

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины

Введение в DevSecOps

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 26 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Целью курса «Введение в DevSecOps» является ознакомление студентов с основополагающими принципами защиты информации с помощью криптографических методов и примерами реализации этих методов на практике. Содействие формированию практических навыков построения систем защиты информации, применение математических методов в информационной безопасности электронного бизнеса.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы и является элективной дисциплиной. Она является частью ядра образования в системе обучения методам криптографической информации, состоящего из дисциплин «Криптографические методы защиты информации», «Теоретико-числовые методы в криптографии», «Программно-аппаратные средства обеспечения безопасности», «Криптографические протоколы». Изучение дисциплины базируется также на курсах «Алгебра», «Теория вероятностей», «Теория чисел».

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции	
ОПК-4 Обладает способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знать: - принципы безопасной разработки ПО; Уметь: - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; Владеть: - навыками работы с научно-технической литературой по тематике дисциплины.
Профессиональные компетенции	
ПК-4 Обладает способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать: - основные задачи DevSecOps; - методы анализа кода на безопасность; - переход от модели безопасности “защита периметра” к модели “построение безопасности процесса разработки”. Уметь: - использовать Docker контейнеры; - настраивать Kubernetes; алгоритмы на практике при решении задач криптографическими методами; - выявлять и устранять уязвимости на всех этапах от проектирования архитектуры до вывода в production;

	- интегрировать в CI/CD и использовать инструменты ИБ из следующих категорий: анализ возможных атак (Threat Modelling), анализ исходного кода на безопасность (SAST), применение защиты для REST-API внутри микро-сервисных приложений и на back-end, применение Web-Application Firewall (WAF), межсетевые экраны нового поколения (NGFW), ручное и автоматизированное тестирование на проникновение (Penetration Testing), мониторинг безопасности и реакция на события в ИБ (SIEM).
--	--

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **3** зачетные единицы, **108** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Вводная лекция. Термины, стандарты и методики ИБ. Рынок ИБ: основные тенденции и инструменты для мониторинга. Основные принципы обеспечения информационной безопасности стека приложений и инфраструктуры.	A	2						
2	Разбор уязвимостей OWASP Top 10 Web и OWASP Top 10 - REST API	A	2	4		1		4	Устный опрос по теме занятия
3	Безопасная разработка и уязвимости программного кода	A	2	2				2	Устный опрос по теме занятия
4	Введение в Docker Работа с данными и сетями в Docker. Сборка и оптимизация Docker-образов. Обеспечение безопасности в Docker контейнерах	A	4	4		1		4	Практическая работа №1
5	Основные компоненты Kubernetes.Обеспечение безопасности в	A	2	2		1		2	Практическая работа №2

	Kubernetes								
6	Обеспечение безопасности непрерывной интеграции и непрерывной доставки (CI/CD)	A	2	2				2	Устный опрос по теме занятия,
7	Анализ исходного кода на безопасность (SAST/DAST/IAST)	A	4	4		1		4	Практическая работа №3
8	Применение защиты для REST-API внутри микросервисных приложений и на back-end . Применение Web-Application Firewall (WAF) для защиты Web, REST API, Bot protection	A	2	2		1		2	Практическая работа №4
9	Современные средства периметральной безопасности сети	A	4	4				4	Устный опрос по теме занятия
10	Средства обнаружения действий внутреннего нарушителя	A	2	2				4	Устный опрос по теме занятия,
11	Мониторинг безопасности и реакция на события в ИБ (SIEM/SOAR)	A	2	2		1		4	Устный опрос по теме занятия
12	Моделирование угроз и тестирование на проникновение. Ручное и автоматизированное тестирование на проникновение (Penetration Testing)	A	2	2				4	Устный опрос по теме занятия
							0,3	5,7	зачет
	ИТОГО		30	30		6	0,3	41,7	

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины,

активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.
- MikTeX (свободно распространяемое ПО).

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используется:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»
<https://www.studentlibrary.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература:

1. Моуэт Э. Использование Docker - Москва: ДМК Пресс, 2017. - 354 с.
<https://www.studentlibrary.ru/book/ISBN9785970604267.html>
2. О. В. Казарин, И. Б. Шубинский Надежность и безопасность программного обеспечения: учебное пособие для вузов — Москва: Издательство Юрайт, 2022. — 342 с. <https://urait.ru/bcode/493262>

б) дополнительная литература

1. Краковский Ю. М. Методы защиты информации: учебное пособие для вузов — Санкт-Петербург: Лань, 2021. — 236 с. <https://e.lanbook.com/book/156401>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

доцент, к.ф.-м.н.

