

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ

Проректор по учебной и научной
работе

 Лейфа А.В. Лейфа

« 1 » сентября 2023 г.

РАБОЧАЯ ПРОГРАММА
«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Направление подготовки 01.04.02 Прикладная математика и информатика

Направленность (профиль) образовательной программы – Математическое и программное обеспечение информационных систем

Квалификация выпускника – Магистр

Год набора – 2023

Форма обучения – Очная

Курс 2 Семестр 3

Зачет с оценкой 3 сем

Общая трудоемкость дисциплины 144.0 (академ. час), 4.00 (з.е)

Составитель С.Г. Самохвалова, доцент, канд. техн. наук

Факультет математики и информатики

Кафедра информационной безопасности

Рабочая программа составлена на основании Федерального государственного образовательного стандарта ВО для направления подготовки 01.04.02 Прикладная математика и информатика, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 10.01.18 № 13

Рабочая программа обсуждена на заседании кафедры информационной безопасности

01.09.2023 г., протокол № 1

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО

Учебно-методическое управление

Чалкина Н.А. Чалкина

« 1 » сентября 2023 г.

СОГЛАСОВАНО

Выпускающая кафедра

Максимова Н.Н. Максимова

« 1 » сентября 2023 г.

СОГЛАСОВАНО

Научная библиотека

Петрович О.В. Петрович

« 1 » сентября 2023 г.

СОГЛАСОВАНО

Центр цифровой трансформации и
технического обеспечения

Тодосейчук А.А. Тодосейчук

« 1 » сентября 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины:

Изучение принципов проектирования и анализа защищенности информационных систем

Задачи дисциплины:

проектирование, эксплуатация и совершенствование системы управления информационной безопасностью информационной системы
участие в проведении аттестации объектов информатизации по требованиям безопасности информационных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Безопасность информационных систем» относится к части, формируемой участниками образовательных отношений образовательной программы. Предшествующие учебные дисциплины (модули) и (или) практики, формирующие знания, умения и навыки, не-обходимые для обучения по дисциплине (модулю): современные Internet-технологии, при-кладное программирование на языке Python. Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами для подготовки выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1 Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ПК-3. Способен использовать программные средства и платформы инфраструктуры информационных технологий организации	ИД-1ПК-3. Знает устройство и функционирование со- временных информационных систем, современные стандарты информационного взаимодействия систем, программные средства и языки программирования, платформы инфраструктуры информационных технологий организаций, требования безопасности информационных систем. ИД-2ПК-3. Обладает навыками управления содержанием проекта: документирование требований, анализ продукта, организация моделируемых совещаний. ИД-3ПК-3. Умеет использовать современное прикладное программное обеспечение для векторной или растровой компьютерной графики.
ПК-4. Способен проводить анализ предметной области, формулировать требования к разрабатываемым информационным системам и прикладному программному обеспечению, разрабатывать сценарии использования	ИД-1ПК-4. Знает подходы к выявлению требований по- требителей, определению источников информации для требований ИД-2ПК-4. Умеет осуществлять выбор методов разра- ботки требований, проводить выбор типов и ат-рибутов требований, определять состава работ по разработке требований. ИД-3ПК-4. Обладает специальными знаниями в

программных продуктов, оформлять технические задания на разработку программного обеспечения в виде спецификации, анализировать риски и причины возникновения ошибок при разработке систем, проводить тестирование и приемку готовых программных продуктов	области разработки планов аналитических работ по отдельным частям системы, интегрирования планов аналитических работ по отдельным частям системы, передачи и согласования плана аналитических работ с менеджером проекта. ИД-4 ПК-4. Знает основы теории систем и системного анализа.
---	--

4. СТРУКТУРА ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4.00 зачетных единицы, 144.0 академических часов.

1 – № п/п

2 – Тема (раздел) дисциплины, курсовая работа (проект), промежуточная аттестация

3 – Семестр

4 – Виды контактной работы и трудоемкость (в академических часах)

4.1 – Л (Лекции)

4.2 – Лекции в виде практической подготовки

4.3 – ПЗ (Практические занятия)

4.4 – Практические занятия в виде практической подготовки

4.5 – ЛР (Лабораторные работы)

4.6 – Лабораторные работы в виде практической подготовки

4.7 – ИКР (Иная контактная работа)

4.8 – КТО (Контроль теоретического обучения)

4.9 – КЭ (Контроль на экзамене)

5 – Контроль (в академических часах)

6 – Самостоятельная работа (в академических часах)

7 – Формы текущего контроля успеваемости

1	2	3	4									5	6	7
			4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9			
1	Обзор стандартов информационных систем		4				2						22	опрос
2	Уязвимости информационных систем		4				4						26	опрос
3	Атаки на информационные системы		4				4						26	опрос
4	Обеспечение информационной безопасности в		4				8						35.8	тест

	информационных системах											
5	Зачет с оценкой							0.2				
	Итого		16.0	0.0	18.0	0.0	0.2	0.0	0.0	109.8		

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Обзор стандартов информационных систем	Особенности анализа и управления безопасностью информационных систем. 2. Классификация стандартов по безопасности. Серия ISO/IEC 27000. Менеджмент информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США. Классы защищенности компьютерных систем.
2	Уязвимости информационных систем	Анализ угроз ИБ ресурсам информационной системы и причины их реализации. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы.
3	Атаки на информационные системы	Удаленные атаки на информационные системы. Типичные сценарии и уровни атак. Классические и современные методы, используемые нападающими для проникновения в информационные системы.
4	Обеспечение информационной безопасности в информационных системах	Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408. Разработка политики безопасности для информационных систем. Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление. Средства обеспечения информационной безопасности в информационных системах. Создание комплексной системы обеспечения безопасности информационных систем.

