

НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДЕНО  
педагогическим советом  
(протокол №06-23 от «26» июня 2023)  
Председатель педагогического совета  
Директор \_\_\_\_\_ Л.Н. Цой



**Рабочая программа дисциплины**

**ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**ППССЗ по специальности**

**10.02.05 Обеспечение информационной безопасности автоматизированных систем**

**Объем дисциплины – 48 час.**

Якутск, 2023


Рабочая программа учебной дисциплины разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Укрупненная группа специальностей 10.00.00 Информационная безопасность.


**Разработчики** НПОУ «ЯКИТ» преподаватель В.В. Максимова  
 программы: \_\_\_\_\_  
 (место работы) (занимаемая должность) (инициалы, фамилия)

**Обсуждено** на заседании «19» июня 2023 протокол №9/1  
 отделения

Председатель Зав. отделением  Пронин И.В.  
 отделения

**Рассмотрено** на заседании «20» июня 2023 г. протокол №6  
 методического совета

Председатель Заместитель МС директора по учебно-методической работе  «20» июня 2023 г.

Заместитель Томская С.И. «26» июня 2023 г.  
 директора по учебно-методической работе 

№ п/п	Прилагаемый к Рабочей программе документ, содержащий текст обновления	Решение отделения		Подпись заведующего отделения	Фамилия И.О. заведующего отделения
		дата	Протокол №		
1.	Приложение № 1				
2.	Приложение № 2				
3.	Приложение № 3				
4.	Приложение № 4				
5.	Приложение № 5				

## 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.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

## **1.1. Область применения рабочей программы**

Рабочая программа дисциплины является частью образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

## **1.2. Место дисциплины в структуре ППССЗС:**

ОПЦ. Общепрофессиональный цикл

## **1.3. ОП.01 Основы информационной безопасности**

Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;

- классифицировать основные угрозы безопасности информации.

В результате освоения 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.

ПК и ОК, которые актуализируются при изучении дисциплины:

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

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

1.4. Количество часов на освоение дисциплины:

Максимальной учебной нагрузки обучающегося 48 часов, в том числе:

- обязательная аудиторная учебная нагрузка (всего) 48 часов;

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.01. Основы информационной безопасности

### 2.1. Объем дисциплины и виды учебной работы

<b>Вид учебной работы</b>	<b>Объем часов</b>
Максимальная учебная нагрузка (всего)	48
Обязательная аудиторная учебная нагрузка (всего)	48
в том числе:	
лекционные занятия <i>(если предусмотрено)</i>	20
лабораторные занятия <i>(если предусмотрено)</i>	28
практические занятия <i>(если предусмотрено)</i>	
контрольные работы <i>(если предусмотрено)</i>	
курсовая работа (проект) <i>(если предусмотрено)</i>	
Самостоятельная работа обучающегося (всего)	
Промежуточная аттестация в форме	зачет

## 2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	4
<b>Раздел 1. Теоретические основы информационной безопасности</b>		<b>17</b>	
<b>Тема 1.1.</b> Основные понятия и задачи информационной безопасности	<b>Содержание учебного материала</b>	<b>3</b>	ОК 3. ОК 09. ОК 10. 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 не информированности в области информационной безопасности.		
<b>Тема 1.2.</b> Основы защиты информации	<b>Содержание учебного материала</b>	<b>3</b>	ОК 3. ОК 09. ОК 10. 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.		
	<b>Лабораторное занятия</b>	<b>4</b>	
	Определение объектов защиты на типовом объекте информатизации. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.		
<b>Тема 1.3.</b> Угрозы	<b>Содержание учебного материала</b>	<b>3</b>	ОК 3.

безопасности защищаемой информации.	Понятие угрозы безопасности информации		ОК 09. ОК 10. ПК 2.4.
	Системная классификация угроз безопасности информации.		
	Каналы и методы несанкционированного доступа к информации		
	Уязвимости. Методы оценки уязвимости информации		
	<b>Лабораторное занятие</b>	<b>4</b>	
	Определение угроз объекта информатизации и их классификация		
<b>Раздел 2. Методология защиты информации</b>		<b>19</b>	
Тема 2.1. Методологические подходы к защите информации	<b>Содержание учебного материала</b>	<b>3</b>	ОК 3. ОК 09. ОК 10. 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.		
Тема 2.2. Нормативно правовое регулирование защиты информации	<b>Содержание учебного материала</b>	<b>3</b>	ОК 3. ОК 09. ОК 10. ПК 2.4.
	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		
	<b>Лабораторное занятие</b>	<b>5</b>	
	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности		
Тема 2.3. Защита	<b>Содержание учебного материала</b>	<b>1</b>	ОК 3.



информации в автоматизированных (информационных) системах	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.		ОК 09. ОК 10. ПК 2.4.
	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.		
	<b>Лабораторное занятие</b>		
Выбор мер защиты информации для автоматизированного рабочего места			
<b><i>Промежуточная аттестация по учебной дисциплине</i></b>		<b>2</b>	
<b>Всего</b>		<b>48</b>	

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.01. Основы информационной безопасности**

#### **3.1. Материально-техническое обеспечение**

Реализация дисциплины требует наличия:

- учебного кабинета.

Технические средства обучения:

Занятия проводятся в учебной аудитории и компьютерном классе, оснащенных необходимым учебным, методическим, информационным, программным обеспечением.

#### **3.2. Информационное обеспечение обучения**

Перечень учебных изданий, интернет – ресурсов, дополнительной литературы.

Основные источники:

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8.

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8.

Дополнительные источники:

1. Информационные технологии в экономике и управлении в 2 ч. Часть 2 : учебник для среднего профессионального образования / В. В. Трофимов [и др.] ; под редакцией В. В. Трофимова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 245 с. — (Профессиональное образование). — ISBN 978-5-534-09139-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: [Uhttps://urait.ru/bcode/494766U](https://urait.ru/bcode/494766U)

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОП.01. Основы информационной безопасности

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	Критерии оценки	Формы и методы оценки
<p><b>Знания:</b></p> <ul style="list-style-type: none"> <li>– сущность и понятие информационной безопасности, характеристику ее составляющих;</li> <li>– место информационной безопасности в системе национальной безопасности страны;</li> <li>– виды, источники и носители защищаемой информации;</li> <li>– источники угроз безопасности информации и меры по их предотвращению;</li> <li>– факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;</li> <li>– жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;</li> <li>– современные средства и способы обеспечения информационной безопасности;</li> <li>– основные методики анализа угроз и рисков информационной</li> </ul>	<p>Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.</p>	<p>Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование</p>

безопасности.		
<p>Умения:  – классифицировать защищаемую информацию по видам тайны и степеням секретности;  – классифицировать основные угрозы безопасности информации;</p>	<p>Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности</p>	<p>Экспертное наблюдение в процессе практических занятий</p>