



**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ЦИФРОВОЙ КОЛЛЕДЖ «СИНЕРГИЯ»**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.01. Основы информационной безопасности

*для специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем
(квалификация – техник по защите информации)*

Якутск, 2023

СОГЛАСОВАНО
на заседании Педагогического совета
Протокол № 1 от « 28 » июня 2023 г.

УТВЕРЖДАЮ
Директор АНО СПО «Цифровой
колледж «Синергия»
_____ С.Н.Семенов
« _____ » _____ 2023 г.

Рабочая программа дисциплины ОП.01. Основы информационной безопасности разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки РФ от 9.12.2016 г. № 1553

Организация-разработчик: АНО СПО «Цифровой колледж «Синергия»

Составитель:
Сидорова А.Ю., зам.директора по УВР

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	стр. 4
2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	6
3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	10
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	12

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

ОП.01. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения программы

Рабочая программа дисциплины ОП.01. Основы информационной безопасности является частью основной профессиональной образовательной программы СПО – программы подготовки квалифицированных рабочих, служащих по специальности 10.02.05 *Обеспечение информационной безопасности автоматизированных систем (квалификация – техник по защите информации)*, входящей в состав укрупненной группы специальностей 10.00.00 *Информационная безопасность*.

1.2 Место дисциплины в структуре образовательной программы:

Дисциплина ОП.01. Основы информационной безопасности является дисциплиной общепрофессионального учебного цикла.

1.3. Требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся **должен уметь:**

У₁ – определять основные угрозы безопасности информации;

знать:

З₁ - сущность и понятие информационной безопасности, характеристику ее составляющих;

З₂ - место информационной безопасности в системе национальной безопасности страны;

З₃ - виды, источники и носители защищаемой информации;

З₄ - источники угроз безопасности информации и меры по их предотвращению;

З₅ - факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

З₆ - жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

З₇ - современные средства и способы обеспечения информационной безопасности;

З₈ - основные методики анализа угроз и рисков информационной безопасности;

С целью овладения **общими компетенциями (ОК):**

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

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

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и *иностранном* языках¹.

и профессиональными компетенциями (ПК):

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

1.4. Количество часов на освоение рабочей программы дисциплины:

максимальная учебная нагрузка обучающегося – 56 часов, в том числе

в форме практической подготовки – 12 часов

включает:

Объем работы обучающегося во взаимодействии с преподавателем – 42 часов, в том числе

практические занятия – 12 часа;

самостоятельная работа обучающегося – 8 часов

промежуточная аттестация – 6 часов

Обязательная часть рабочей программы составляет – 40 часов, вариативная часть – 16 часов.

¹ Выделенное курсивом не формируется в рамках данной дисциплины

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем дисциплины (всего)	56
<i>в том числе:</i>	
в форме практической подготовки	12
Объем работы обучающегося во взаимодействии с преподавателем	42
<i>в том числе:</i>	
практические занятия	12
Самостоятельная работа обучающегося (всего)	8
<i>в том числе:</i>	
изучение нормативной документации	2
подготовка к промежуточной аттестации	6
Промежуточная аттестация	6

2.2. Формы промежуточной аттестации

2 семестр – экзамен

2.2. Тематический план и содержание дисциплины ОП.01. Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающихся	Объем часов	В т.ч. практическая подготовка	Формируемые компетенции	
Тема 1. Нормативные основы информационной безопасности	<i>Содержание учебного материала</i>	<i>16</i>			
	1	Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание	2		ОК 05, ОК 10, ПК 1.3, ПК 2.2
	2	Информационная безопасность в системе национальной безопасности Российской Федерации. Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере	2		
	3	Государственная информационная политика. Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности	2		
	4	Информация - наиболее ценный ресурс современного общества. Понятие «информационный ресурс». Классы информационных ресурсов	2		
	5	Проблемы информационной войны. Информационное оружие и его классификация. Информационная война	2		
	6	Проблемы информационной безопасности в сфере государственного и муниципального управления. Информационные процессы в сфере государственного и муниципального управления. Виды информации и информационных ресурсов в сфере ГМУ. Состояние и перспективы информатизации сферы ГМУ	2		
	7	Информационные системы. Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах	2		
	8	Методы и модели оценки уязвимости информации. Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита»	2		
	Самостоятельная работа		2		
Изучение нормативной документации					

Тема 2. Проблемы информационной безопасности	<i>Содержание учебного материала</i>		<i>10</i>		ОК 05, ОК 10, ПК 1.3, ПК 2.2	
	1	Основные понятия и анализ угроз информационной безопасности. Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности	2			
	2	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей	2			
	3	Политика безопасности. Основные понятия политики безопасности. Структура политики безопасности организации.	2			
	4	Стандарты информационной безопасности. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий	2			
Практические занятия			2		ОК 04, ОК 05, ОК 09 -ОК 10, ПК 1.3, ПК 2.2	
5	Практическое занятие № 1. Определение угроз объекта информатизации и их классификация		2			
Тема 3. Технологии защиты данных	<i>Содержание учебного материала</i>		<i>20</i>	<i>10</i>	ОК 05, ОК 10, ПК 1.3, ПК 2.2	
	1	Принципы криптографической защиты информации. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования. Электронная цифровая подпись и функция хэширования.	2			
	2	Криптографические алгоритмы. Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы.	2			
	3	Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.	2			
	Практические занятия			10		ОК 04, ОК 05, ОК 09 -ОК 10, ПК 1.3, ПК 2.2
	4	Практическое занятие № 2. Криптографическое шифрование методом простой замены		10		
	5	Практическое занятие № 3. Криптографическое шифрование методом многоалфавитной одноконтурной замены				
6	Практическое занятие № 4. Криптографическое шифрование методом усложнённой перестановки по маршрутам					
7	Практическое занятие № 5. Составление блок-схемы алгоритма идентификации и установки подлинности пользователя					

