Саратовский колледж машиностроения и энергетики
федерального государственного бюджетного образовательного учреждения
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

УТВЕРЖДАЮ
ДиректорСКМ и Э
СГТУ имени Гагарина Ю.А.
_____В.В. Лобанов
«__» июня 2018 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине

ОП. 14 Информационная безопасность

специальности

09.02.07Информационные системы и программирование

Рабочая программа рассмотрена
на заседании ПЦМК математики и ИТ
«07» июня 2018 года, протокол № 14

Председатель ПЦМК Дмитриева

Саратов 2018

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
- направления обеспечения информационной безопасности
- действия, приводящие к незаконному овладению. информацией
- виды тайн как объекта защиты
- компоненты и уровни системы информационной безопасности
- порядок защиты информационных активов
- основные положения политики информационной безопасности

В результате освоения дисциплины обучающийся должен уметь:

- определять виды активы организации
- определять ценность каждого актива организации
- формулировать требования к обеспечению сотрудниками защиты информации

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.17 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 защиты информации**	**12**		
Тема 1.1.	**Международные стандарты информационного обмена**	**6**	2	[1], Партыка Т.Л., Попов И.И. информационная безопасность. – М.:ФОРУМ: ИНФА-М, 2017. Глава 1
	1 Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации.	2		
	2 Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.	2		
	3 Требования к защите информации. Комплексность защиты информации: инструментальная, структурная, функциональная, временная.	2		
	Самостоятельная работа Ср№1. Доклад на тему «Защита информации, тайна»			
Тема 1.2.	**Понятия и угрозы.**	**6**		[2], Байбурин В.Б., Бровкова М.Б. и др. Введение в защиту информации - М.:ФОРУМ: ИНФА-М, 2014 Глава 1
	1 Основные понятия. Механизмы безопасности. Классы безопасности.	2	2	
	2 Основные определения и критерии классификации угроз	2		
	Практические работы Пр. №1. Криптографические методы защиты			
	Самостоятельная работа Ср№2. Выявление угроз и уязвимостей, каналов утечки информации			
Раздел 2.	**Государственная система информационной безопасности**	**8**	*2*	[1], Глава 2
Тема 2.1.	**Информационная безопасность в условиях функционирования в России глобальных сетей.**	**8**		
	1 Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации	2		
	2 Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности.	2		
	3 Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны	2		

	Практические занятия Пр. №2. Шифрование методом IDEA	2		
	Самостоятельная работа обучающихся Ср №3. Виды противников или «нарушителей». Понятие о видах вируса			
Раздел 3.	**Угрозы безопасности**	**4**	*2*	[1], Глава 3
Тема 3.1	**Угрозы безопасности.**			
	1 Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения	2		
	2 Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации	2		
Раздел 4.	**Теоретические основы методов защиты информационных систем**	**4**	*2*	[2], Глава 4
Тема 4.1.	**Теоретические основы методов защиты информационных систем**	**4**		
	1 Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности	2		
	2 Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла- ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей	2		
	Самостоятельная работа обучающихся Ср №4. Три вида возможных нарушений информационной системы.			
Раздел 5.	**Методы защиты средств вычислительной техники**	**6**	*2*	[1], Глава 4
Тема 5.1.	**Методы защиты средств вычислительной техники**	**6**		
	1 Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД.	2		
	2 Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.	2		
	Практические занятия Пр. №3. Криптосистема Эль-Гамаля	2		
	Самостоятельная работа обучающихся Ср №5. Виды защиты. Выявление угроз и уязвимостей			
Раздел 6.	**Основы криптографии**	**10**		
Тема 6.1.	**Основы криптографии**	**10**	*2*	[1], Глава 5
	1 Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи	2		
	2 Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты.	2		

	Криптанализ и атаки на криптосистемы.			
	Практические занятия Пр. №4. Шифрование заменой Пр. №5. Схема шифрования Вижинера. Пр. №6. Монофоническая замена	6		
	Самостоятельная работа обучающегося Ср. №6. Подготовка сообщения ««Криптоанализ», «Электронно-цифровая подпись»»			
Раздел 7.	**Архитектура защитных экономических систем**			
Тема 7.1.	**Системы менеджмента качества**	**4**	*2*	[2], Глава 5
	1 Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации.	2		
	2 Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.	2		
	Самостоятельная работа обучающегося Ср. №7. Подготовка сообщения «Стратегии защиты информации»			
Раздел 8.	**Алгоритмы и привязки программного обеспечения к аппаратному окружению**	**8**		
Тема 8.1	**Алгоритмы и привязки программного обеспечения к аппаратному окружению**	**4**	*2*	[2], Глава 6
	1 Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы. Временные метки и запись в реестр	2		
	2 Обеспечение требуемого количества запусков (trial version). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода	2		
	Самостоятельная работа обучающегося Ср. №8. Подготовка сообщения «Технология spyware»			
Тема 8.2.	**Алгоритмы безопасности в компьютерных сетях**	**4**	*2*	[1], Глава 7
	1 Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты.	2		
	2 Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.	2		
	Самостоятельная работа обучающегося Ср. №9. Сокрытие информации методом стеганографии	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. 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.

Дополнительные учебные издания:

1. 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 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.
2. 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.
3. 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 Казанцева Т.И.,2018 г.
2. Методические указания по организациисамостоятельной работы студентов по специальности 09.02.07 Информационная безопасность, преподаватель СКМ и Э Казанцева Т.И.,2018 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**
Уметь У.1. Определять виды активы организации – применять классификацию активов	Д, П, У, Т
У.2. Определять ценность каждого актива организации – применять документацию для определения ценности активов	Р,П, У, Т
У.3. Формулировать требования к обеспечению сотрудниками защиты информации - применять основные правила системы информационной безопасности; - применять основные способы защиты информации	Р,П,У, Т
Знать – и – й – и – в – и З.1. Основные термины и понятия информационной безопасности – основные термины информационной безопасности; – основные понятия информационной безопасности	У, Т
З.2. Направления обеспечения информационной безопасности – основные понятия угроз информационной безопасности; – основные направления обеспечения безопасности	У, Т
З.3. Действия, приводящие к незаконному овладению. информацией - источники права на доступ к информации; - ответственность за нарушение законодательства в информационной сфере	У, Т
З.4. Виды тайн как объекта защиты – врачебная тайна; – тайна связи; – нотариальная тайна; – адвокатская тайна; – тайна усыновления; – тайна страхования; – тайна исповеди	У, Т
З. 5. Компоненты и уровни системы информационной	У, Т

безопасности – личностный уровень; – уровень гражданского общества; – государственный уровень	
З.6. Порядок защиты информационных активов - защита государственной тайны; - защита коммерческой тайны; - защита банковской тайны	У, Т
З 7. Основные положения политики информационной безопасности - открытость политики; - равенство интересов; - приоритетность отечественного производителя; - социальная ориентация; - государственная поддержка	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