

**ФГОС СПО по специальности**

**10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

Требования к результатам освоения профессиональных компетенций по видам деятельности образовательной программы среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Вид деятельности	Требования к знаниям, умениям, действиям
<p>эксплуатация автоматизированных (информационных) систем в защищённом исполнении;</p>	<p>знания:</p> <ul style="list-style-type: none"> <li>– состава и принципов работы автоматизированных систем, операционных систем и сред;</li> <li>– принципов разработки алгоритмов программ, основных приемов программирования;</li> <li>– моделей баз данных;</li> <li>– принципов построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;</li> <li>– теоретических основ компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;</li> <li>– порядка установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;</li> </ul> <p>умения:</p> <ul style="list-style-type: none"> <li>– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;</li> <li>– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;</li> <li>– организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;</li> <li>– настраивать и устранять неисправности программно-</li> </ul>

	<p>аппаратных средств защиты информации в компьютерных сетях по заданным правилам;</p> <p>действия:</p> <ul style="list-style-type: none"> <li>– эксплуатация компонентов систем защиты информации автоматизированных систем, их диагностика, устранения отказов и восстановления работоспособности;</li> <li>– администрирование автоматизированных систем в защищенном исполнении;</li> <li>– установка компонентов систем защиты информации автоматизированных информационных систем.</li> </ul>
<p>защита информации в автоматизированных системах программными и программно-аппаратными средствами;</p>	<p>знания:</p> <ul style="list-style-type: none"> <li>– особенностей и способов применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</li> <li>– типовых моделей управления доступом, средств, методов и протоколов идентификации и аутентификации;</li> <li>– типовых средств и методов ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;</li> <li>– основных понятий криптографии и типовых криптографических методов и средств защиты информации;</li> </ul> <p>умения:</p> <ul style="list-style-type: none"> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</li> <li>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</li> <li>– проверять выполнение требований по защите информации от НСД при аттестации объектов информатизации по требованиям безопасности информации;</li> <li>– использовать типовые программные криптографические средства, в том числе электронную подпись;</li> <li>– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;</li> <li>– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;</li> </ul> <p>действия:</p> <ul style="list-style-type: none"> <li>– установка и настройка программных средств защиты информации;</li> <li>– тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;</li> <li>– учет, обработка, хранение и передачи информации, для которой установлен режим конфиденциальности;</li> </ul>

<p>защита информации техническими средствами.</p>	<p>знания:</p> <ul style="list-style-type: none"> <li>– физических основ, структуры и условий формирования технических каналов утечки информации, способов их выявления и методов оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;</li> <li>– номенклатуры и характеристик аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;</li> <li>– основных принципов действия и характеристик, порядка технического обслуживания, устранения неисправностей и организации ремонта технических средств защиты информации;</li> <li>– основных способов физической защиты объектов информатизации;</li> <li>– методик инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;</li> <li>– номенклатуры применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации;</li> </ul> <p>умения:</p> <ul style="list-style-type: none"> <li>– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;</li> <li>– применять технические средства для криптографической защиты информации конфиденциального характера;</li> <li>– применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;</li> <li>– применять инженерно-технические средства физической защиты объектов информатизации;</li> </ul> <p>действия:</p> <ul style="list-style-type: none"> <li>– выявление технических каналов утечки информации;</li> <li>– применение, техническое обслуживание, диагностика, устранение отказов, восстановление работоспособности, установка, монтаж и настройка инженерно-технических средств физической защиты и технических средств защиты информации;</li> <li>– проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;</li> <li>– проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.</li> </ul>
---	--

## **Требования к материально-техническому и программно-аппаратному обеспечению**

### *Кабинет информатики:*

рабочие места на базе вычислительной техники, подключенными к локальной вычислительной сети и сети «Интернет», учебным сетевым программным обеспечением, обучающим программным обеспечением.

### *Лаборатория электроники и схемотехники:*

учебно-лабораторные стенды для освоения типовых схемотехнических решений; контрольно-измерительная аппаратура для измерения временных характеристик, амплитуды и формы сигналов; генераторами сигналов с заданными параметрами;

### *Лаборатория электротехники, электроники и схемотехники:*

учебно-лабораторные стенды;  
контрольно-измерительная аппаратура для измерения частотных свойств, форм и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов;

### *Лаборатория информационных технологий, программирования и баз данных:*

рабочими местами на базе вычислительной техники по одному рабочему месту на обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»; программным обеспечением сетевого оборудования; обучающим программным обеспечением;

### *Лаборатория сетей и систем передачи информации:*

рабочие места на базе вычислительной техники; стендами сетей передачи данных; структурированная кабельная система; эмулятор (эмуляторы) активного сетевого оборудования; программное обеспечение сетевого оборудования;

### *Лаборатория программных и программно-аппаратных средств защиты информации:*

антивирусные программные комплексы, программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности; программные и программно-аппаратные средства обнаружения вторжений; средства уничтожения остаточной информации в запоминающих устройствах; программные средства выявления

уязвимостей в АС и СВТ; программные средства криптографической защиты информации; программные средства защиты среды виртуализации;

*Лаборатория технических средств защиты информации:*

аппаратные средства аутентификации пользователя, средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок; средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.); стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов.

## УЧЕБНАЯ ЛИТЕРАТУРА

№ п/п	Позиция Перечня	Учебные материалы	Год издания	Издательство
	<b>08.00.00 Техника и технологии в строительстве</b>			
	ОПД	Барабанщиков Ю.Г. Строительные материалы и изделия (ППССЗ)	2014 (4-ое изд. ст.)	ОИЦ «Академия»
		Куликов О.Н., Ролин Е.И. Охрана труда в строительстве (ППКРС)	2014 (10-ое изд. ст.)	ОИЦ «Академия»
		Гусарова Е.А., Митина Т.В., Полежаев Ю.О., Тельной В.И. Основы строительного черчения (ППКРС)	2012 (1-ое изд.)	ОИЦ «Академия»
	<b>Общепрофессиональные дисциплины</b>	Гохберг Г.С., Зафиевский А.В., Короткин А.А. Информационные технологии	2014 (2-ое изд. ст.)	ОИЦ «Академия»
		Игошин В.И. Теория алгоритмов	2013 (1-ое изд.)	ОИЦ «Академия»
		Игошин В.И. Элементы математической логики	2016 (2-ое изд. ст.)	ОИЦ «Академия»
		Каганов В.И. Прикладная электроника	2015 (1-ое изд.)	ОИЦ «Академия»
		Келим Ю.М. Вычислительная техника	2015 (10-ое изд. ст.)	ОИЦ «Академия»
		Сенкевич А.В. Архитектура ЭВМ и вычислительные системы	2014 (1-ое изд.)	ОИЦ «Академия»
15.	<b>Техник по защите информации</b>	Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности	2015 (1-е изд.)	ОИЦ Академия
		Бубнов А.А., Бубнов С.А., Пржегорлинский В.Н. Программно-аппаратные и технические средства	2015 (1-е изд.)	ОИЦ Академия

		защиты информации		
		Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности	2015 (1-е изд.)	ОИЦ Академия