МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Костромской государственный университет»

(КГУ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение безопасности процессов разработки информационных систем

Направление подготовки *09.04.02 Информационные системы и технологии*

Направленность «*Руководство разработкой программного обеспечения*»

Квалификация выпускника: *магистр*

Кострома
2023

Рабочая программа дисциплины **Обеспечение безопасности процессов разработки информационных систем** разработана в соответствии с Федеральным государственным образовательным стандартом 09.04.02 Информационные системы и технологии, утв. приказом Министерства образования и науки РФ от 19 сентября 2017 г. N 917

Разработал: Дружинина А.Г., к.т.н., доцент

Рецензент: Панин И.Г., профессор кафедры информационных систем и технологий, д.т.н., доцент

ПРОГРАММА УТВЕРЖДЕНА:
На заседании кафедры информационных систем и технологий:
Протокол заседания кафедры № «_6_» от _27.04.2023_г.

Заведующий кафедрой информационных систем и технологий:
Киприна Л.Ю., к.т.н., доцент

1. Цели и задачи освоения дисциплины

Цель дисциплины:

формирование у студентов теоретической и практической базы для обеспечении безопасности процессов разработки информационных систем в соответствии с российскими и международными стандартами.

Задачи дисциплины:

- формирование ключевых знаний и умений по обеспечению безопасности процессов разработки информационных систем;
- освоение методов управления организации безопасности процессов разработки информационных систем
- профессионально-трудовое воспитание обучающихся посредством содержания дисциплины и актуальных воспитательных технологий

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать:

- методологии управления проектами разработки программного обеспечения;
- методы и средства организации проектных данных;
- нормативно-технические документы (стандарты и регламенты), регулирующие безопасность процессов управления инфраструктурой коллективной среды разработки.

уметь:

- применять методологии управления проектами разработки программного обеспечения;
- применять безопасные методы и средства организации проектных данных;
- организовывать работу с использованием защищенных систем управления доступом и аутентификации пользователей.

владеть:

- навыками работы с инструментами и системами для обеспечения безопасности;
- навыками работы со средствами создания и ведения репозитория, учета задач, сборки и непрерывной интеграции, базы знаний;
- навыками организации процессов безопасного использования инфраструктуры.

освоить компетенции:

ПК-1 Способность проводить непосредственное руководство процессами разработки программного обеспечения, программно-техническими, технологическими и человеческими ресурсами

Код и содержание индикаторов компетенции:

ПК-1.2 Способен осуществлять управление программно-техническими и технологическими ресурсами

3. Место дисциплины в структуре ОП ВО

Дисциплина относится к части учебного плана, формируемой участниками образовательных отношений.

Изучение дисциплины является основой для освоения последующих дисциплин/практик, подготовке и защите ВКР.

4. Объем дисциплины (модуля)

4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	3
Общая трудоемкость в часах	108
Аудиторные занятия в часах, в том числе:	42
Лекции	14
Лабораторные занятия	28
Самостоятельная работа в часах	65,75
Форма промежуточной аттестации	Зачет

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	14
Лабораторные занятий	28
Зачет	0,25
Всего	42,25

5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

5.1 Тематический план учебной дисциплины

№	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекц.	Лаб.	
1	Введение в безопасность информационных систем	10/0,28	2		8
2	Анализ требований к безопасности информационных систем	18/0,5	2	2	14
3	Безопасность в процессе разработки информационных систем	18/0,5	2	6	10
4	Безопасность в эксплуатации информационных систем	18/0,5	2	6	10
5	Особенности безопасности при разработке распределенных информационных систем	18/0,5	2	2	14
6	Практические задания и проекты	26/0,72	4	12	10
	Итого:	**108/3**	**14**	**28**	**65,75**

5.2. Содержание:

Раздел 1. Введение в безопасность информационных систем

Определение понятий "безопасность", "информационная система", "риск". Роль безопасности информационной системы в современном мире. Виды угроз и атак на информационные системы

Раздел 2. Анализ требований к безопасности информационных систем

Методы анализа рисков. Требования к стандартам и сертификация в области безопасности информационных систем. Проектирование системы безопасности информационной системы

Раздел 3. Безопасность в процессе разработки информационных систем

Безопасность водопадной модели разработки. Безопасность инкрементальной и итеративной моделей разработки. Безопасность DevOps-моделей разработки

Раздел 4. Безопасность в эксплуатации информационных систем

Средства защиты информации. Протоколирование и мониторинг безопасности. Управление доступом и авторизация в информационных системах

Раздел 5. Особенности безопасности при разработке распределенных информационных систем

Безопасность веб-приложений и сервисов. Защита данных в облачных хранилищах. Безопасность мобильных приложений

