МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ ГАГАРИНА Ю.А.»
(СГТУ имени Гагарина Ю.А.)
САРАТОВСКИЙ КОЛЛЕДЖ МАШИНОСТРОЕНИЯ И ЭНЕРГЕТИКИ

УТВЕРЖДАЮ
Директор СКМ и Э
СГТУ имени Гагарина Ю.А.
_____ В.В. Лобанов
«29» апреля 2021 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине

ОП.14 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

специальности

09.02.07 Информационные системы и программирование

Рабочая программа рассмотрена
на заседании ПЦМК ПОИ и ИТ
«28» 06 202 1 года, протокол № 8
Председатель ПЦМК _____ / Дмитриев /

Саратов, 2021

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫДИСЦИПЛИНЫ
ОП.14 Информационная безопасность

1.1. Область применения программы

Рабочая программа является частью программы подготовки специалистов среднего звена (ППССЗ) в соответствии с ФГОС по специальности СПО 09.02.07Информационные системы и программирование.

Рабочая программа может быть использованапри получении среднего общего образования для специальностей технического профиляпри получении среднего профессионального образования для специальностей укрупненной группы 09.00.00. Информатика и вычислительная техника.

1.2. Место дисциплины в структуре ППССЗ

Дисциплина ОП.14 Информационная безопасность относится к Профильным дисциплинам общеобразовательной подготовки.

Изучение данной дисциплины необходимо для освоения таких дисциплин как Технические средства информатизации, Компьютерные сети и т.д., она закладывает начальные знания и навыки оформления технической документации для сертификации и разработки программного обеспечения.

1.3. Цели и задачи дисциплины

Целью изучения дисциплины «Информационная безопасность» является ознакомление студентов с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей и, конечно, методов их применения

1.4. Требования **к результатам освоения дисциплины**

Изучение дисциплины направлено на формирование следующих компетенций:

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 9. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

ОК 11. Планировать предпринимательскую деятельность в профессиональной сфере

ПК 11.4. Реализовывать базу данных в конкретной системе управления базами данных.

ПК 11.5. Администрировать базы данных.

ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.

ПК 2.5. Производить инспектирование компонент программного обеспечения на предмет соответствия стандартам кодирования

В результате освоения дисциплины обучающийся **должен знать**:

- основные термины и понятия информационной безопасности
- принципы разграничения доступа к ресурсам
- Методы идентификации и аутентификации субъектов информационных систем
- Основные методы и средства криптографической защиты информации
- Методы контроля целостности информации
- Порядок хранения и распределения ключевой информации
- Методы защиты от разрушающих программных воздействий
- Методы защиты информации в компьютерных сетях

В результате освоения дисциплины обучающийся **должен уметь**:

- Применять методы разграничения доступа к ресурсам
- Применять методы идентификации и аутентификации субъектов информационных систем
- Применять и средства криптографической защиты информации
- Применять средства контроля целостности информации
- Применять средства защиты от разрушающих программных воздействий
- Применять средства защиты информации в компьютерных сетях

1.5. Количество часов на освоение программы дисциплины

Максимальной учебной нагрузки обучающегося 60 часов,

в том числе:

обязательной аудиторной учебной нагрузки обучающегося 60 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	*60*
Обязательная аудиторная учебная нагрузка (всего)	*60*
в том числе:	
лабораторные занятия	
практические занятия	*12*
контрольные работы	
курсовая работа (проект) (*если предусмотрено)*	
Самостоятельная работа обучающегося (всего)	-
Итоговая аттестация в форме *дифференцированного зачета 4 семестр*	

