

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
«ГУБЕРНСКИЙ КОЛЛЕДЖ Г. СЫЗРАНИ»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

обще профессиональный цикл

программы подготовки специалистов среднего звена по специальности:

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Сызрань, 2020 г.

РАССМОТРЕНА

Предметной (цикловой) комиссией
общепрофессиональных и профессиональных
дисциплин

от 28 мая 2020 г. протокол № 10

Составитель: А.Л.Анищенко, методист строительного профиля ГБПОУ «ГК г. Сызрани»

Внутренняя экспертиза (техническая и содержательная): А.Л.Анищенко, методист
строительного профиля ГБПОУ «ГК г. Сызрани»

СОДЕРЖАНИЕ

Название разделов	стр.
1. Паспорт рабочей программы учебной дисциплины	4
2. Структура и содержание учебной дисциплины	7
3. Условия реализации программы учебной дисциплины	15
4. Контроль и оценка результатов освоения учебной дисциплины	17
5. Лист актуализации программы	18
6. Приложение 1 «Планирование учебных занятий с использованием активных и интерактивных форм и методов обучения»	

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем базовой подготовки.

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена: общепрофессиональный цикл.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

Базовая часть:

В результате освоения учебной дисциплины обучающийся должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

В результате освоения учебной дисциплины обучающийся должен знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

Вариативная часть:

- не предусмотрено

Содержание дисциплины должно быть ориентировано на подготовку студентов к освоению профессиональных модулей ППССЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и овладению профессиональными компетенциями (ПК):

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

В процессе освоения дисциплины у студентов должны формироваться общие компетенции (ОК):

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей;

ОК 09. Использовать информационные технологии в профессиональной деятельности;

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках;

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Всего - 57 часов, в том числе:

- всего во взаимодействии с преподавателем - 57 часа, в том числе:
- самостоятельная работа - 0 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной деятельности	Объем часов
Всего часов на учебную дисциплину	57
Самостоятельная работа	0
Всего во взаимодействии с преподавателем	57
из них:	
Теоретическое обучение	21
Лабораторные и практические занятия	18
Консультации	12
Экзамен	6
Промежуточная аттестация в форме экзамена	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности			
Тема 1.1. Основные понятия и задачи информационной безопасности	Содержание учебного материала	2	ОК 3, ОК 6, ОК 9, ПК.2.4
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.		
	Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.		
Тема 1.2. Основы защиты информации	Содержание учебного материала	5	ОК 3, ОК 6, ОК 9, ПК 2.4
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.		
	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.		
	Цели и задачи защиты информации. Основные понятия в области защиты информации.		
	Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.		
	Практические занятия	6	
	Определение объектов защиты на типовом объекте информатизации. Классификация защищаемой информации по видам тайны и степеням конфиденциальности. Построение модел интеграции информационной безопасности в основную деятельность организации		
Тема 1.3. Угрозы	Содержание учебного материала	4	ОК 3, ОК 6,

безопасности защищаемой информации.	Понятие угрозы безопасности информации		ОК 9, ПК.2.4
	Системная классификация угроз безопасности информации.		
	Каналы и методы несанкционированного доступа к информации		
	Уязвимости. Методы оценки уязвимости информации		
	Практическое занятие	4	
	Определение угроз объекта информатизации и их классификация		
	Определение методов оценки уязвимости информации		
Раздел 2. Методология защиты информации			
Тема 2.1. Методологические подходы к защите информации	Содержание учебного материала	2	ОК 3, ОК 6, ОК 9, ПК 2.4
	Анализ существующих методик определения требований к защите информации.		
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.		
	Виды мер и основные принципы защиты информации.		
	Практическое занятие	2	
	Оценка факторов, влияющих на требуемый уровень защиты информации		
Тема 2.2. Нормативно правовое регулирование защиты информации	Содержание учебного материала	4	ОК 3, ОК 6, ОК 9, ОК 10
	Организационная структура системы защиты информации		
	Законодательные акты в области защиты информации.		
	Российские и международные стандарты, определяющие требования к защите информации.		
	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации		
	Практическое занятие	2	
	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности		
Тема 2.3. Защита	Содержание учебного материала	4	ОК 3, ОК 6,

информации в автоматизированных (информационных) системах	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.		ОК 9, ОК 10
	Программные и программно-аппаратные средства защиты информации		
	Инженерная защита и техническая охрана объектов информатизации		
	Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.		
	Практическое занятие	4	
	Определение основных механизмов защиты информации		
	Выбор мер защиты информации для автоматизированного рабочего места		
	Консультации	12	
	Экзамен	6	
	Всего	57	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета информационной безопасности, лаборатории информационных технологий.

Оборудование учебного кабинета: персональный компьютер, проектор, презентации уроков, стенды, плакаты, методические пособия.

Оборудование лаборатории информационных технологий: посадочные места по количеству обучающихся; рабочее место преподавателя; мультимедийное оборудование.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением и мультимедиапроектор.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

1.2.1. Основные печатные источники:

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2015.

1.2.2. Дополнительные печатные источники:

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. - М: Горячая линия-Телеком, 2006. - 544 с.: ил. Допущено УМО ИБ.

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016.

4. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М. : КНОРУС, 2016.

5. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.

6. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2016.

7. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2015.

8. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - –М.: Академия. 2012.

9. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

10. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2012.

3.2.3 Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: <http://cyberrus.com/>
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

1.2.3. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
1	2
<p>уметь: классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации;</p>	<p>Оценка за контрольную работу; наблюдение и оценка результатов практических работ; Оценка защиты рефератов, докладов, сообщений; Оценка за оформление документации.</p>
<p>Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности;</p>	<p>Опрос; отчеты по самостоятельной работе; защиты рефератов, докладов, сообщений</p>

5. ЛИСТ АКТУАЛИЗАЦИИ ПРОГРАММЫ

Дата актуализации	Результаты актуализации

**ПЛАНИРОВАНИЕ УЧЕБНЫХ ЗАНЯТИЙ С ИСПОЛЬЗОВАНИЕМ
АКТИВНЫХ И ИНТЕРАКТИВНЫХ ФОРМ И МЕТОДОВ ОБУЧЕНИЯ**

№ п/п	Тема учебного занятия	Кол- во часов	Активные и интерактивные формы и методы обучения	Код формируемых компетенций
1	Понятие информации и информационной безопасности	1	Комбинированный урок Презентация	ПК 2.4 ОК 03, 06, 09, 10
2	Модель интеграции информационной безопасности в основную деятельность организации	1	Проблемная лекция презентация	ПК 2.4 ОК 03, 06, 09, 10
3	Виды мер и основные принципы защиты информации	1	Изучение нового материала Работа над понятием	ПК 2.4 ОК 03, 06, 09, 10