5.2. Лабораторные занятия

Наименование темы	Содержание темы
Обзор стандартов информационных систем	ISO/ IEC 27000 Использование антивирусных программ
Уязвимости информационных систем	Сканирование уязвимостей информационной системы
Уязвимости информационных систем	Сетевые вирусы

систем	
Атаки на информационные системы	Атака отказ в обслуживании
Обеспечение информационной безопасности в информационных системах	Создания защищенных средств связи объектов на основе стандартов ISO 7498-2, 17799, 15408.
Обеспечение информационной безопасности в информационных системах	Разработка политики и правил информационной безопасности

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в академических часах
1	Обзор стандартов информационных систем	Работа с лекционным материалом. Подготовка к лабораторным занятиям	22
2	Уязвимости информационных систем	Работа с лекционным материалом. Подготовка к лабораторным занятиям. Подготовка к опросу	26
3	Атаки на информационные системы	Работа с лекционным материалом. Подготовка к лабораторным занятиям. Подготовка к опросу	26
4	Обеспечение информационной безопасности в информационных системах	Работа с лекционным материалом. Подготовка к лабораторным занятиям. Подготовка к тесту	35.8

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе подготовки по дисциплине используется совокупность методов и средств обучения, позволяющих осуществлять целенаправленное методическое руководство учебно-познавательной деятельностью магистров, в том числе на основе интеграции информационных и традиционных педагогических технологий.

1. На занятиях используются методы активного обучения: лекция с заранее запланированными ошибками (лекция-провокация), лекция с разбором конкретных ситуаций, мозговой штурм. Рекомендуется использование информационных технологий при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа-средств при проведении лекционных и лабораторных занятий.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация по итогам освоения дисциплины: зачет с оценкой

Примерный перечень вопросов к зачету

На каких принципах основывается информационная безопасность информационных систем?

Опишите средства защиты используемые в информационных системах.

Сетевые вирусы.

Удаленные атаки на распределенные системы.
 Типичные сценарии и уровни атак.
 Классические и современные методы, используемые нападающими для проникновения в открытые системы.
 Специфика защиты ресурсов распределенных систем на примере интранета.
 Принципы создания защищенных средств связи объектов в распределенных системах.
 Средства обеспечения информационной безопасности в распределенных системах.
 Управление безопасностью распределенных систем.
 Организационно-правовые методы защиты распределенных систем.
 Аутентификация субъектов и объектов взаимодействия в распределенных системах.
 Системы анализа защищенности.
 Системы обнаружения и предотвращения вторжений
 Политика безопасности для информационных систем.
 Создание комплексной системы обеспечения безопасности для информационных систем.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/515435> (дата обращения: 19.04.2023).
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512268> (дата обращения: 19.04.2023).
3. Проектирование информационных систем : учебник и практикум для вузов / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук ; под общей редакцией Д. В. Чистова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 293 с. — (Высшее образование). — ISBN 978-5-534-15923-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/510287> (дата обращения: 13.04.2023).
4. Казарин, О. В. Программно- аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513300> (дата обращения: 19.04.2023).

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
2	Операционная система Linux	GNU-лицензия (GNU General Public License)
3	Система защиты информации от несанкционированного доступа Dallas Lock	Договор о сотрудничестве с образовательным учреждением 127-17-153/1.
4	http://www.e.lanbook.com	Электронная библиотечная система «Издательства Лань», тематические пакеты: инженерно-технические науки

5	http://irbis.amursu.ru/ www.	Электронно- библиотечная система Амурского государственного университета
6	https://urait.ru	Электронная библиотечная система «Юрайт». Фонд электронной библиотеки составляет более 4000 наименований и постоянно пополняется новинками, в большинстве своем это учебники и учебные пособия для всех уровней профессионального образования от ведущих научных школ с соблюдением требований новых ФГОСов.
7	http://www.intuit.ru/	Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки

в) профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	http://www.ict.edu.ru/about	Портал "Информационно- коммуникационные технологии в образовании" входит в систему федеральных образовательных порталов и на-целен на обеспечение комплексной информационной поддержки образования в области современных информационных и телекоммуникаци- онных технологий, а также деятельности по применению ИКТ в сфере образования.
2	https://reestr.minsvyaz.ru	Единый реестр российских программ для электронных вычислительных машин и баз данных. Реестр создан в соответствии со статьей 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации» в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из РФ, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки
3	www.elibrary.ru	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия по дисциплине проводятся в специальных помещениях, представляющих собой учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Все помещения, в которых проводятся занятия, соответствуют действующим противопожарным правилам и нормам.

Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно- библиотечным системам и к электронной информационно- образовательной среде университета.

Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду университета.