2.2. Тематический план и содержание учебной дисциплиныОП.14 Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
Раздел 1. Основные понятия и определения предмета защиты информации	1.1 Правовое обеспечение информационной безопасности. Организационно-распорядительная документация	**2**	1, 2	[1] глава 1
	1.2 Санкционированный и несанкционированный доступ. Угрозы безопасности и каналы реализации угроз	**2**		
	1.3. Основные принципы обеспечения информационной безопасности. Ценность информации Характеристика способов защиты компьютерной информации	2		[1] глава 2
Раздел 2. Разграничение доступа к ресурсам	2.1. Политики безопасности. Дискреционные политики безопасности	**2**	1, 2	
	2.2. Мандатные политики безопасности. Контроль доступа, базирующийся на ролях Политика безопасности сети	2		[1] глава 3
Раздел 3. Идентификация и аутентификация субъектов	3.1. Классификация подсистем идентификации и аутентификации субъектов Парольные системы идентификации и аутентификации пользователей	**2**	*1, 2*	
Раздел 4.. Методы и средства криптографической защиты	4.1 Принципы криптографической защиты информации	**2**	*1, 2*	[1] глава 4
	4.2. Традиционные симметричные криптосистемы. Шифрование методом замены (подстановки)	**2**		
	4.3. Шифрование методами перестановки. Шифрование методом гаммирования	2		
	4.4 Элементы криптоанализа Современные симметричные системы шифрования	2		
	4.6 Ассиметричные криптосистемы. Принципы асимметричного шифрования	**2**		
	4.7 Однонаправленные функции. Алгоритм шифрования RSA Сравнение симметричных криптосистем с асимметричными	**2**		
	ПР1 Симметричное шифрование			
	ПР2 Ассиметричное шифрование			

Раздел 5. Контроль целостности информации	5.1 Проблема обеспечения целостности информации	**2**	*1, 2*	[1] глава 5
	5.2. Функции хеширования и электронно-цифровая подпись	**2**		
	5.3. Инфраструктура открытых ключей PKI	2		
	ПР3 Контроль целостности информации			
Раздел 6. Хранение и распределение ключевой информации	6.1. Типовые схемы хранения ключевой информации. Защита баз данных аутентификации в ОС Windows NT и UNIX	**2**	*1, 2*	[1] глава 6
	6.2. Алгоритмы хеширования MD4, MD5. Иерархия ключевой информации. Распределение ключей	**2**		
	6.3. Протоколы безопасной удаленной аутентификации пользователей	2		
	ПР4 Хранение и распределение ключей			
Раздел 7. Защита от разрушающих программных воздействий	7.1 Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и РПВ	**2**		[1] глава 7
	7.2. Компьютерные вирусы как класс РПВ. Защита от РПВ. Изолированная программная среда	**2**	*1, 2*	
	ПР5 Антивирусная защита			
Раздел 8. Защита информации в компьютерных сетях	8.1. Основные угрозы и причины уязвимости сети Interne. Классификация типовых удаленных атак на интрасети	2	*1, 2*	[1] глава 8
	8.2. Ограничение доступа в сеть. Межсетевые экраны. Виртуальные частные сети (VPN)	2		
	8.3. Служба Active Directory Централизованный контроль удаленного доступа. Серверы аутентификации. Прокси-сервер	2		
	ПР6 Безопасность в компьютерных сетях			
	Зачет	**2**		
Всего:		**60**		

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

3.1. Требования к минимальному материально-техническому обеспечению обучения по дисциплине

Реализация рабочей программы дисциплины требует наличия учебной лаборатории информационных ресурсов;

Оборудование учебной лаборатории: доска учебная; рабочее место для преподавателя; рабочие места по количеству обучающихся

Технические средства обучения: компьютер с лицензионным программным обеспечением; мультимедиа проектор

Электронно-библиотечная система:
Доступ авторизированных пользователей через Интернет
- ЭБС «БиблиоТех (договор г/к «42-16ЭА (бессрочный) от 28.02.2011)

Доступ с компьютеров университетской сети
- Коллекция российских журналов в полнотекстовоми электронном виде, Elibrary.ruhttp://Elibrary.ru/projects/subscription/rus_titles_open.asp.
- ЭБС «Лань» http://e/lanbook.com/. Доступ к некоторым разделам ЭБС, в соответствии с Соглашением о сотрудничестве.

