федерации

Муромский институт (филиал)

федерального государственного бюджетного образовательного учреждения высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(МИ ВлГУ)

Кафедра *ПИн*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
17.05.2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защищенные информационные системы

Направление подготовки *09.04.04 Программная инженерия*

Профиль подготовки

Семестр	Трудоемкость, час./зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
3	**144 / 4**	**12**		**28**	**3,2**	**0,35**	**43,55**	**64,8**	**Экз.(35,65)**
Итого	**144 / 4**	**12**		**28**	**3,2**	**0,35**	**43,55**	**64,8**	**35,65**

Муром, 2022 г.

1. Цель освоения дисциплины

Цель дисциплины: освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защищенные информационные системы» является необходимым компонентом образования магистров. Для освоения дисциплины «Защищенные информационные системы» студенты используют знания, умения, навыки, способы деятельности и установки, полученные и сформированные в ходе изучения дисциплин направления подготовки «Программная инженерия», уровень - бакалавриат. Изучение дисциплины «Защищенные информационные системы» является базой для дальнейшего освоения студентами дисциплин направления «Программная инженерия» и для прохождения практики и занятиям научно-исследовательской работы. Знания, умения и навыки, приобретенные при изучении данной дисциплины, используются при написании магистерской диссертации.

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	Результаты обучения по дисциплине	
ОПК-7 Способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях	ОПК-7.2 Реализует технические и организационные меры, обеспечивающие защиту от несанкционированного доступа к информации в реализуемой системе	Знать методики формирования команд и эффективного руководства коллективами (ОПК-7.2) Знать современное программное и аппаратное обеспечение информационных и автоматизированных систем (ОПК-7.2) Уметь модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач (ОПК-7.2) Уметь разрабатывать командную стратегию; организовывать работу коллективов; управлять коллективом; разрабатывать мероприятия по личностному, образовательному и профессиональному росту (ОПК-7.2) Иметь навыки разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	тест

		(ОПК-7.2) Владеть методами организации и управления коллективом, планированием его действий (ОПК-7.2)	

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

4.1. Форма обучения: очная

Уровень базового образования: высшее.
Срок обучения 2г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Управление рисками. Методики построения систем защиты информации	3	8		4					34	тестирование
2	Протоколы защиты данных	3	2		12					15	тестирование
3	Инфраструктура открытых ключей. Цифровые сертификаты	3	2		12					15,8	тестирование
Всего за семестр		144	12		28			3,2	0,35	64,8	Экз.(35,65)
Итого		144	12		28			3,2	0,35	64,8	35,65

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 3

Раздел 1. Управление рисками. Методики построения систем защиты информации

Лекция 1.

Управление рисками. Модель безопасности с полным перекрытием (2 часа).

Лекция 2.

Методы защиты информации (2 часа).

Лекция 3.

Методики и программные продукты для оценки рисков (2 часа).

Лекция 4.

Проведение оценки рисков в соответствии с методикой Microsoft (2 часа).

Раздел 2. Протоколы защиты данных

Лекция 5.

Протокол Kerberos (2 часа).

Раздел 3. Инфраструктура открытых ключей. Цифровые сертификаты
Лекция 6.

Инфраструктура открытых ключей. Цифровые сертификаты (2 часа).

4.1.2.2. Перечень практических занятий

Не планируется.

4.1.2.3. Перечень лабораторных работ

Семестр 3
Раздел 1. Управление рисками. Методики построения систем защиты информации
Лабораторная 1.

Исследование системы анализа рисков и проверки политики информационной безопасности предприятия (4 часа).
Раздел 2. Протоколы защиты данных
Лабораторная 2.

Исследование защищенности беспроводных сетей передачи данных (4 часа).
Лабораторная 3.

Исследование и администрирование средств обеспечения информационной безопасности Web-сервера Microsoft IIS Server (4 часа).
Лабораторная 4.

Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server (4 часа).
Раздел 3. Инфраструктура открытых ключей. Цифровые сертификаты
Лабораторная 5.

Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA (4 часа).
Лабораторная 6.

Исследование и развертывание сетевой инфраструктуры Microsoft Windows Exchange Server (4 часа).
Лабораторная 7.

Использование цифровых сертификатов (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:
1. Модели безопасности Windows.
2. Современные стандарты в области информационной безопасности, использующие концепцию управление рисками ISO/IEC 15408. Критерии оценки безопасности информационных технологий.
3. Стандарты ISO/IEC 17799/27002 и 27001.
4. Lifecycle Security; Модель многоуровневой защиты;.
5. Методика управления рисками, предлагаемая Microsoft.
6. Управление рисками по методикам: -Методика CRAMM; -Методика FRAP; - Методика OCTAVE; - Методика RiskWatch.
7. Анализ существующих подходов к оценке рисков.
8. Технические мероприятия по снижению уровня риска.
9. Идентификация и аутентификация.
10. Протокол защиты электронной почты SSL.
11. Протокол IPSec.
12. Межсетевые экраны.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

4.2 Форма обучения: заочная

Уровень базового образования: высшее.

