Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»
(МФТИ,Физтех)

УТВЕРЖДАЮ
Ректор МФТИ
д.т.н., физ.-мат. наук, профессор
_____ Д. В. Ливанов
«12» февраля 2024 г.

Дополнительная профессиональная программа повышения квалификации «AppSec: разработка безопасного программного обеспечения»

УГСН 09.00.00 Информатика и вычислительная техника

Направление подготовки 09.03.01 Информатика и вычислительная техника

ОКВЭД 62.02 - Деятельность консультативная и работы в области компьютерных технологий

Москва 2024

1. Общая характеристика программы

1.1.Цель реализации программы

Целью реализации дополнительной профессиональной программы повышения квалификации «AppSec: разработка безопасного программного обеспечения» является развитие навыков безопасной разработки, обеспечения безопасности инфраструктуры, поиску уязвимости.

1.2.Совершенствуемые и/или приобретаемые компетенции

Компетенции, формируемые и совершенствуемые в результате обучения, представлены в таблицах 1 и 2.

Таблица 1

№	Компетенции в соответствии с профессиональным стандартом 06.015 Специалист по информационным системам	Код компетенции
1	Способен принимать меры в случае обнаружения инцидентов информационной безопасности, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	ПК-1

Таблица 1

№	Компетенции в соответствии с направлением подготовки 09.03.01 Информатика и вычислительная техника	Код компетенции
1	Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2

1.3.Планируемые результаты обучения

Планируемые результаты обучения представлены в таблице 3.

Таблица 3

№	Уметь - знать	Профессиональный стандарт 06.015 Специалист по информационным системам
		Код компетенции
1	Знать: − принципы разработки безопасных приложений, методы безопасной разработки (актуальные стандарты и фреймворки безопасности); − современное устройство, этапы, участники и роли SSDLC; − методологии и стандарты OWASP, MITRE, NIST и др.; Уметь:	ПК-1

	– разрабатывать стратегию развития безопасной разработки в компании и дорожная карта развития; – работать с угрозами и рисками в процессе безопасной разработки; – анализировать программный код на наличие уязвимостей;	
		Направление подготовки 09.03.01 Информатика и вычислительная техника
		квалификация: бакалавр
	Знать: – инструменты анализа сторонних компонентов ПО (Software Composition Analysis); – методологии моделирования угроз, актуальные российские и зарубежные подходы к управлению рисками; – принципы обеспечения безопасности контейнерной инфраструктуры; – принципы обеспечения облачной безопасности; – подходы и технологии DevSecOps; – программы bug-bounty. Уметь: – настраивать CI/CD конвейер; – использовать SAST- и DAST-решения; – настраивать и использовать продукты PT Application Inspector, PT Black Box, PT Container Security, PT Application Firewall; – пользоваться Docker контейнерами.	ОПК-2

1.4.Категория обучающихся

Программа повышения квалификации предназначена для практикующих разработчиков, DevOps-инженеров и администраторов, тестировщиков, специалистов информационной безопасности.

1.5.Форма обучения

Очная с применением дистанционных образовательных технологий.
Программа может быть реализована в сетевой форме.

1.6.Объем программы

72 академических часа.

1.7.Режим обучения

18 недель.

2. Содержание программы

2.1.Учебный (тематический) план

Учебный (тематический) план программы представлен в таблице 4а.