3.2. Учебно-методическое обеспечение обучения по дисциплине

Основные учебные издания:

1. Прохорова О.В. Информационная безопасность и защита информации : учебник для СПО / О.В.Прохорова. – 2-е изд., стер. – Санкт-Петербург : Лань, 2021 – 124 с.
2. Нестеров С.А. Основы информационной безопасности : учебник для вузов / С.А.Нестеров– Санкт-Петербург : Лань, 2021 – 324 с.
3. Кабанов А.С. Основы информационной безопасности : учеб. для студ. учреждений высш. Образования / А.С.Кабанов , А.Б.Лось, А.В.Сорокин. – Издательский центр «Академия», 2021 с. – 240 с.

Дополнительные учебные издания:

1. Партыка Т.Л., Попов И.И. Информационная безопасность. – М.:ФОРУМ: ИНФА-М, 2017.
2. Байбурин В.Б., Бровкова М.Б. и др. Введение в защиту информации - М.:ФОРУМ: ИНФА-М, 2014.
3. Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. - 3-е изд. (эл.). - М. :

БИНОМ, 2015. - (Программисту). - http://www.studentlibrary.ru/book/ISBN9785996329526.html

4. Электронное издание на основе: Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ.-3-е изд. (эл.).-Электрон. текстовые дан. (1 файл pdf : 482 с.).- М. : БИНОМ. Лаборатория знаний, 2015.- (Программисту).- Систем. требования: Adobe Reader XI ; экран 10". - ISBN 978-5-9963-2952-6.
5. Интеллектуальные системы защиты информации [Электронный ресурс] : учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html Электронное издание на основе: Интеллектуальные системы защиты информации: учеб. пособие/ В. И. Васильев. 2-е изд., испр. и доп. - М.: Машиностроение, 2013.- 172 с. - ISBN 978-5-94275-667-3.
6. Соколов А. В., Степанюк О. М. Защита от компьютерного терроризма. Справоч-ное пособие. - СПб.: БХВ - Петербург, Арлит, 2012.- 496с.:ил.

Методические указания для обучающихся по освоению дисциплины:

1. Методические указания для проведения практических работ по специальности 09.02.07 Информационная безопасность, преподаватель СКМ и Э Дмитриева Е.Н.,2021 г.

Интернет-ресурсы:

1 Система федеральных образовательных порталов Информационно - коммуникационные технологии в образовании. [Электронный ресурс] – режим доступа: http://www.ict.edu.ru

2 Сайт информационной поддержки ЕГЭ в компьютерной форме http://www.ege.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

4.1. Формы и методы контроля и оценки результатов обучения

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения	Р,П, У, Т
Применять методы разграничения доступа к ресурсам	Р,П, У, Т
Применять методы идентификации и аутентификации субъектов информационных систем	Р,П, У, Т
Применять и средства криптографической защиты информации	Д, П, У, Т
Применять средства контроля целостности информации	Р,П, У, Т
Применять средства защиты от разрушающих программных воздействий	Р,П,У, Т
Применять средства защиты информации в компьютерных сетях	Р,П, У, Т
Знания	
основные термины и понятия информационной безопасности	У, Т
принципы разграничения доступа к ресурсам	У, Т
Методы идентификации и аутентификации субъектов информационных систем	У, Т
Основные методы и средства криптографической защиты информации	У, Т
Методы контроля целостности информации	У, Т
Порядок хранения и распределения ключевой информации	У, Т
Методы защиты от разрушающих программных воздействий	У, Т
Методы защиты информации в компьютерных сетях	У, Т
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Д, У
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	У, П
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	У
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	У, УП, Р
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	УП, Р
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	У

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	У
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	У, Т
ОК 9. Использовать информационные технологии в профессиональной деятельности	У, П
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	У, П
ОК 11. Планировать предпринимательскую деятельность в профессиональной сфере	У, П
ПК 2.5. Производить инспектирование компонент программного обеспечения на предмет соответствия стандартам кодирования	Р, Т, УП
ПК 11.5. Администрировать базы данных.	Р, Т, УП
ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.	Р, Т, УП
ПК 11.4. Реализовывать базу данных в конкретной системе управления базами данных.	Р, Т, УП

У – устный ответ; Д – доклад; УП – упражнения; Э – экскурсия Т – тестирование; Лр – лабораторная работа; Р - расчётные задачи; П – презентация; К - конференция