ГПОУ «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 – 60 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 программы:	НПОУ «ЯКИТ»	преподаватель	В.В. Максимова
	(место работы)	(занимаемая должность)	(инициалы, фамилия)

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

Председатель отделения Зав. отделением Пронин И.В.

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

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

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

№ 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 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 ППССЗ:

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 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой

грамотности в различных жизненных ситуациях.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

ОК 09. 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 60 часов, в том числе:

– обязательная аудиторная учебная нагрузка (всего) 48 часов;
– самостоятельная работа -12 часов.

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

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	60
Обязательная аудиторная учебная нагрузка (всего)	48
в том числе:	
лекционные е занятия *(если предусмотрено)*	20
лабораторные занятия *(если предусмотрено)*	
практические занятия *(если предусмотрено)*	28
контрольные работы *(если предусмотрено)*	
курсовая работа (проект) *(если предусмотрено)*	
Самостоятельная работа обучающегося (всего)	12
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	Уровень освоения
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности			
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**		1,2
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	3	
	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.		
Тема 1.2. Основы защиты информации	**Содержание учебного материала**		1,2
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.	3	
	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.		
	Практическая работа	**7**	
	Определение объектов защиты на типовом объекте информатизации.		
	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.		
Тема 1.3. Угрозы безопасности защищаемой информации.	**Содержание учебного материала**		1,2
	Понятие угрозы безопасности информации	4	
	Системная классификация угроз безопасности информации.		
	Каналы и методы несанкционированного доступа к информации		
	Уязвимости. Методы оценки уязвимости информации		
	Практическая работа	**7**	
	Определение угроз объекта информатизации и их классификация		
Раздел 2. Методология защиты информации			
Тема 2.1. Методологические подходы к защите информации	**Содержание учебного материала**		1,2
	Анализ существующих методик определения требований к защите информации.	4	
	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	**Содержание учебного материала**		1,2
	Организационная структура системы защиты информации	3	
	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		
	Практическая работа	**7**	

	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**		1,2
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	3	
	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.		
	Практическая работа	**7**	
	Выбор мер защиты информации для автоматизированного рабочего места		
Самостоятельная работа		12	
Всего		***60***	

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

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
Знания: – 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;	Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование

– основные методики анализа угроз и рисков информационной безопасности.		
Умения: – 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	Экспертное наблюдение в процессе практических занятий