Срок обучения 2г 6м.

Семестр	Трудоемкость, час./ зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль,час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
5	**144 / 4**	**8**		**12**	**4**	**0,6**	**24,6**	**110,75**	**Экз.(8,65)**
Итого	**144 / 4**	**8**		**12**	**4**	**0,6**	**24,6**	**110,75**	**8,65**

4.2.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Управление рисками. Методики построения систем защиты информации	5	2		4					20	тестирование
2	Протоколы защиты данных.	5	4		4					54	тестирование
3	Инфраструктура открытых ключей. Цифровые сертификаты	5	2		4					36,75	тестирование
Всего за семестр		144	8		12	+		4	0,6	110,75	Экз.(8,65)
Итого		144	8		12			4	0,6	110,75	8,65

4.2.2. Содержание дисциплины

4.2.2.1. Перечень лекций

Семестр 5

Раздел 1. Управление рисками. Методики построения систем защиты информации

Лекция 1.

Управление рисками. Модель безопасности с полным перекрытием (2 часа).

Раздел 2. Протоколы защиты данных.

Лекция 2.

Методики построения систем защиты информации (2 часа).

Лекция 3.

Методики и программные продукты для оценки рисков (2 часа).

Раздел 3. Инфраструктура открытых ключей. Цифровые сертификаты

Лекция 4.

Инфраструктура открытых ключей. Цифровые сертификаты (2 часа).

4.2.2.2. Перечень практических занятий

Не планируется.

4.2.2.3. Перечень лабораторных работ

Семестр 5

Раздел 1. Управление рисками. Методики построения систем защиты информации

Лабораторная 1.

Исследование системы анализа рисков и проверки политики информационной безопасности предприятия (4 часа).

Раздел 2. Протоколы защиты данных.

Лабораторная 2.

Исследование защищенности беспроводных сетей передачи данных (4 часа).

Раздел 3. Инфраструктура открытых ключей. Цифровые сертификаты

Лабораторная 3.

Использование цифровых сертификатов (4 часа).

4.2.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Модели безопасности Windows.
2. Современные стандарты в области информационной безопасности, использующие концепцию управление рисками ISO/IEC 15408. Критерии оценки безопасности информационных технологий.
3. Стандарты ISO/IEC 17799/27002 и 27001.
4. Lifecycle Security; Модель многоуровневой защиты;.
5. Методика управления рисками, предлагаемая Microsoft.
6. Управление рисками по методикам: -Методика CRAMM; -Методика FRAP; - Методика OCTAVE; - Методика RiskWatch.
7. Анализ существующих подходов к оценке рисков.
8. Технические мероприятия по снижению уровня риска.
9. Идентификация и аутентификация.
10. Протокол защиты электронной почты SSL.
11. Протокол IPSec.
12. Межсетевые экраны.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.2.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

1. 1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними.
2. 2 Современные средства защиты информации.
3. 3 Современные системы компьютерной безопасности.
4. 4 Современные средства противодействия экономическому шпионажу.
5. 5 Современные криптографические системы.
6. 6 Криптоанализ, современное состояние.

7. 7 Правовые основы защиты информации.
8. 8 Технические аспекты обеспечения защиты информации. Современное состояние.
9. 9 Атаки на систему безопасности и современные методы защиты.
10. 10 Современные пути решения проблемы информационной безопасности РФ.

4.2.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В рамках изучения дисциплины используются интерактивные технологии преподавания, выраженные в виде совместных обсуждений проблемных ситуаций, совместного анализа путей решения поставленных задач. В рамках выполнения лабораторных работ формируются небольшие коллективы из студентов для совместного решения задач. Результаты работы отдельных коллективов обсуждаются всей группой, при этом используются средства мультимедийной техники.

Преподаватель выступает в роли координатора работы коллективов студентов, дает оценку их работе.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонды оценочных материалов (средств) приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины.

7.1. Основная учебно-методическая литература по дисциплине

1. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с. - https://www.iprbookshop.ru/120489.html

2. Епишкина, А. В. Нормативное регулирование в области защиты информации. Конспект лекций : учебное пособие / А. В. Епишкина, С. В. Запечников. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2021. — 116 с. - https://www.iprbookshop.ru/125496.html

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. — Москва, Вологда : Инфра-Инженерия, 2022. — 104 с. - https://www.iprbookshop.ru/124242.html

2. Разработка и защита баз данных в Microsoft SQL Server 2005 : учебное пособие / . — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 147 с. - https://www.iprbookshop.ru/102058.html

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;

- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

Электронная библиотека ВлГУ (http://dspace.www1.vlsu.ru);

Электронная библиотечная системы "IPRBooks" (http://www.iprbookshop.ru/).

