Бюджетное учреждение высшего образования
Ханты-Мансийского автономного округа-Югры
"Сургутский государственный университет"

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

16 июня 2022 г., протокол УС №6

МОДУЛЬ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ
Основы защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Автоматики и компьютерных систем**

Учебный план b090304-ПОСВТ-22-4.plx
09.03.04 ПРОГРАММНАЯ ИНЖЕНЕРИЯ
Направленность (профиль): Программное обеспечение компьютерных систем

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 48
самостоятельная работа 60
часов на контроль 36

Виды контроля в семестрах:
экзамены 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	32	32	32	32
В том числе инт.	16	16	16	16
Итого ауд.	48	48	48	48
Контактная работа	48	48	48	48
Сам. работа	60	60	60	60
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Программу составил(и):
нет, 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 16.06.2022 протокол № 6.

Рабочая программа одобрена на заседании кафедры
Автоматики и компьютерных систем

Зав. кафедрой к.т.н., доцент Запевалов А.В.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью преподавания дисциплины является раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе личной, корпоративной и национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.
1.2	- сформировать понятийный аппарат в области информационной безопасности и защиты информации, раскрыть базовые содержательные положения в области информационной безопасности и защиты информации;
1.3	- определить цели и принципы защиты информации, раскрыть современные доктрины информационной безопасности;
1.4	- установить факторы, влияющие на защиту информации, и структуры угроз защищаемой информации;
1.5	- установить назначение, сущность и структуру систем защиты информации и их компонентов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.04
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Алгоритмы и структуры данных
2.1.2	Объектно-ориентированное программирование
2.1.3	Программирование и основы алгоритмизации
2.1.4	Математические основы теории систем
2.1.5	Дискретная математика
2.1.6	Теория вероятностей
2.1.7	Иностранный язык
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Системы управления базами данных
2.2.2	Производственная практика, преддипломная практика
2.2.3	Производственная практика, научно-исследовательская работа (CDIO)

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.
3.3	**Владеть:**
3.3.1	навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;
3.3.2	навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации, алгоритмы постановки и проверки электронной цифровой подписи.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Примечание**
	Раздел 1. Ведение					
1.1	Источники и формы атак на информацию. Актуальность проблематики защиты информационных ресурсов. Классификация источников и форм атак на информационные ресурсы. Задержка, изменение, подмена сообщений. Способы получения парольной информации и прав доступа. Уязвимость ОС. Включение в программное обеспечение недокументированных функций /Лек/	7	2	ПК-7.1	Л1.1 Л1.2Л2.2 Л2.4 Э1 Э3 Э4	
1.2	Источники и формы атак на информацию, уязвимости программного обеспечения /Ср/	7	4	ПК-7.1	Л1.1 Л1.2Л2.2 Л2.4Л3.1 Э1 Э3 Э4	
	Раздел 2. Основы криптологии					
2.1	Криптографические протоколы. Основные понятия криптологии. Стойкость, защищенность, имитостойкость, аутентичность. Стеганография. Подстановочные и перестановочные шифры. Элементы криптографических протоколов, элементы криптосистем /Лек/	7	2	ОПК-3.2 ПК-7.1	Л1.3 Л1.4Л2.1 Л2.3 Э1 Э2	
2.2	Лабораторная работа № 1. Реализация собственных способов шифрования /Лаб/	7	4	ОПК-3.2	Л1.4Л2.3Л3.1 Э2	
2.3	Криптографические протоколы и их свойства /Ср/	7	10	ОПК-3.2 ПК-7.1	Л1.3 Л1.4Л2.1 Л2.3Л3.1 Э1 Э2	
	Раздел 3. Симметричные криптосистемы					
3.1	Блочные шифры. Модель криптосистемы с секретным ключом. Описание блочных алгоритмов DES, ГОСТ. Стандарт шифрования AES. Режимы применения блочных шифров /Лек/	7	2	ОПК-3.2	Л1.3 Л1.4Л2.1 Л2.3 Э1 Э3	
3.2	Лабораторная работа № 2. Симметричные блочные шифры /Лаб/	7	8	ОПК-3.2	Л1.4Л2.3Л3.1 Л3.2 Э2 Э3	
3.3	Потоковые шифры. Синхронные и самосинхронизирующиеся поточные криптоалгоритмы. Принципы построения. Стандарт безопасности GSM. Описание потоковых алгоритмов A5, RC4 /Лек/	7	2	ОПК-3.2	Л1.3 Л1.4Л2.1 Л2.3 Э1 Э3	
3.4	Лабораторная работа № 3. Симметричные потоковые шифры /Лаб/	7	8	ОПК-3.2	Л1.4Л2.3Л3.1 Л3.2 Э2	
3.5	Симметричные криптосистемы. Блочные и потоковые шифры, применение /Ср/	7	18	ОПК-3.2	Л1.3 Л1.4Л2.1 Л2.3Л3.1 Э1 Э2 Э3	
	Раздел 4. Асимметричные криптосистемы					

