

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 20.06.2025 09:04:47
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Бюджетное учреждение высшего образования

Ханты-Мансийского автономного округа-Югры
"Сургутский государственный университет"

УТВЕРЖДАЮ
Проректор по УМР

Е.В. Коновалова

11 июня 2025г., протокол УМС №5

МОДУЛЬ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ

Основы защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Автоматики и компьютерных систем**

Учебный план bz090304-ПОКС-25-5.plx
09.03.04 ПРОГРАММНАЯ ИНЖЕНЕРИЯ
Направленность (профиль): Программное обеспечение компьютерных систем

Квалификация **Бакалавр**

Форма обучения **заочная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144

в том числе:

аудиторные занятия 16

самостоятельная работа 119

часов на контроль 9

Виды контроля на курсах:
экзамены 5

Распределение часов дисциплины по курсам

Курс	5		Итого	
	уп	рп		
Вид занятий				
Лекции	6	6	6	6
Лабораторные	10	10	10	10
Итого ауд.	16	16	16	16
Контактная работа	16	16	16	16
Сам. работа	119	119	119	119
Часы на контроль	9	9	9	9
Итого	144	144	144	144

Программу составил(и):

Ст.преп., Кривицкая М.А.

Рабочая программа дисциплины

Основы защиты информации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.04 Программная инженерия (приказ Минобрнауки России от 19.09.2017 г. № 920)

составлена на основании учебного плана:

09.03.04 ПРОГРАММНАЯ ИНЖЕНЕРИЯ

Направленность (профиль): Программное обеспечение компьютерных систем
утвержденного учебно-методическим советом вуза от 11.06.2025 протокол № 5.

Рабочая программа одобрена на заседании кафедры

Автоматики и компьютерных систем

Зав. кафедрой Запевалов А.В.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Освоение методов и средств защиты информации для обеспечения безопасной разработки и эксплуатации информационных систем.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.В.04
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Объектно-ориентированное программирование
2.1.2	Теория вероятностей
2.1.3	Операционные системы
2.1.4	Иностранный язык
2.1.5	Дискретная математика
2.1.6	Производственная практика, эксплуатационная практика
2.1.7	Теория языков программирования и методы трансляции
2.1.8	Программирование мобильных устройств
2.1.9	Технология разработки программного обеспечения
2.1.10	WEB-программирование
2.1.11	Инженерное проектирование
2.1.12	Основы WEB-технологий
2.1.13	Компьютерные сети
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Производственная практика, научно-исследовательская работа (CDIO)
2.2.2	Производственная практика, преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-7.1: Использует в проектной деятельности основные методы информационной безопасности

ОПК-3.2: Применяет алгоритмы и методы защиты информации при решении задач профессиональной деятельности

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	правовые основы защиты информации;
3.1.2	организационные, технические и программные методы защиты информации в современных системах и сетях;
3.1.3	основные стандарты, модели и методы шифрования;
3.1.4	основы инфраструктуры систем, построенных с использованием открытых и секретных ключей;
3.1.5	методы передачи конфиденциальной информации по каналам связи, методы установления подлинности передаваемых сообщений и хранимой информации.
3.2	Уметь:
3.2.1	применять известные методы и средства поддержки информационной безопасности в компьютерных системах;
3.2.2	проводить сравнительный анализ, выбирать подходящие методы и средства защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Введение в информационную безопасность					

1.1	Основные понятия информационной безопасности (ИБ). Актуальность и важность ИБ в веб-разработке. Угрозы ИБ в веб-приложениях. Классификация угроз. /Лек/	5	1	ОПК-3.2	Л1.2Л2.1Л3.1	
1.2	Идентификация и анализ основных угроз информационной безопасности для веб-приложений (OWASP Top 10). /Лаб/	5	1	ПК-7.1	Л1.3	
1.3	Анализ и защита от угроз информационной безопасности, не входящих в OWASP Top 10. /Ср/	5	20	ОПК-3.2	Л1.1 Э4 Э5	
	Раздел 2. Аутентификация и авторизация					
2.1	Методы аутентификации пользователей в веб-приложениях. Парольная аутентификация, многофакторная аутентификация (MFA), социальная аутентификация (OAuth). /Лек/	5	1	ПК-7.1	Л1.1Л2.1 Э6	
2.2	Реализация парольной аутентификации с использованием хэширования и солей (bcrypt, Argon2). /Лаб/	5	2	ОПК-3.2	Л3.1 Э4	
2.3	Интеграция MFA в веб-приложение (например, с использованием TOTP). /Лаб/	5	0	ОПК-3.2	Л1.3 Э1 Э3	
2.4	Методы аутентификации по сертификатам и ключам доступа (API keys). /Ср/	5	25	ПК-7.1	Л2.1 Э1 Э6	
	Раздел 3. Безопасная обработка данных и конфиденциальность					
3.1	Принципы безопасной обработки персональных данных. Законодательство о защите персональных данных (GDPR, ФЗ-152). Методы обеспечения конфиденциальности (шифрование, маскирование данных). /Лек/	5	1	ОПК-3.2	Л1.1Л2.1 Э2 Э5	
3.2	Использование шифрования для хранения конфиденциальных данных (например, паролей, номеров кредитных карт). /Лаб/	5	2	ПК-7.1	Л3.1 Э3 Э4	
3.3	Реализация маскирования данных для отображения конфиденциальной информации (например, частичное скрывание номера телефона). /Лаб/	5	0	ОПК-3.2	Л1.3 Э1 Э2	
3.4	Практические кейсы обеспечения защиты данных. /Ср/	5	25	ПК-7.1 ОПК-3.2	Л1.3 Э1 Э3	
	Раздел 4. Криптографические методы.					
4.1	Симметричное шифрование. Алгоритмы и стандарты. Ограничения. Область использования. /Лек/	5	1	ОПК-3.2	Л2.1Л3.1 Э2	
4.2	Реализация одного из симметричных алгоритмов шифрования. /Лаб/	5	1	ПК-7.1	Л3.1 Э2 Э4	
4.3	Ассиметричное шифрование. алгоритмы и стандарты. Ограничения. Область использования. /Лек/	5	1	ПК-7.1 ОПК-3.2	Л2.1 Э2	
4.4	Реализация одного из симметричных алгоритмов шифрования. /Лаб/	5	0	ПК-7.1	Л1.3Л3.1 Э2	
4.5	Библиотеки современных алгоритмов шифрования. /Ср/	5	25	ОПК-3.2	Л2.1 Э2	
	Раздел 5. Защита от CSRF (Cross-Site Request Forgery).					

