Специальность по ТОП-50

**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 |
| эксплуатация автоматизированных (информационных) систем в защищённом исполнении; | знания:  – состава и принципов работы автоматизированных систем, операционных систем и сред;  – принципов разработки алгоритмов программ, основных приемов программирования;  – моделей баз данных;  –принципов построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;  – теоретических основ компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;  *–* порядка установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;  умения:  – обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;  – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;  – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;  *–* настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;  действия:  – эксплуатация компонентов систем защиты информации автоматизированных систем, их диагностика, устранения отказов и восстановления работоспособности;  – администрирование автоматизированных систем в защищенном исполнении;  – установка компонентов систем защиты информации автоматизированных информационных систем. |
| защита информации в автоматизированных системах программными и программно-аппаратными средствами; | знания:  – особенностей и способов применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;  – типовых моделей управления доступом, средств, методов и протоколов идентификации и аутентификации;  – типовых средств и методов ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;  – основных понятий криптографии и типовых криптографических методов и средств защиты информации;  умения:  – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;  – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;  – проверять выполнение требований по защите информации от НСД при аттестации объектов информатизации по требованиям безопасности информации;  – использовать типовые программные криптографические средства, в том числе электронную подпись;  – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;  – 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;  действия:  – установка и настройка программных средств защиты информации;  – тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;  –учет, обработка, хранение и передачи информации, для которой установлен режим конфиденциальности; |
| защита информации техническими средствами. | знания:  – 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;  – номенклатуры и характеристик аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;  – основных принципов действия и характеристик, порядка технического обслуживания, устранения неисправностей и организации ремонта технических средств защиты информации;  – основных способов физической защиты объектов информатизации;  – методик инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;  – номенклатуры применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации;  умения:  – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;  – применять технические средства для криптографической защиты информации конфиденциального характера;  – применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;  – применять инженерно-технические средства физической защиты объектов информатизации;  действия:  – выявление технических каналов утечки информации;  – применение, техническое обслуживание, диагностика, устранение отказов, восстановление работоспособности, установка, монтаж и настройка инженерно-технических средств физической защиты и технических средств защиты информации;  – проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;  – проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. |

# 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; программные 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 (виброаккустическому) 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** |
|  | **08.00.00 Техника и технологии в строительстве** | | | |
|  | 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» |
|  | **Общепрофессиональные дисциплины** | 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.** | **Техник по защите информации** | 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 защиты информации | 2015  (1-е изд.) | ОИЦ Академия |
| Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности | 2015  (1-е изд.) | ОИЦ Академия |