Якимова О. П.

**Приложение №1 к рабочей программе дисциплины
«Введение в DevSecOps»**

**Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине**

**1. Типовые контрольные задания или иные материалы,
необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,
характеризующих этапы формирования компетенций**

**1.1. Контрольные задания и иные материалы. Задания для самостоятельной
работы,используемые в процессе текущей аттестации
(ОПК-10)**

Практическая работа № 1.

Установить Docker на своем компьютере. Развернуть веб-сайт в докер-контейнере

Практическая работа № 2.

Получить бесплатный сертификат. Настроить Kubernetes

Практическая работа № 3.

Проверить сканерами код веб-сайта. Устранить найденные уязвимости.

Практическая работа № 4.

Настроить Firewall для защиты веб-сайта.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету (ОПК-10)

1. Термины, стандарты и методики ИБ.
2. Рынок ИБ основные тенденции и инструменты для мониторинга.
3. Основные принципы обеспечения информационной безопасности стека приложений и инфраструктуры.
4. Разбор уязвимостей OWASP Top 0 Web
5. Разбор уязвимостей OWASP Top 0 - REST API
6. Безопасная разработка в HTML/CSS и PHP
7. Безопасная разработка в Java/Node.js
8. Безопасная разработка в .NET
9. Безопасная разработка в Python
10. Основные компоненты Kubernetes
11. Обеспечение безопасности в Kubernetes
12. Обеспечение безопасности в ОС Linux и ОС Windows
13. Обеспечение безопасности CI/CD
14. Анализ исходного кода на безопасность (SAST/ DAST/IAST)
15. Применение защиты для REST-API внутри микро-сервисных приложений и на back-end Применение Web-Application Firewall (WAF) для защиты Web, REST API, Bot protection
16. Современные средства периметральной безопасности сети (NGFW/Sandbox)

17. Средства обнаружения действий внутреннего нарушителя (PAM и другие решения)
Мониторинг безопасности и реакция на события в ИБ (SIEM/SOAR)
18. Моделирование угроз и тестирование на проникновение. Ручное и автоматизированное тестирование на проникновение (Penetration Testing)

3. Описание процедуры выставления оценки

Оценка ответа на зачете в значительной степени зависит от работы студента в течение семестра.

Оценка **«зачтено»** ставится в случае, если выполняются 2 условия:

- 1) студент ответил на зачете на оценку, составляющую *не менее 60%* от максимально возможного количества баллов (6 баллов из 10).
- 2) студент выполнил тесты *не ниже, чем на оценку «удовлетворительно»* (схема выставления оценки по тестам приведена выше в настоящей Программе).

Баллы по ответу на зачете

Минимальный порог 6 баллов из 10.

- 10 баллов выставляется за полный ответ на поставленный вопрос с включением в содержание ответа лекции, материалов учебников, дополнительной литературы без наводящих вопросов.

- 8-9 баллов выставляется за полный ответ на поставленный вопрос в объеме лекции с включением в содержание ответа материалов учебников с четкими ответами на наводящие вопросы преподавателя.

- 6-7 баллов выставляется за ответ, в котором озвучено более половины требуемого материала, с положительным ответом на большую часть наводящих вопросов.

Оценка **«не зачтено»** ставится в случае, если выполняется хотя бы одно из условий:

- 1) студент ответил на зачете на оценку, составляющую *50% и меньше* от максимально возможного количества баллов (5 и меньше баллов из 10).
- 2) студент выполнил тесты *ниже, чем на оценку «удовлетворительно»* (схема выставления оценки по тестам приведена выше в настоящей Программе).

5 и менее баллов выставляется за ответ, в котором озвучено менее половины требуемого материала, не озвучено главное в содержании вопроса с отрицательными ответами на наводящие вопросы или студент отказался от ответа без предварительного объяснения уважительных причин.

Приложение №2 к рабочей программе дисциплины «Введение в DevSecOps»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Введение в DevSecOps» являются лекции. По большинству тем предусмотрены практические занятия.

Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях и более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы в течение обучения проводятся мероприятия текущей аттестации в виде контрольных работ. Также проводятся консультации по разбору заданий для самостоятельной работы, которые вызвали затруднения.

В конце семестра изучения дисциплины студенты сдают зачет.

Освоить вопросы, излагаемые в процессе изучения дисциплины, самостоятельно студенту крайне сложно. Это связано со сложностью изучаемого материала. Поэтому высокий уровень посещения аудиторных занятий является необходимым.