МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ САМАРСКОЙ ОБЛАСТИ

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

УТВЕРЖДЕНО

Приказ ГБПОУ «ГК г. Сызрани»
от « 30 » мая 2024 г. № 268-о

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП. 01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

общепрофессиональный цикл

основной образовательной программы по специальности:

10.02.05 Обеспечение информационной безопасности автоматизированных систем

ЭП

C=RU, OU=Директор, O="ГБПОУ ""ГК г. Сызрани""", CN=Павел Салугин, E=gk_szr@samara.edu.ru
00d644d85759a06e75
2024-06-15 11:30:36

Сызрань, 2024 г.

РАССМОТРЕНА

Предметной (цикловой) комиссией
общепрофессиональных и
профессиональных циклов
от « 23 » мая 2024г. протокол № 9

Составитель: М.В. Киреева, преподаватель дисциплины ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГБПОУ «ГК г. Сызрани»

Внутренняя экспертиза (техническая и содержательная): И.Н. Ежкова, методист ГБПОУ «ГК г. Сызрани»

Рабочая программа разработана в соответствии с требованиями к оформлению, установленными в ГБПОУ «ГК г. Сызрани».

Содержание программы реализуется в процессе освоения студентами основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП. 01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины (далее – УД) является частью основной образовательной программы подготовки специалистов среднего звена по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанной в соответствии с ФГОС.

Рабочая программа составляется для очной формы обучения.

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

1.3. Цель и планируемые результаты освоения дисциплины

По результатам освоения дисциплины ОП.01 Основы информационной безопасности у обучающихся должны быть сформированы образовательные результаты в соответствии с ФГОС СПО:

Код ПК, ОК	Умения	Знания
ПК 2.4, ОК.03, ОК.06, ОК.09, ОК.10	классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации.	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;

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, применять стандарты антикоррупционного поведения;

ОК 09. Использовать информационные технологии в профессиональной деятельности;

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

Вариативная часть:

По результатам освоения дисциплины ОП.01 Основы информационной безопасности у обучающихся должны быть сформированы вариативные образовательные результаты, ориентированные на выполнение требований рынка труда.

С целью реализации требований профессионального стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации и квалификационных запросов предприятий/ регионального рынка труда, обучающийся должен*:*

иметь практический опыт:

– текущий, в том числе автоматизированный контроль функционирования СССЭ с установленными показателями

уметь:

– проводить текущий контроль показателей и процесса функционирования СССЭ

знать:

– организационные меры по защите информации.

1.4. Количество часов на освоение программы учебной дисциплины:

Всего - 77 часов, в том числе:

- всего во взаимодействии с преподавателем - 74 часа, в том числе:

теоретическое обучение – 19 часов

лабораторные и практические занятия – 43 часа

консультации – 6 часов,

промежуточная аттестация – 6 часов

- самостоятельная работа - 3 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной деятельности	Объём часов
Суммарная учебная нагрузка во взаимодействии с преподавателем	**74**
Самостоятельная работа	**3**
Объем образовательной программы	77
в том числе:	
теоретическое обучение	19
лабораторные работы	не предусмотрено
практические занятия	43
контрольная работа	не предусмотрено
консультации	6
Промежуточная аттестация	6
Самостоятельная работа	3
Промежуточная аттестация в форме	Экзамен

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
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.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	6	
	1 Исследование и настройка межсетевого экрана		
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	**6**	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.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**12**	
	2	Определение объектов защиты на типовом объекте информатизации		
	3	Классификация защищаемой информации по видам тайны и степеням конфиденциальности		
	4	Построение модели интеграции информационной безопасности в основную деятельность организации		
Самостоятельная работа: Подготовка отчетов по практическим занятиям			**3**	
Тема 1.3. Угрозы безопасности защищаемой информации.	**Содержание учебного материала**		**3**	ОК 3, ОК 6, ОК 9, ПК.2.4
	Понятие угрозы безопасности информации			
	Системная классификация угроз безопасности информации.			
	Каналы и методы несанкционированного доступа к информации			
	Уязвимости. Методы оценки уязвимости информации			
	Лабораторные работы		Не предусмотрено	
	Практическое занятие		**9**	
	5	Определение угроз объекта информатизации и их классификация		
	6	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.		
	Лабораторные работы	Не предусмотрено	
	Практическое занятие	**8**	
	7 Оценка факторов, влияющих на требуемый уровень защиты информации		
	8 Работа с программой вскрытия паролей AZRP		
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание учебного материала**	**3**	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		
	Лабораторные работы	Не предусмотрено	
	Практическое занятие	**4**	
	9 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности		
Тема 2.3. Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала**	**3**	ОК 3, ОК 6, ОК 9, ОК 10
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.		
	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.		

