Аннотация
рабочей программы дисциплины

Б1.В.04 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ СРЕДАХ»

Объем трудоемкости: 5 зач. ед.

Цели изучения дисциплины определены государственным образовательным стандартом высшего образования. Цели изучения дисциплины соотнесены с общими целями ООП ВО по направлению подготовки «Прикладная математика и информатика», в рамках которой преподается дисциплина.

Данная дисциплина ставит своей **целью** изучение истории появления информационной безопасности, отечественных и зарубежных регламентов, получение опыта эффективного использования принципов информационной безопасности в облачных средах, формирование профессиональных навыков управление доступом.

Процесс освоения данной дисциплины направлен на получения необходимого объема теоретических знаний, отвечающих требованиям ФГОС ВО и обеспечивающих успешное проведение магистром профессиональной деятельности, владение методологией формулирования и решения прикладных задач, а также на выработку умений применять на практике принципы информационной безопасности. Цели дисциплины соответствуют следующим формируемым компетенциям: ОПК-3,ОПК-1

Задачи дисциплины

Основные **задачи** дисциплины:

- идентификация угроз безопасности облачной информационной системы, а также обзор основных методов защиты информации в облачных системах;
- формирование навыков оценки возможных угроз безопасности в облачной системе;
- формирование навыков использования основных средств защиты информации в облачных технологиях.

Место дисциплины в структуре ООП ВО:

Курсы обязательные для предварительного изучения: Основы информационной безопасности, Методы программирования, Разработка приложений в интегрированных средах, Технологии программирования.

Дисциплины, в которых используется материал данной дисциплины: производственная практика, итоговая государственная аттестация; Технологии проектирования и сопровождения программных систем, Современные проблемы прикладной математики и информатики.

Результаты обучения (владение знаниями, умениями, опытом, компетенциями):

В результате освоения курса «Информационная безопасность в облачных средах» обучающийся должен обладать профессиональными компетенциями: ОПК-3,ОПК-1

ОПК-1	**Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий**
Знать	ОПК-1.1 Обладает фундаментальными знаниями в области математических и естественных наук, теории коммуникаций Знает современные методы анализа сетевых уязвимостей, методы и подходы к поиску и устранению уязвимостей. Методы и приемы формализации задач сетевой, серверной, программной безопасности.
Уметь	ОПК-1.2 Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты Планировать анализ исполнения требований программной безопасности в рамках установленной нормативной базы предприятия.
Владеть	ОПК-1.3 Имеет практический опыт работы с решением математических задач

и применяет его в профессиональной деятельности.
Методами и приемами формализации актуальных сетевых и программных уязвимостей для программных продуктов в облачных средах.

ОПК-3 **Способен проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования**

Знать ОПК-3.1 Знает методы теории алгоритмов, методы системного и прикладного программирования, основные положения и концепции в области математических, информационных и имитационных моделей.
Возможности современных и перспективных средств в области поиска и анализа сетевых, программных, серверных уязвимостей в рамках разработки программного обеспечения.
Методологии разработки программного обеспечения и технологии программирования, методы планирования и этапы выполнения работ

Уметь ОПК-3.2 Умеет соотносить знания в области программирования, интерпретацию прочитанного, определять и создавать информационные ресурсы глобальных сетей, образовательного контента, средств тестирования систем.
Проводить анализ исполнения требований сетевой и программной безопасности, учитывая современные описания CVE, оформляя отчеты по выявленным уязвимостям.
составлять технические описания и инструкции по результатам выявления уязвимостей.

Владеть ОПК-3.3 Имеет практический опыт применения разработки программного обеспечения и тестирования программных продуктов.
Правилами разработки регламентационной документации для решения задач по предотвращению программных уязвимостей разрабатываемого программного обеспечения.

Содержание и структура дисциплины

№	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Внеаудиторная работа
			Л	ЛЗ	СРС
1	2	3	4	5	7
1.	Введение в информационную безопасность	1	1	–	–
2.	Применение асимметричного шифрования.	16	4	2	10
3.	Безопасность контейнеров.	11	1	2	8
4.	Мониторинг, аудит, выявление аномалий и реагирование на инциденты в облачных средах.	12	1	1	10
5.	WAF, DDoS	14	2	2	10
6.	ИИ и социальная инженерия	15	1	–	14
7.	Правовые аспекты.	12	1	1	10
8	Популярные веб-уязвимости (языков программирования)	13	1	2	10
9	Популярные веб-уязвимости (инфраструктуры)	13	1	2	10
10	Популярные веб-уязвимости (фронтенд)	13	1	2	10

№	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Внеаудиторная работа
			Л	ЛЗ	СРС
1	2	3	4	5	7
11	Аутентификация и управление доступом: многофакторная аутентификация и IAM + OAuth/OIDC	17	1	2	14
12	Беспроводные сети	16	3	2	11
Промежуточная аттестация (ИКР)		0,3	–	–	–
Подготовка к экзамену		26,7			
Итого:		**180**	**18**	**16**	**117**

Курсовые проекты или работы: *не предусмотрены*

Интерактивные образовательные технологии, используемые в аудиторных занятиях: IT-методы, разбор конкретных ситуаций

Вид аттестации: 1 семестр – экзамен

Программу составили:

Тыщенко В.В., ведуший разработчик АО «Точка»
Прутский А.С., ст. преподаватель кафедры информационных технологий КубГУ