Таблица 4а

№ п/п	Наименование разделов (модулей) и тем	Всего, час.	Лекции	Практич. работа	Самост. работа	Форма контроля
1.	**Модуль 1. Основы безопасной разработки программного обеспечения**	**20**	**7**	**7**	**6**	**Итоговый проект**
1.1	Введение в безопасную разработку	2	2	0	0	
1.2	Основные подходы и методологии безопасной разработки	3	0	2	1	Задание на самопроверку
1.3	Моделирование угроз, управление рисками и threat hunting	3	0	2	1	Задание на самопроверку
1.4	Основные практики и принципы безопасной разработки	3	3	0	0	
1.5	Роли и участники процесса безопасной разработки	2	2	0	0	
1.6	Стратегия развития безопасной разработки в компании и дорожная карта развития	4	0	3	1	Задание на самопроверку
	Итоговый проект 1 модуля	*3*	*0*	*0*	*3*	
2.	**Модуль 2. Технологии и практики безопасной разработки**	**29**	**9**	**12**	**8**	**Итоговый проект**
2.1	Знакомство с безопасным циклом разработки ПО	3	0	2	1	Задание на самопроверку
2.2	Security на этапах сбора требованиях и проектирования инфраструктуры	3	3	0	0	
2.3	Security на этапе написания кода. Статические анализаторы кода, линтеры, инструменты code style	3	0	2	1	Задание на самопроверку
2.4	Инструменты анализа сторонних компонентов ПО (Software Composition Analysis)	3	0	2	1	Задание на самопроверку

2.5	Динамический анализ уязвимостей и фаззинг тестирование	3	0	2	1	Задание на самопроверку
2.6	Реализация Pipeline	3	0	2	1	Задание на самопроверку
2.7	Предрелизные проверки безопасности	1	1	0	0	
2.8	Безопасность в продакшене	2	0	2	0	Задание на самопроверку
2.9	Программы BugBounty	1	1	0	0	
2.10	Security Culture	2	2	0	0	
2.11	Security Education	2	2	0	0	
	Итоговый проект 2 модуля	*3*	*0*	*0*	*3*	
3.	**Модуль 3. Безопасность окружения приложений**	**23**	**10**	**8**	**5**	**Итоговый проект**
3.1	Окружение приложений	2	0	2	0	Задание на самопроверку
3.2	Безопасность на уровне ОС	2	2	0	0	
3.3	Введение в Docker контейнеры	2	2	0	0	
3.4	Побеги из Docker	2	0	2	0	Задание на самопроверку
3.5	Безопасность Docker	3	0	2	1	Задание на самопроверку
3.6	Введение в Kubernetes	2	2	0	0	
3.7	Безопасность в Kubernetes	3	0	2	1	Задание на самопроверку
3.8	Обеспечение безопасности облачных сред	2	2	0	0	
3.9	Управление жизненным циклом контейнера и атаки на CICD	2	2	0	0	
	Итоговый проект 3 модуля	*3*	*0*	*0*	*3*	
	Итого:	72	26	27	19	

2.2.Учебная программа

Содержание учебной программы приведено в таблице 5.

Таблица 5

№ п/п	Наименование модуля, разделов и тем	Содержание обучения, наименование и тематика практических занятий (семинаров), самостоятельной работы	Объем, ак.час.
1	Основы безопасной разработки программного обеспечения	***Лекция*** 1. Введение в безопасную разработку 2. Основные практики и принципы безопасной разработки 3. Роли и участники процесса безопасной разработки ***Практическая работа*** 1. Основные подходы и методологии безопасной разработки 2. Моделирование угроз, управление рисками и threat hunting 3. Стратегия развития безопасной разработки в компании и дорожная карта развития Задания на самопроверку, итоговый проект ***Самостоятельная работа*** Самостоятельное выполнение заданий по теме лекции, изучение дополнительных материалов.	20
2	Технологии и практики безопасной разработки	***Лекция*** 1. Security на этапах сбора требованиях и проектирования инфраструктуры 2. Предрелизные проверки безопасности 3. Программы BugBounty 4. Security Culture 5. Security Education ***Практическая работа*** 1. Знакомство с безопасным циклом разработки ПО 2. Security на этапе написания кода. Статические анализаторы кода, линтеры, инструменты code style 3. Инструменты анализа сторонних компонентов ПО (Software Composition Analysis) 4. Динамический анализ уязвимостей и фаззинг тестирование 5. Реализация Pipeline 6. Безопасность в продакшене Задания на самопроверку, итоговый проект ***Самостоятельная работа*** Самостоятельное выполнение заданий по теме лекции, изучение дополнительных материалов.	29
3	Безопасность окружения приложений	***Лекция*** 1. Безопасность на уровне ОС 2. Введение в Docker контейнеры 3. Введение в Kubernetes 4. Обеспечение безопасности облачных сред	23