Программное обеспечение:

LibreOffice (Mozilla Public License v2.0)

Microsoft Windows 10 Professional (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Microsoft Visual Studio (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

iprbookshop.ru

dspace.www1.vlsu.ru);

mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лаборатория технологий разработки баз данных

12 шт. компьютеров Intel Core i5-2400 3,10 GHz, 4гб, DVD-R/ Philips 19’; проектор ACER P1100 DLP Projector EMEA; экран проекционный настенный DRAPPER Apex STAR; маршрутизатор Gigabit Switch TEG-S16S; плоттер HP Design Jet T610. Маркерная доска. Доступ к сети Интернет.

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями. Учебные пособия дополняют материал, которые дается на лекциях. В Информационно-образовательном портале имеется демонстрационный материал к лекциям.

До выполнения лабораторных работ обучающийся изучает соответствующий раздел теории. Перед занятием студент знакомится с описанием заданий для выполнения работы, внимательно изучает содержание и порядок проведения лабораторной работы. Лабораторная работа проводятся в компьютерном классе. Обучающиеся выполняют индивидуальную задачу компьютерного моделирования в соответствии с заданием на лабораторную работу. Полученные результаты исследований сводятся в отчет и защищаются по традиционной методике в классе на следующем лабораторном занятии. При необходимости студент консультируется у преподавателя по содержанию своего задания. Необходимый теоретический материал, индивидуальное задание, шаги выполнения лабораторной работы и требование к отчету приведены в методических указаниях, размещенных на информационно-образовательном портале института.

Самостоятельная работа оказывает важное влияние на формирование личности будущего специалиста, она планируется обучающимся самостоятельно. Каждый обучающийся самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием дисциплины. Он выполняет внеаудиторную работу и изучение разделов, выносимых на самостоятельную работу, по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий. Материал, изученный при самостоятельной работе, необходим при итоговом тестированиии.

Форма заключительного контроля при промежуточной аттестации – экзамен. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и

своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *09.04.04 Программная инженерия*
Рабочую программу составил *к.т.н., доцент Белякова А.С.*_____

Программа рассмотрена и одобрена на заседании кафедры *ПИн*

протокол № 11 от 05.05.2022 года.
Заведующий кафедрой *ПИн* _____*Жизняков А.Л.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета

протокол № 4 от 12.05.2022 года.
Председатель комиссии ФИТР _____ *Рыжкова М.Н.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине
Защищенные информационные системы

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Задания для текущего контроля знаний приведены в Приложении 2.

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	Устный опрос (2 вопроса)	До 20 баллов
Рейтинг-контроль 2	Устный опрос (2 вопроса)	До 20 баллов
Рейтинг-контроль 3	Устный опрос (2 вопроса)	До 20 баллов
Посещение занятий студентом	Отметка в журнале посещений	5 баллов
Дополнительные баллы (бонусы)		
Выполнение семестрового плана самостоятельной работы	Защита лабораторных работ	1 балл за работу

2. Промежуточная аттестация по дисциплине

Перечень вопросов к экзамену / зачету / зачету с оценкой.
Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)

Тест рейтинг-контроль 1: https://www.mivlgu.ru/iop/mod/quiz/view.php?id=54956
Тест рейтинг-контроль 2: https://www.mivlgu.ru/iop/mod/quiz/view.php?id=54957
Тест рейтинг-контроль 3: https://www.mivlgu.ru/iop/mod/quiz/view.php?id=54958

Методические материалы, характеризующие процедуры оценивания

На основе перечня вопросов к тестированию программным комплексом информационно-образовательного портала МИ ВлГУ формируются в автоматическом режиме тестовые задания для студентов: 8 вопросов из блока 1, 4 вопроса из блока 2 и 3 вопроса из блока 3. Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Результатом тестирования является балл, рассчитанный на основе количества правильных ответов. С учетом индивидуального семестрового рейтинга студента формируется итоговый балл по курсу.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	***Уровень сформированности компетенций***
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все	***Высокий уровень***

		предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	***Продвинутый уровень***
50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	***Компетенции не сформированы***

3. Задания в тестовой форме по дисциплине

Примеры заданий:

1) Какие средства защиты информации связаны применением инструментов шифрования?

a. Организационные средства
b. Аппаратно-программные
c. Криптографические средства
d. Программные средства

2) Принцип, согласно которому секретность закрытого сообщения определяется секретностью ключа называется принципом...

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке https://www.mivlgu.ru/iop/question/edit.php?courseid=3054

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.