4.1	Асимметричные криптосистемы. Модель криптосистемы с открытым ключом. Однонаправленные преобразования. Криптосистема Эль-Гамаля. Открытое распределение ключей, система Диффи и Хеллмана. Система Ривеста-Шамира-Адлемана (RSA). Криптосистемы Меркля-Хеллмана и Хора-Ривеста /Лек/	7	2	ОПК-3.2	Л1.3 Л1.4Л2.1 Л2.3 Э1 Э3	
4.2	Лабораторная работа № 4. Асимметричные шифры /Лаб/	7	8	ОПК-3.2	Л1.4Л2.3Л3.1 Л3.2 Э2	
4.3	Асимметричные криптосистемы, реализация и применение /Ср/	7	16	ОПК-3.2	Л1.3 Л1.4Л2.1 Л2.3Л3.1 Э1 Э2 Э3	
	Раздел 5. Регулирование в сфере защиты информации					
5.1	Законодательные и правовые аспекты защиты информации. Информация и информационные ресурсы. Компьютерные преступления. Основные законы, регламентирующие законодательство в области защиты информации. Федеральный закон "Об информации, информатизации и защите информации". Закон Российской Федерации "О государственной тайне". Правовая защита ПО /Лек/	7	2	ПК-7.1	Л1.1 Л1.2Л2.2 Л2.4 Э1 Э3 Э4	
5.2	Стандарты безопасности. Роль стандартов. Классический подход к безопасности – "Оранжевая книга". Классы безопасности. Критерии оценки защищенности информационных систем. Международный стандарт ISO/IEC 15408-1999 и его российский аналог ГОСТ Р ИСО/МЭК 15408-2002. Международный стандарт информационной безопасности ISO 17799. Стандарт ITU-T Recommendation X.805 /Лек/	7	2	ПК-7.1	Л1.1 Л1.2Л2.2 Л2.4 Э1 Э3 Э4	
5.3	Политика безопасности. Определение политики. Цели информационной безопасности: конфиденциальность, целостность, пригодность. Уровни безопасности. Реализация политики безопасности. Реализация организационных и технических мер /Лек/	7	1	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Э1 Э3 Э4	
5.4	Требования к системам защиты информации. Общие требования. Организационные требования. Требования к техническому обеспечению. Требования к программному обеспечению. Требования по применению способов, методов и средств защиты. Требования к документированию /Лек/	7	1	ПК-7.1	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Э1 Э3 Э4	
5.5	Лабораторная работа № 5. Защита информации в базах данных и информационных системах /Лаб/	7	4	ОПК-3.2 ПК-7.1	Л1.4Л2.2 Л2.3Л3.1 Э2 Э3	

5.6	Регулирование в сфере защиты информации /Ср/	7	12	ОПК-3.2 ПК-7.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.2 Л2.4Л3.1 Э1 Э2 Э3 Э4	
	Раздел 6. Промежуточная					
6.1	/Экзамен/	7	36	ОПК-3.2 ПК-7.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3 Э4	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

представлено отдельным документом

5.2. Темы письменных работ

представлено отдельным документом

5.3. Фонд оценочных средств

представлено 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	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017, электронный ресурс	1
Л1.2	Коваленко Ю.И., Москвитин Г.И., Тараскин М.М.	Методика защиты информации в организациях: монография	Москва: Русайнс, 2016, электронный ресурс	1
Л1.3	Шаньгин В.Ф.	Защита компьютерной информации. Эффективные методы и средства: учебное пособие	Саратов: Профобразование, 2017, электронный ресурс	1
Л1.4	Бехроуз А., Берлин А. Н.	Криптография и безопасность сетей: Учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Нечаев В. И.	Элементы криптографии (Основы теории защиты информации)	М.: Высшая школа, 1999	15
Л2.2	Аверченков В. И., Рытов М. Ю.	Служба защиты информации. Организация и управление: Учебное пособие для вузов	Брянск: Брянский государственный технический университет, 2012, электронный ресурс	1
Л2.3	Аграновский А. В., Хади Р. А.	Практическая криптография. Алгоритмы и их программирование: учебное пособие	Москва: СОЛОН-ПРЕСС, 2009, электронный ресурс	1

Л2.4	Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2013, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Казаковцева Е. А.	Методы и средства защиты информации: учебно-методическое пособие	Сургут: Издательский центр СурГУ, 2009	20
Л3.2	Каторин Ю.Ф., Разумовский А.В., Спивак А.И.	Техническая защита информации: практикум	Санкт-Петербург: Университет ИТМО, 2013, 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	Your Private Network http://ypn.ru/
Э5	Run-Time Library Reference http://msdn.microsoft.com/en-us/library/aa249835(v=vs.60).aspx
Э6	Справочник C/C++ http://codenet.ru/cat/Languages/C-CPP/

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.