	Лабораторные работы		Не предусмотрено	
	Практическое занятие		**4**	
	10	Определение основных механизмов защиты информации		
	11	Выбор мер защиты информации для автоматизированного рабочего места		
		Консультации	**6**	
		Экзамен	**6**	
		Всего	**77**	

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

Основные источники:

Для преподавателей:

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

2. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

3. Журналы Защита информации. Инсайд: Информационно-методический журнал

4. Информационная безопасность регионов: Научно-практический журнал

Для обучающихся:

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

2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

3. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

Дополнительные источники:

Для преподавателей:

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.

Для обучающихся:

1. 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.

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

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

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

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

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

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

Электронные ресурсы:

Для преподавателей

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/

Для обучающихся:

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» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	Критерии оценки	Формы и методы контроля и оценки результатов обучения
уметь: классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации	Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Фронтальный опрос, беседа.
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;	Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.	Экспертное наблюдение в процессе практических занятий, ответ на экзамене

5. ЛИСТ АКТУАЛИЗАЦИИ ПРОГРАММЫ

Дата актуализации	Результаты актуализации

ПРИЛОЖЕНИЕ 1

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	Формируемые ОК, ПК, знания и умения
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

ПРИЛОЖЕНИЕ 2

Сопоставление требований профессионального стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного Приказом Минтруда России от 3 ноября 2016 г. № 608н, и образовательных результатов УД ОП.01 Основы информационной безопасности

Требования профессионального стандарта	**Наименование профессиональных модулей (МДК) с образовательными результатами, имеющими взаимосвязь с ОР дисциплины**	**Образовательные результаты дисциплины**	**Наименование разделов/тем и рабочей программе по дисциплине**
Необходимые умения: ТУ1 Проводить проверку комплектности СССЭ, средств и систем защиты СССЭ от НСД	ПМ 01. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении: ПК 1.1 Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. Опыт практической деятельности: установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем Уметь: проводить текущий контроль показателей и процесса функционирования СССЭ Знать: организационные меры по защите информации	**Уметь:** У1 классифицировать защищаемую информацию по видам тайны и степеням секретности У2 классифицировать основные угрозы безопасности информации.	**Тема 1.1.** Основные понятия и задачи информационной безопасности **Тема 1.2.** Основы защиты информации **Тема 1.3.** Угрозы безопасности защищаемой информации. **Тема 2.3.** Защита информации в автоматизированных (информационных) системах
Необходимые знания: ТЗ 1. Номенклатура, функциональное назначение и основные характеристики СССЭ		**Знать:** З 1 основные методики анализа угроз и рисков информационной безопасности; З 2 виды, источники и носители защищаемой информации; З 3 источники угроз безопасности информации и меры по их предотвращению.	

ПРИЛОЖЕНИЕ 3

Сопоставление требований демонстрационного экзамена по состоянию на декабрь 2023 год, по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» и образовательных результатов УД

ОП.01 Основы информационной безопасности

Требования ДЭ	Образовательные результаты дисциплины	Наименование разделов/тем в рабочей программе по дисциплине
Уметь Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; Демонстрировать уверенность и упорство в решении проблем ***Знать*** Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности; границы собственных знаний, навыков и полномочий;	**Знать:** основные методики анализа угроз и рисков информационной безопасности; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению. **Уметь:** классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации.	**Тема 1.1.** Основные понятия и задачи информационной безопасности **Тема 1.2.** Основы защиты информации **Тема 1.3.** Угрозы безопасности защищаемой информации. **Тема 2.3.** Защита информации в автоматизированных (информационных) системах

ПРИЛОЖЕНИЕ 4

Сопоставление требований РЧ/НЧ 2022 года по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» и образовательных результатов УД ОП.01 Основы информационной безопасности

Требования РЧ	Образовательные результаты дисциплины	Наименование разделов/тем и рабочей программе по дисциплине
Уметь		
Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости; Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; Демонстрировать уверенность и упорство в решении проблем	**Уметь:** классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации.	**Тема 1.1.** Основные понятия и задачи информационной безопасности **Тема 1.2.** Основы защиты информации **Тема 1.3.** Угрозы безопасности защищаемой информации. **Тема 2.1.** Методологические подходы к защите информации **Тема 2.3.** Защита информации в автоматизированных (информационных) системах
знать		
Типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации; Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; Демонстрировать уверенность и упорство в решении проблем; Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей;	**Знать:** основные методики анализа угроз и рисков информационной безопасности; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению.	**Тема 1.1.** Основные понятия и задачи информационной безопасности **Тема 1.2.** Основы защиты информации **Тема 1.3.** Угрозы безопасности защищаемой информации. **Тема 2.1.** Методологические подходы к защите информации **Тема 2.3.** Защита информации в автоматизированных (информационных) системах