

НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Директор НПОУ «ЯКИТ»
Л.Н. Цой
«31» августа 2020 г.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.14 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении

Специальность: 09.02.07 Информационные системы и программирование

Профиль подготовки: технический

Квалификация программист

Форма обучения очно - заочная

Год набора 2020

Якутск, 2020

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование.

ОДОБРЕНО:

Научно-методической комиссией

Протокол № 34 от «25» июня 2020 г.

Председатель



Л.Л. Маркова

РАССМОТРЕНО

на заседании отделения экономики, менеджмента и информационных технологий.

Протокол № 12 от «22» июня 2020 г.

Зав. отделением



И.В. Пронин

СОДЕРЖАНИЕ

1.	ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	4
2.	СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	6
3.	УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	8
4.	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	13

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.14 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

1.1. Область применения рабочей программы

Рабочая программа дисциплины является частью образовательной программы в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

1.2. Место дисциплины в структуре ППССЗС:

ОПЦ. Общепрофессиональный цикл

ОП.14. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении.

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

В результате изучения профессионального модуля студент должен освоить основной вид деятельности Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующие ему профессиональные и общие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ДПК.1.1. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок

ДПК.1.2. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от утечки по техническим каналам

ДПК.1.3. Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа

В результате освоения дисциплины обучающийся должен:

Иметь практический опыт установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем;

- администрирования автоматизированных систем в защищенном исполнении;

- эксплуатации компонентов систем защиты информации автоматизированных систем;

- диагностики компонентов систем защиты информации автоматизированных систем,

- устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении

В результате освоения дисциплины обучающийся должен уметь:

- осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;

- организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

- осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

- настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;

- обеспечивать работоспособность, обнаруживать и устранять неисправности

В результате освоения дисциплины обучающийся должен знать

- состав и принципы работы автоматизированных систем, операционных систем и сред;

- принципы разработки алгоритмов программ, основных приемов программирования;

- модели баз данных;

- принципы построения, физические основы работы периферийных устройств;

- теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, - - протоколов и принципов адресации;

- порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;

- принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

1.4. Количество часов на освоение дисциплины:

- Максимальной учебной нагрузки обучающегося 98 часов, в том числе:
- обязательная аудиторная учебная нагрузка (всего) 65 часов;

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.14 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	98
Обязательная аудиторная учебная нагрузка (всего)	
в том числе:	
лекционные занятия <i>(если предусмотрено)</i>	32
лабораторные занятия <i>(если предусмотрено)</i>	
практические занятия <i>(если предусмотрено)</i>	32
контрольные работы <i>(если предусмотрено)</i>	
курсовая работа (проект) <i>(если предусмотрено)</i>	
Самостоятельная работа обучающегося (всего)	
Промежуточная аттестация в форме	экзамен

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) <i>(если предусмотрено)</i>	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		42	
Тема 1.1. Основы информационных систем как объекта защиты.	Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.	6	
	Практические занятия. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система,	4	

	автоматизированная информационная система компании)		
Тема 1.2. Жизненный цикл автоматизированных систем	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	6	
	Практические занятия Разработка технического задания на проектирование автоматизированной системы	2	
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации	6	
	Практические занятия Категорирование информационных ресурсов. Анализ угроз безопасности информации. Построение модели угроз	2	
Тема 1.4. Содержание и порядок эксплуатации АС в защищенном исполнении	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	6	
	Практические занятия. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	2	
Тема 1.5. Угрозы безопасности информации в автоматизированных системах	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации	6	
	Практические занятия. Категорирование информационных ресурсов	2	
Раздел 2. Эксплуатация защищенных		56	

автоматизированных систем.			
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	6	
	Практические занятия. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	2	
Тема 2.2. Администрирование автоматизированных систем	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	8	
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	4	
	Практические занятия. Классификация автоматизированных систем. Требования по защите информации от НСД для АС	4	
Тема 2.4. Защита от несанкционированного доступа к информации	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.	5	
	Практические занятия. Требования защищенности СВТ от НСД к информации	2	
Тема 2.5. СЗИ от НСД	Назначение и основные возможности системы защиты от несанкционированного доступа.	6	

	Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.		
	Практические занятия. Установка и настройка СЗИ от НСД	4	
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	4	
	Практические занятия. Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	2	
Тема 2.7. Документация на защищаемую автоматизированную систему	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	5	
	Практические занятия. Оформление основных эксплуатационных документов на автоматизированную систему.	4	
ВСЕГО		98	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.14 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

3.1. Материально-техническое обеспечение

Реализация программы предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета:

- автоматизированные рабочие места обучающихся;
- компьютеры, объединенные в локальную вычислительную сеть;
- проектор;
- экран;
- акустическая система;
- учебно-наглядные пособия:
- схемы;
- таблицы;
- учебные презентации.

Технические средства обучения:

- компьютеры, объединенные в локальную вычислительную сеть;
- мультимедиа проектор;
- интерактивная доска.
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности в виде: ПАК Соболев (имеется в наличии) – 1 шт.

3.2. Информационное обеспечение обучения

Перечень учебных изданий, интернет – ресурсов, дополнительной литературы.

Основные источники:

1. Системы управления технологическими процессами и информационные технологии : учебное пособие для среднего профессионального образования / В. В. Троценко, В. К. Федоров, А. И. Забудский, В. В. Комендантов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 136 с. — (Профессиональное образование). — ISBN 978-5-534-09939-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: [Uhttps://urait.ru/bcode/493021U](https://urait.ru/bcode/493021U)

2. Системы управления технологическими процессами и информационные технологии : учебное пособие для среднего профессионального образования / В. В. Троценко, В. К. Федоров, А. И. Забудский, В. В. Комендантов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 136 с. — (Профессиональное

образование). — ISBN 978-5-534-09939-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: [Uhttps://urait.ru/bcode/493021U](https://urait.ru/bcode/493021U)

Дополнительные источники:

1. Колошкина, И. Е. Автоматизация проектирования технологической документации : учебник и практикум для среднего профессионального образования / И. Е. Колошкина. — Москва : Издательство Юрайт, 2022. — 371 с. — (Профессиональное образование). — ISBN 978-5-534-13635-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: [Uhttps://urait.ru/bcode/497426U](https://urait.ru/bcode/497426U)

2. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук ; под общей редакцией Д. В. Чистова. — Москва : Издательство Юрайт, 2022. — 258 с. — (Профессиональное образование). — ISBN 978-5-534-03173-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: [Uhttps://urait.ru/bcode/491568U](https://urait.ru/bcode/491568U)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОП.14 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ.

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
<p>Умения:</p> <ul style="list-style-type: none"> – осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности 	<p>Практические занятия, домашняя работа, тестирование</p>
<p>Знания:</p> <ul style="list-style-type: none"> – состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; 	<p>Домашняя работа, тестирование</p>

- | | |
|---|--|
| <ul style="list-style-type: none">– принципы построения, физические основы работы периферийных устройств;– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;– принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации. | |
|---|--|