Раздел 6. Практические задания и проекты

Проектирование системы безопасности для конкретной информационной системы. Разработка плана действий в случае инцидента информационной безопасности Анализ известных уязвимостей и их эксплуатация

6. Методические материалы для обучающихся по освоению дисциплины

6.1. Самостоятельная работа обучающихся по дисциплине

№ п/п	Раздел (тема) дисциплины	Задание	Часы	Методические рекомендации по выполнению задания	Форма контроля
6.1.1	Введение в безопасность информационных систем	Изучить материалы лекции и рекомендованной литературы.	8	Использовать материалы лекции и рекомендованной литературы	Устный опрос, заслушивание и обсуждение докладов
6.1.2	Анализ требований к безопасности информационных систем	Изучить материалы лекции и рекомендованной литературы.	14	Использовать материалы лекции и рекомендованной литературы	Устный опрос
6.1.3	Безопасность в процессе разработки информационных систем	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	10	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
6.1.4	Безопасность в эксплуатации информационных систем	Изучить материалы лекции и рекомендованной литературы Создание	10	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы

		отчета по лабораторной работе			
6.1.5	Особенности безопасности при разработке распределенных информационны х систем	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	14	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
6.1.6	Практические задания и проекты	Изучить материалы лекции и рекомендованной литературы. Создание отчетов по лабораторным работам	10	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работ

6.2. Тематика и задания для лабораторных занятий

6.2.1	Методы и средства анализа уязвимостей приложений и сетевых инфраструктур
6.2.2	Методы и средства анализа уязвимостей приложений и сетевых инфраструктур
6.2.3	Методы и средства тестирования безопасности приложений и инфраструктуры
6.2.4	Разработка и анализ требований к защите конфиденциальной информации
6.2.5	Управления доступом и аутентификация пользователей
6.2.6	Управления доступом и аутентификация пользователей
6.2.7	Проведение оценки угроз информационной безопасности и разработка мер по их предотвращению
6.2.8	Проведение оценки угроз информационной безопасности и разработка мер по их предотвращению
6.2.9	Анализ и диагностика проблем информационной безопасности процессов
6.2.10	Анализ и диагностика проблем информационной безопасности процессов
6.2.11	Координация действий команды разработки для обеспечения безопасности приложений
6.2.12	Координация действий команды разработки для обеспечения безопасности приложений
6.2.13	Организация обучения пользователей принципам безопасности информационных систем
6.2.14	Разработка мер по повышению осведомленности пользователей в вопросах обеспечения безопасности информационных систем

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022 (дата обращения: 23.06.2023).
2 Роберт Сикорд: Безопасное программирование на C и C++: учеб. пособие / Сикорд Роберт С. — Москва : Издательство: Вильямс, 2016 г. - 496 с. - ISBN: 978-5-8459-1908-3

Дополнительная литература

3. Сердюк В.А.Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных систем предприятий: учебное пособие / В.А.Сердюк ; Министерство образования и науки Российской Федерации, - Москва : Издательство: Вильямс, 2011. - 575 с. - ISBN:978-5-7598-0698-1
4. Adam Shostack Threat Modeling: Designing for Security: Учебное пособие / Adam Shostack. - Wiley, 2014. - 627 с. - ISBN:9781118822692

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

Информационно-образовательные ресурсы:

1. Федеральный портал «Российское образование»;

2. Сайт национальной сертификационной палаты

URL: http://www.nspru.ru/sertsoftware/

3. Сайт «Российского научно-технического центра информации по стандартизации, метрологии и оценке соответствия» (ФГУП «СТАНДАРТИНФОРМ»)

URL: http://www.gostinfo.ru/catalog/gostlist/

4. Материалы ISTQB

URL: https://www.rstqb.org/ru/istqb-downloads.html

5. Академия Microsoft: Верификация программного обеспечения

URL: https://www.intuit.ru/studies/courses/1040/209/info

Электронные библиотечные системы:

1. ЭБС Университетская библиотека онлайн - http://biblioclub.ru
2. ЭБС «ZNANIUM.COM» - http://znanium.com

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения всех видов занятий по дисциплине необходимо следующее материально-техническое обеспечение:

№ п/п	**Специализированные аудитории и классы**	Номер аудитории
1	Аудитория, оборудованная мультимедиа, для лекций	Е-326, Е-226
2	Компьютерные классы	Е-327, Е-320
	Кроме указанных аудиторий занятия могут проводится в лекционных аудиториях и компьютерных классах университета, оснащенных необходимым оборудованием с установленным указанным в данной РПД программным обеспечением	
Учебное оборудование		
	Персональные компьютеры, объединенные в локальную сеть, с выходом в Интернет	
№ п/п	**Программное обеспечение**	
1	MS Windows (Dream Spark Premium), Linux	Е-327
2	Офисный пакет	Е-327, Е-320