	8	Практическое занятие № 6. Аутентификация пользователей			
		Самостоятельная работа	6		ОК 03-ОК 05, ОК 09, ОК10, ПК 1.3, ПК 2.2
		Подготовка к промежуточной аттестации			
			Экзамен	6	
			ВСЕГО:	56	12

2.3 Вариативная часть дисциплины

№ п/п	Наименование тем	Количество часов	Примечание
1	Тема 1. Нормативные основы информационной безопасности	2	Для совершенствования знаний и умений
2	Самостоятельная работа	8	
3	Экзамен	6	Для проверки знаний и умений по ОП.01
	ИТОГО:	16	

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация рабочей программы дисциплины проходит в лаборатории информатики и информационных технологий.

Оборудование лаборатории:

- посадочные места по количеству обучающихся;
- персональные компьютеры для обучающихся;
- проектор, экран;
- маркерная доска;
- рабочее место преподавателя – АРМ преподавателя;
- принтер.

3.2. Учебно-методическое обеспечение

По дисциплине ОП.01. Основы информационной безопасности разработана учебно-методическая документация:

- рабочая программа дисциплины;
- оценочные материалы;
- методические указания по выполнению заданий на практических занятиях;
- методические указания по выполнению самостоятельной работы.

3.3. Информационное обеспечение обучения

Литература:

1. Богатырев В. А. Надежность информационных систем: учебное пособие для среднего профессионального образования / В. А. Богатырев. — Москва: Издательство Юрайт, 2023. — 318 с. — (Профессиональное образование). — ISBN 978-5-534-15205-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/520442> (дата обращения: 29.06.2023).

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. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518006> (дата обращения: 29.06.2023).

3. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519364> (дата обращения: 30.06.2023).

4. Щербак А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519614> (дата обращения: 29.06.2023).

Электронные источники:

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» <http://www.ict.edu.ru>

10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе текущего контроля знаний, проверки выполнения заданий практических занятий, а также во время промежуточной аттестации.

Оценка качества подготовки обучающихся осуществляется через оценку знаний, умений по дисциплине и оценку сформированности компетенций.

Результаты обучения (знания, умения)	Формы и методы контроля и оценки результатов обучения	
	Текущий контроль	Промежуточная аттестация
уметь:		
У ₁ - определять основные угрозы безопасности информации;	- оценка выполнения заданий на практических занятиях; - оценка участия обучающегося на уроках; - оценка выполнения заданий самостоятельной работы	- экзамен
знать:		
З ₁ - сущность и понятие информационной безопасности, характеристику ее составляющих;	- оценка выполнения заданий на практических занятиях; - устный опрос; - тестирование; - оценка выполнения заданий самостоятельной работы	- экзамен
З ₂ - место информационной безопасности в системе национальной безопасности страны;		
З ₃ - виды, источники и носители защищаемой информации;		
З ₄ - источники угроз безопасности информации и меры по их предотвращению;		
З ₅ - факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;		
З ₆ - жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;		
З ₇ - современные средства и способы обеспечения информационной безопасности;		
З ₈ - основные методики анализа угроз и рисков информационной безопасности;		

Оценка *общих компетенций (ОК)*:

<i>Результат (общие компетенции)</i>	<i>Основные показатели</i>
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	<ul style="list-style-type: none"> - берет на себя ответственность за принятое решение/совершенный поступок - ответственно выполняет разовые/постоянные поручения в группе - может спрогнозировать результат - умеет оценить свои действия, поступки и проанализировать их
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	<ul style="list-style-type: none"> - устанавливает позитивный стиль общения - выбирает стиль общения в соответствии с ситуацией - признает чужое мнение - при необходимости отстаивает собственное мнение - принимает критику - ведет деловую беседу в соответствии с этическими нормами - соблюдает официальный стиль при оформлении документов - выполняет письменные и устные рекомендации преподавателя - способен к эмпатии - организует коллективное обсуждение рабочей ситуации
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	<ul style="list-style-type: none"> - умеет передавать информацию другому человеку - способен правильно формулировать свои мысли в устной и письменной формах - способен оценить уровень своих знаний по дисциплине
ОК 09. Использовать информационные технологии в профессиональной деятельности	<ul style="list-style-type: none"> - осуществляет поиск информации в сети Интернет и различных электронных носителях - извлекает информацию с электронных носителей - использует средства ИТ для обработки и хранения информации - представляет информацию в различных формах с использованием разнообразного программного обеспечения - создает презентации в различных формах
ОК 10. Пользоваться профессиональной документацией на государственном и <i>иностранном</i> языках ² .	<ul style="list-style-type: none"> - осуществлять эффективный поиск необходимой информации в российских и зарубежных источниках: нормативно-правовой документации, стандартов, научных публикации, технической документации; - уметь анализировать, систематизировать и применять в профессиональной деятельности информацию, содержащуюся в документации профессиональной области.

² Выделенное курсивом не формируется в рамках данной дисциплины

Освоение профессиональной компетенции (ПК) осуществляется через знания и умения.

Критерии и методы оценки освоения дисциплины отражены в фонде оценочных средств.