АННОТАЦИЯ рабочей программы дисциплины «Б1.О.2 КРИПТОГРАФИЯ И СЕТЕВАЯ БЕЗОПАСНОСТЬ»

Направление подготовки/специальность 10.03.01 Информационная безопасность

Объем трудоемкости: 5 зачетных единиц (180 часов, из них – 56,3 часа аудиторной нагрузки: лекционных 18 ч., лабораторных работ - 18 ч., 91 часов самостоятельной работы, 20 часа КСР, 0,3 часа ИКР, 26,7 подготовка к экзамену).

Цель дисциплины

Сформировать у студентов практические навыки применения криптографических протоколов для защиты каналов связи, аутентификации пользователей и обеспечения безопасности веб-приложений, сетевых сервисов и современных инфраструктур

Задачи дисциплины

1. Освоить архитектуру и настройку TLS/SSL, включая mTLS и анализ уязвимостей.
2. Научиться развёртывать и администрировать IPsec VPN в различных режимах.
3. Получить навыки настройки OpenVPN и WireGuard для защищённых каналов.
4. Изучить структуру и применение JWT-токенов, включая безопасное хранение и уязвимости.
5. Освоить протоколы OAuth 2.0 и OpenID Connect для федеративной аутентификации.
6. Научиться защищать веб-приложения от распространённых атак (OWASP Top 10).
7. Изучить криптографические протоколы для защиты электронной почты (PGP).
8. Освоить защиту сетевых сервисов: SSH, DNSSEC.
9. Изучить протоколы защиты беспроводных сетей (WPA3, 802.1X).
10. Познакомиться с современными трендами: Zero Trust, Service Mesh, постквантовая криптография.

Место дисциплины в структуре ООП ВО

Дисциплина «Криптография и сетевая безопасность» относится к Блоку 1 «Дисциплины (модули)» учебного плана, к обязательной части. В соответствии с рабочим учебным планом дисциплина изучается на 1 курсе в 1 семестре по очной форме обучения. Вид промежуточной аттестации: экзамен.

Дисциплина «Криптография и сетевая безопасность» представляет собой преддисциплину для таких дисциплин, как «Основы управления информационной безопасностью», «Безопасность в облачных средах».

Требования к уровню освоения дисциплины

Процесс освоения дисциплины направлен на формирование следующих компетенций: УК-2,ОПК-9,ОПК-10,ОПК-1.1

Код и наименование индикатора*	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	
ОПК-1.1: Знает требования к системе обеспечения информационной безопасности	Знает требования к системе обеспечени информационной безопасности
ОПК-1.2: Умеет разрабатывать проект технического задания на создание системы обеспечения информационной безопасности	Умеет разрабатывать проект технического задания н создание системы обеспечения информационно безопасности

ОПК-1.3: Владеет навыками формулирования и обоснования требований к системам обеспечения информационной безопасности	Владеет навыками формулирования и обоснования требований к системам обеспечения информационной безопасности
ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	
ОПК-5.1: Знает теорию и методологию научного исследования, основы проведения эксперимента и методы обработки экспериментальных данных	Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-5.2: Умеет обрабатывать и оформлять результаты научных исследований и оформлять научно-технические отчеты	Умеет применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-5.3: Владеет навыками подготовки научно-технических отчетов, обзоров, научных докладов и статей в области информационной безопасности	Владеет средствами криптографической и технической защиты информации для решения задач профессиональной деятельности

Структура дисциплины

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины.Разделы дисциплины, изучаемые в 1 семестре *(очная форма)*.

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Протокол TLS/SSL: архитектура, настройка, анализ	20	4		2	14
2.	Протокол IPsec: режимы, IKE, настройка	18	2		2	14
3.	VPN-протоколы: OpenVPN и WireGuard	20	2		4	14
4.	Защита веб-приложений: OWASP, JWT	22	4		4	14
5.	Протоколы аутентификации: OAuth 2.0, OpenID Connect	20	2		4	14
6	Защита сетевых сервисов: SSH, DNSSEC, беспроводные сети (WPA3)	*18*	*2*		*2*	*14*
7	Современные тренды: mTLS, Zero Trust, Service Mesh, постквантовая криптография	*15*	*2*		*0*	*13*
	ИТОГО по разделам дисциплины	133	18		18	97
	Контроль самостоятельной работы (КСР)	20				
	Курсовой проект	-				
	Промежуточная аттестация (ИКР)	0.3				
	Подготовка к экзамену	26,7				

	Общая трудоёмкость по дисциплине	180				

Примечание: Л – лекции, ПЗ – практические занятия / семинары, КСР – контрольные и самостоятельные работы, ЛР – лабораторные занятия, СРС – самостоятельная работа студента, Д-доклад, РГЗ – расчётно-графическое задание.

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: экзамен.

Автор:
доцент кафедры ВТ ФКТ и ПМ
Жук Арсений Сергеевич