

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 20.06.2025 07:44:37
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 ДИСЦИПЛИН ПРОФИЛЬНОЙ НАПРАВЛЕННОСТИ

Управление информационной безопасностью

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Информатики и вычислительной техники		
Учебный план	b090302-БезопИнфСист-25-3.plx 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ Направленность (профиль): Безопасность информационных систем и технологий		
Квалификация	Бакалавр		
Форма обучения	очная		
Общая трудоемкость	3 ЗЕТ		
Часов по учебному плану	108	Виды контроля в семестрах:	
в том числе:		зачеты 6	
аудиторные занятия	48		
самостоятельная работа	60		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
	17 2/6			
Неделя	уп	рп	уп	рп
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Итого ауд.	48	48	48	48
Контактная работа	48	48	48	48
Сам. работа	60	60	60	60
Итого	108	108	108	108

Программу составил(и):

кандидат, Доцент, Лысенкова С.А.

Рабочая программа дисциплины

Управление информационной безопасностью

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)

составлена на основании учебного плана:

09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Направленность (профиль): Безопасность информационных систем и технологий

утвержденного учебно-методическим советом вуза от 11.06.2025 протокол № 5.

Рабочая программа одобрена на заседании кафедры

Информатики и вычислительной техники

Зав. кафедрой к.ф.-м.н., доцент, Лысенкова С.А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Формирование знаний об основных положениях теории и практики информационной безопасности; умений применять современные методы и средства защиты информации в вычислительных системах и сетях; компетенций в области разработки и использования средств защиты компьютерной информации в процессе ее обработки, передачи и хранения в информационных системах; овладение методами и технологиями разработки защищенных информационных систем; получение навыков в области анализа уязвимостей и рисков в информационных системах, а также разработки мер по их устранению; понимание принципов управления доступом к информационным ресурсам и методов аутентификации и авторизации пользователей у студентов профиля подготовки – Безопасность информационных систем и технологий.
-----	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.В.01
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Теория информационных процессов и систем
2.1.2	Сети ЭВМ
2.1.3	Безопасность баз данных
2.1.4	Разработка WEB-приложений
2.1.5	Основы информационной безопасности
2.1.6	Управление данными
2.1.7	Алгоритмы и языки программирования
2.1.8	Информационные технологии
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Информационная безопасность и защита информации
2.2.2	Методы и средства проектирования информационных систем
2.2.3	Управление IT-проектами
2.2.4	Разработка мобильных приложений
2.2.5	Нейронные сети
2.2.6	Тестирование и сопровождение программного обеспечения

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

ПК-5.1: Демонстрирует знания этапов, методов и технологий по созданию (модификации) информационных систем

ПК-5.2: Разрабатывает и модифицирует информационные системы

ПК-5.3: Сопровождает информационные системы

ПК-6.1: Демонстрирует знания этапов и методов разработки технической документации на продукцию в сфере информационных технологий и технических документов информационно-методического и маркетингового назначения

ПК-6.2: Разрабатывает техническую документацию на продукцию в сфере информационных технологий и технических документов информационно-методического и маркетингового назначения

ПК-6.3: Управляет технической информацией

ПК-16.1: Демонстрирует знания методов анализа защищенности информационных систем

ПК-16.2: Применяет на практике методы проведения анализа защищенности информационных систем

ПК-16.3: Проводит анализ защищенности информационных систем

ПК-17.1: Демонстрирует знания методов организации разработки, внедрения, и сопровождения информационной системы с учетом требования информационной безопасности

ПК-17.2: Применяет на практике методы организации разработки, внедрения, и сопровождения информационной системы с учетом требования информационной безопасности

ПК-17.3: Выполняет разработку, внедрение, и сопровождение информационной системы с учетом требования информационной безопасности