5.1	Сущность CSRF-атак. Методы защиты от CSRF (использование CSRF-токенов, SameSite cookies). /Лек/	5	1	ПК-7.1	Л1.3 Э3 Э4	
5.2	Реализация CSRF-токенов для защиты от CSRF-атак. /Лаб/	5	0	ОПК-3.2	Л2.1 Э3 Э4	
5.3	Настройка SameSite cookies. /Лаб/	5	4	ПК-7.1 ОПК-3.2	Л1.3Л3.1 Э1 Э4	
5.4	методы защиты от CSRF-атак, особенно фокусируясь на использовании токенов (Synchronizer Tokens, Double Submit Cookie, Encrypted Token). /Ср/	5	24	ОПК-3.2	Л1.1Л2.1 Э7	
5.5	/Контр.раб./	5	0	ПК-7.1 ОПК-3.2		
5.6	/Экзамен/	5	9			

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Оценочные материалы для текущего контроля и промежуточной аттестации

Представлены отдельным документом

5.2. Оценочные материалы для диагностического тестирования

Представлены отдельным документом

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИОИ, 2018, электронный ресурс	1
Л1.2	Никифоров С. Н.	Методы защиты информации. Защита от внешних вторжений: учебное пособие для вузов	Санкт-Петербург: Лань, 2023, электронный ресурс	1
Л1.3	Раков А. С., Маслов О. Н., Губарева О. Ю., Почепцов А. О., Гуреев В. О.	Техническая защита информации: учебное пособие	Самара: ПГУТИ, 2020, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Шаньгин В.Ф.	Защита компьютерной информации. Эффективные методы и средства: учебное пособие	Саратов: Профобразование, 2017, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"	
Э1	Курс лекций Защита Информации
Э2	ПРАКТИЧЕСКАЯ КРИПТОГРАФИЯ: АЛГОРИТМЫ И ИХ ПРОГРАММИРОВАНИЕ http://citforum.ru/security/cryptography/cryptobook/
Э3	Технологии и продукты Microsoft в обеспечении информационной безопасности https://www.intuit.ru/studies/courses/600/456/info
Э4	NUIT Guide to Securing Web Applications — руководство по безопасной разработке и тестированию веб-приложений https://www.it.northwestern.edu/departments/cyberinfrastructure/
Э5	К.Митник Искусство быть невидимым https://www.litres.ru/book/kevin-mitnik/iskusstvo-byt-nevidimym-43004637/
Э6	Аутентификация в веб-приложениях: презентация https://lms.crafted.su/web-app-development/2023-1-ivt-2/docs/course/03-authentication/19-authentication/presentation/index.reveal.html#/
Э7	CSRF-угрозы в PHP: Как защититься и спать спокойно https://kurshub.ru/journal/blog/csrf-ugrozy-v-php-kak-zashhititsya-i-spat-spokojno/
6.3.1 Перечень программного обеспечения	
6.3.1.1	Интегрированная свободно-распространяемая среда разработки Dev-C++, Qt, CodeBlocks, Microsoft Visual Studio, Embarcadero C++ Builder или др.
6.3.1.2	Пакет программ Microsoft Office
6.3.1.3	Adobe Acrobat Reader
6.3.1.4	Операционные системы Microsoft
6.3.2 Перечень информационных справочных систем	
6.3.2.1	Информационно-правовой портал "Гарант" http://www.garant.ru/
6.3.2.2	Справочно-правовая система "Консультант-плюс" http://www.consultant.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (лабораторных занятий), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации оснащена: комплект специализированной учебной мебели, маркерная (меловая) доска, комплект переносного мультимедийного оборудования - компьютер, проектор, проекционный экран, компьютеры с возможностью выхода в Интернет и доступом в электронную информационно-образовательную среду. Обеспечен доступ к сети Интернет и в электронную информационную среду организации.