		5. Управление жизненным циклом контейнера и атаки на CICD ***Практическая работа*** 1. Окружение приложений 2. Побеги из Docker 3. Безопасность Docker 4. Безопасность в Kubernetes Задания на самопроверку, итоговый проект ***Самостоятельная работа*** Самостоятельное выполнение заданий по теме урока, изучение дополнительных материалов	
	Итого:		72

3. Формы аттестации и оценочные материалы

3.1.Формы аттестации

Оценка «зачтено» выставляется обучающемуся, если он показал всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «не зачтено» выставляется обучающемуся, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

Максимальная сумма, которую можно набрать, успешно выполнив все контрольные мероприятия, составляет 100 баллов. Для получения положительной оценки «зачтено» необходимо набрать не менее 75% за итоговый проект каждого модуля.

В зачетно-экзаменационную ведомость оценка выставляется в соответствии с нижеприведенной таблицей 6.

Таблица 6

Сумма баллов	Оценка
75-100	Зачтено
менее 75	Не зачтено

Составляющие процесса обучения, которые оцениваются в ходе обучения, и их вклад в итоговую оценку представлены в таблице 7.

Таблица 7

№ п/п	Основные показатели оценки	Вклад в итоговую оценку
1	Итоговый проект 1 модуля	33,3%
2	Итоговый проект 2 модуля	33,3%
3	Итоговый проект 3 модуля	33,3%

3.2.Оценочные материалы

Таблица 8

Наименование модуля, разделов и тем	Основные показатели оценки	Формы и методы контроля и оценки	Вес задания, %
Основы безопасной разработки программного обеспечения	ПК-1	Итоговый проект	33,3%
Технологии и практики безопасной разработки	ОПК-2	Итоговый проект	33,3%
Безопасность окружения приложений	ПК-1, ОПК-2	Итоговый проект	33,3%

Пример задания

1) Составить таблицу сравнения требований стандарта ГОСТ56939 и BSIMM14.
2) Составить базовую модель угроз для WEB-приложения.

Пример итогового проекта

Задание: Собрать безопасный пайплайн и провести необходимые проверки с разбором обнаруженных уязвимостей.

Описание:

Ваша задача - используя полученные знания и навыки, собрать пайплайн безопасной разработки в системе CI/CD, провести сканирония и проверки информационной безопасности, сформировать технический долг и разобрать уязвимости, обнаруженные в процессе работы.

Шаги выполнения:

1) Изучение проекта: Изучите проект, составьте его архитектуру и основные блоки приложения.

2) Составление пайплайна: Используя полученные знания и навыки, составьте пайплайн, в котором будут подключены проверки информационной безопасности в автоматическом режиме: то есть, вызываемые по триггеру.

3) Проведение сканирований и формирование отчета: Проведите несколько сканирований проекта и составьте подробный отчет о найденных уязвимостях, включая их описание, шаги для их воспроизведения, а также рекомендации по устранению. Отчет должен быть структурированным и понятным для технических и не технических специалистов.

4) Представление результатов: Подготовьте презентацию, в которой кратко изложите основные выводы вашего анализа, представьте найденные уязвимости в процессе сканирований и рекомендации по их устранению. Обсудите результаты с вашими коллегами и преподавателем.

5) Оценка: Оценка будет основана на полноте предоставленных результатов, а также на качестве представленного отчета и презентации.