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	Основные принципы информационной безопасности. Законы и нормативные акты, регулирующие область информационной безопасности. Основные угрозы информационной безопасности и способы их предотвращения. Принципы управления рисками в области информационной безопасности.
3.2	Уметь:
3.2.1	Анализировать уязвимости и риски в информационных системах. Разрабатывать и внедрять политику информационной безопасности в организации. Организовывать проверки и аудит систем информационной безопасности. Планировать и реализовывать меры по защите информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Основы информационной безопасности					
1.1	Основные принципы защиты информации. Законы и нормативные акты в области информационной безопасности. Международные стандарты и методологии в области информационной безопасности. /Лек/	6	8	ПК-5.1 ПК-5.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.2	Определение уязвимостей информационных систем. /Лаб/	6	4	ПК-5.1 ПК-5.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.3	Основные принципы защиты информации. Законы и нормативные акты в области информационной безопасности. Международные стандарты и методологии в области информационной безопасности. Определение уязвимостей информационных систем. /Ср/	6	5	ПК-5.1 ПК-5.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 2. Управление рисками в информационной безопасности					
2.1	Управление рисками и разработка политики информационной безопасности. Методы оценки эффективности мер по защите информации. Расследование инцидентов информационной безопасности. Разработка плана восстановления после инцидентов информационной безопасности. /Ср/	6	5	ПК-5.2 ПК-5.3 ПК-6.1 ПК-6.2 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
2.2	Управление рисками и разработка политики информационной безопасности. Методы оценки эффективности мер по защите информации. Расследование инцидентов информационной безопасности. /Лек/	6	8	ПК-5.2 ПК-5.3 ПК-6.1 ПК-6.2 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	

2.3	Разработка плана восстановления после инцидентов информационной безопасности. /Лаб/	6	3	ПК-5.2 ПК-5.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
Раздел 3. Технологии и методы защиты информации						
3.1	Криптографические методы защиты информации. Сетевая безопасность и защита от кибератак. Физическая безопасность информационных систем. /Лек/	6	8	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
3.2	Управление доступом и идентификация в информационных системах. Практическое применение криптографических методов защиты информации. /Лаб/	6	3	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
3.3	Управление доступом и идентификация в информационных системах. Практическое применение криптографических методов защиты информации. /Ср/	6	5	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
Раздел 4. Аудит и контроль информационной безопасности						
4.1	Методы и техники аудита систем информационной безопасности. Использование инструментов и систем для контроля информационной безопасности. /Лек/	6	4	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	

УП: b090302-БезопИнфСист-25-3.plx

4.2	Мониторинг безопасности информационных систем. /Лаб/	6	2	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
4.3	Методы и техники аудита систем информационной безопасности. Использование инструментов и систем для контроля информационной безопасности. Мониторинг безопасности информационных систем. /Ср/	6	5	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
Раздел 5. Управление информационной безопасностью в организации						
5.1	Разработка стратегии информационной безопасности. Управление проектами безопасности. /Лек/	6	4	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
5.2	Планирование и управление проектами безопасности. /Лаб/	6	2	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	

5.3	Разработка стратегии информационной безопасности. Управление проектами безопасности. Планирование и управление проектами безопасности. /Ср/	6	5	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
Раздел 6. Работа над проектом						
6.1	Самостоятельная работа над проектом. /Лаб/	6	2	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
6.2	Самостоятельная работа над проектом. /Ср/	6	5	ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
6.3	/Контр.раб./	6	0	ПК-5.1 ПК-5.2 ПК-5.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4	
Раздел 7. Экзамен						

7.1	Зачет /Зачёт/	6	30	ПК-5.2 ПК-5.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-16.1 ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
-----	---------------	---	----	------------------------------------------------------------------------------------	-----------------------------------------	--

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	Анисимов А. А.	Менеджмент в сфере информационной безопасности: Учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020, электронный ресурс	1

Л1.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие	Москва: Издательский Центр РИО, 2020, электронный ресурс	1
------	---------------------------	----------------------------------------------------------------------------------------------------------	----------------------------------------------------------	---

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Шилов А.К.	Управление информационной безопасностью: Учебное пособие	Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2018, электронный ресурс	1
Л2.2	Партыка Т. Л., Попов И.И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2021, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Фомин Д. В.	Информационная безопасность: Учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика»	Саратов: Вузовское образование, 2018, электронный ресурс	1
Л3.2	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2021, электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	«SecurityLab» https://www.securitylab.ru
Э2	«WebGoat» https://owasp.org/www-project-webgoat/
Э3	«Damn Vulnerable Web Application» https://github.com/digininja/DVWA/ ,
Э4	«OWASP Juice Shop» https://owasp.org/www-project-juice-shop/

6.3.1 Перечень программного обеспечения

6.3.1.1	Операционная система Windows, Пакет программ Microsoft Office бесрочно
---------	------------------------------------------------------------------------

6.3.2 Перечень информационных справочных систем

6.3.2.1	СПС «КонсультантПлюс» - www.consultant.ru/
6.3.2.2	СПС «Гарант» - www.garant.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.
-----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------