Аннотация по дисциплине
Б1.В.04 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ СРЕДАХ»
2 курс 01.04.02, семестр 3 количество з.е. 3

Цель дисциплины: изучение истории появления информационной безопасности, отечественных и зарубежных регламентов, получение опыта эффективного использования принципов информационной безопасности в облачных средах, формирование профессиональных навыков управление доступом.

Задачи дисциплины:

1. идентификация угроз безопасности облачной информационной системы, а также обзор основных методов защиты информации в облачных системах;
2. формирование навыков оценки возможных угроз безопасности в облачной системе;
3. 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):

ПК-1	Способен находить и извлекать актуальную научно-техническую информацию из электронных библиотек, реферативных журналов и т.п.

ИПК-1.1 (D/29.7 Зн.8) Современный отечественный и зарубежный опыт в решении актуальных и значимых задач фундаментальной и прикладной математики ИПК-1.2 (A/01.6 Зн.1) Методы и приемы формализации задач фундаментальной и прикладной математики ИПК-1.3 (D/01.6 У.1) Проводить анализ исполнения требований при решении задач фундаментальной и прикладной математики ИПК-1.4 (A/01.6 У.1) Использовать методы и приемы формализации актуальных и значимых задач фундаментальной и прикладной математики ИПК-1.3 (D/01.6 У.1) Проводить анализ исполнения требований при решении задач фундаментальной и прикладной математики ИПК-1.4 (A/01.6 У.1) Использовать методы и приемы формализации актуальных и значимых задач фундаментальной и прикладной математики ИПК-1.5 (D/04.7 У.1) Планировать проектные работы, формулировать и решать актуальные	**Знает**	современные методы анализа сетевых уязвимостей, методы и подходы к поиску и устранению уязвимостей. Методы и приемы формализации задач сетевой, серверной, программной безопасности.
	Умеет	планировать анализ исполнения требований программной безопасности в рамках установленной нормативной базы предприятия.
	Владеет	методами и приемами формализации актуальных сетевых и программных уязвимостей для программных продуктов в облачных средах.

и значимые задачи фундаментальной и прикладной математики ИПК-1.7 (D/04.7 Тд.4) Распределение ролей и аналитических работ по участникам аналитической группы проекта при решении задач фундаментальной и прикладной математики ИПК-1.8 (D/04.7 Тд.5) Ответы на вопросы и предложения участников аналитической группы проекта при решении задач фундаментальной и прикладной математики		
ПК-2	Способен эффективно планировать необходимые ресурсы и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий, составлять на высоком уровне соответствующие технические описания и инструкции	
ИПК-2.1 (D/01.6 Зн.2) Возможности современных и перспективных средств разработки программных продуктов, технических средств в области математического моделирования и информационно-коммуникационных технологий ИПК-2.2 (D/01.6 Зн.3) Методологии разработки программного обеспечения и технологии программирования, методы планирования и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий ИПК-2.8 (D/01.6 У.1) Проводить анализ исполнения требований, эффективно планировать необходимые ресурсы и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий, составлять на высоком уровне соответствующие технические описания и инструкции ИПК-2.11 (D/29.7 У.2) Разрабатывать регламентные документы, составлять на высоком уровне соответствующие технические описания и инструкции ИПК-2.18 (D/01.6 Тд.4) Оценка и согласование сроков выполнения поставленных задач, планирование необходимых ресурсов и этапов выполнения работ в области математического моделирования и информационно-коммуникационных технологий,	**Знает**	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
	Умеет	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.
	Владеет	правилами разработки регламентационной документации для решения задач по предотвращению программных уязвимостей разрабатываемого программного обеспечения.

составление на высоком уровне соответствующих технических описаний и инструкций		
ПК-5	Способен составлять и публично представлять научные обзоры, рефераты и отчеты по тематике проводимых исследований, а также подготовить научную публикацию	
ИПК-5.7 (A/01.6 У.8) Применять лучшие мировые практики оформления программного кода, составлять и публично представлять отчеты по тематике проводимых исследований ИПК-5.12 (D/04.7 Тд.5) Ответы на вопросы и предложения участников аналитической группы проекта, представление соответствующих обзоров и документов	**Умеет**	применять лучшие мировые практики оформления программного кода для улучшения прозрачности и сетевой безопасности разрабатываемого продукта.

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.	9	3	2	4
3.	Безопасность контейнеров.	6	1	1	4
4.	Мониторинг, аудит, выявление аномалий и реагирование на инциденты в облачных средах.	6	1	1	4
5.	WAF, DDoS	6	1	1	4
6.	ИИ и социальная инженерия	7	1	–	6
7.	Правовые аспекты.	4	1	1	2
8	Популярные веб-уязвимости (языков программирования)	5	1	2	2
9	Популярные веб-уязвимости (инфраструктуры)	7	1	2	4
10	Популярные веб-уязвимости (фронтенд)	7	1	2	4
11	Аутентификация и управление доступом: многофакторная аутентификация и IAM + OAuth/OIDC	9	1	2	6
12	Беспроводные сети	5	1	–	4
Промежуточная аттестация (ИКР)		0,3	–	–	–
Подготовка к экзамену		35,7			
Итого:		**108**	**14**	**14**	**44**

Курсовые проекты или работы: *не предусмотрены*

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

Вид аттестации: 3 семестр – экзамен

Основная литература

1. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 05.06.2025). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

2. Щерба, Е. В. Противодействие сетевым атакам в локальных сетях : учебное пособие : [16+] / Е. В. Щерба, М. В. Щерба, А. А. Магазев ; ред. О. В. Маер ; Омский государственный технический университет. – Омск : Омский государственный технический университет (ОмГТУ), 2021. – 119 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 05.06.2025). – Библиогр. в кн. – ISBN 978-5-8149-3250-1. – Текст : электронный.

3. Ларина, Т. Б. Администрирование операционных систем. Управление системой : учебное пособие для студентов направлений подготовки «Информатика и вычислительная техника» и «Информационная безопасность» : / Т. Б. Ларина ; Российский университет транспорта (РУТ (МИИТ)), Институт управления и информационных технологий, Кафедра «Вычислительные системы и сети». – Москва : Российский университет транспорта (РУТ (МИИТ)), 2020. – 72 с. : ил., таб. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=703233 (дата обращения: 05.06.2025). – Библиогр. в кн. – Текст : электронный.

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