4. Организационно-педагогические условия реализации программы

4.1.Учебно-методическое обеспечение и информационное обеспечение программы

4.1.1. Список литературы

Основная литература

1) Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542339 (дата обращения: 08.02.2024).
2) Белл Л., Брантон-Сполл М., Смит Р., Бэрд Дж. Безопасность разработки в agile-проектах. // O'Reilly, 448 с., 2018.
3) Роберт Сикорд. Безопасное программирование на C и C++ // Вильямс, 496 с., 2016 г.
4) Вехен Джульен. Безопасный DevOps. Эффективная эксплуатация систем. // СПб.: Питер, 2020. - 432 С.

Дополнительная литература

1. Michal Zalewski. The Tangled Web: A Guide to Securing Modern Web Applications. // No Starch Press, 320 pp, 2011
2. Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. // Wiley, 1996

4.1.2. Ресурсы информационно-телекоммуникационной сети "Интернет"

1. Google Project Zero — команда аналитиков безопасности, нанятая Google для поиска 0-day уязвимостей - https://googleprojectzero.blogspot.com/
2. OWASP Foundation — организация, которая классифицирует проблемы безопасности и создаёт методики их поиска и устранения - https://owasp.org/
3. MITRE ATT&CK - globally-accessible knowledge base of adversary tactics and techniques based on real-world observations - https://attack.mitre.org/

4.2.Описание материально-технической базы, необходимой для осуществления образовательного процесса по программе

Таблица 9

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Система дистанционного обучения	Лекция	Слушателю необходимо наличие доступа в сеть интернет, компьютер. Преподавателю курса необходимо наличие доступа администратора курса и оборудование для проведения дистанционных семинаров (вебинаров), качественный отказоустойчивый доступ в сеть интернет.
Система дистанционного обучения	Практические задания	Слушателю необходимо наличие доступа в сеть интернет, компьютер.

Система дистанционного обучения	Самостоятельная работа	Слушателю необходимо наличие доступа в сеть интернет, компьютер.

5. Организация образовательного процесса

В таблице 10 описаны образовательные технологии.

Таблица 10

№ п/п	Вид занятия	Форма проведения занятий	Цель
1	Лекция	Присутствие на видеолекциях	актуализация и систематизация теоретических знаний по дисциплине
2	Практические задания	Выполнение заданий на самопроверку и итоговых проектов	осознание связей между теорией и практикой, повышение степени понимания материала
3	Самостоятельная работа	Самостоятельное изучение дополнительных материалов и литературы.	получение дополнительных теоретических знаний

6. Составители программы

Орлова Лидия Сергеевна, методист Отдела сопровождения образовательных программ, Центр «Пуск», МФТИ

Зубцова Жанна Исхаковна, ведущий специалист Отдела сопровождения образовательных программ, Центр «Пуск», МФТИ

Газизова Светлана Григорьевна, руководитель направления построения процесса безопасной разработки Positive Technologies.

Согласовано,
Эксперт ОСОП

_____ Ж. И. Зубцова

Согласовано,
Заместитель директора (Центр дополнительного, дополнительного профессионального и онлайн-образования "Пуск")

_____ А. И. Рыбакова

Федеральное государственное автономное образовательное учреждение
высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»
(МФТИ, Физтех)

ВЫПИСКА ИЗ ПРОТОКОЛА № 7

заседания учебно-методического совета от 29 февраля 2024 года.

ПОВЕСТКА:

Рассмотрение дополнительных общеобразовательных и профессиональных программ.

Проректор по учебной работе А. А. Воронов.

СЛУШАЛИ: заместителя директора (Центр дополнительного, дополнительного профессионального и онлайн-образования "Пуск") А. И. Рыбакову о представлении дополнительных общеобразовательных и профессиональных программ (Центр «Пуск», МФТИ).

ПОСТАНОВИЛИ:
Рекомендовать к утверждению в установленном порядке дополнительную профессиональную программу повышения квалификации
«AppSec: разработка безопасного программного обеспечения».

Решение принято единогласно.

Форма проведения заседания: заочная.

Председатель УМС МФТИ А.А. Воронов

Ученый секретарь УМС МФТИ М.В. Березникова