

Приложение № 3 Рабочие программы учебных дисциплин  
к ОПОП по специальности  
10.02.05 Обеспечение информационной безопасности  
автоматизированных систем

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**  
**ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Регистрационный № 22ИБ/24

Санкт-Петербург

2022

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного Приказом Министерства образования и науки от 09.12.2016 № 1553

**Организация-разработчик:**

Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Академия промышленных технологий» (СПб ГБОУ «АПТ»)

**Разработчик:**

Федотов Д.В.– преподаватель СПб ГБПОУ «АПТ»

Рабочая программа рассмотрена на заседании учебной цикловой комиссии  
**Информационных технологий**

Рабочая программа соответствует требованиям к содержанию, структуре, оформлению.  
Протокол № 10 от 07.06.2022

Председатель УЦК Еропкин И.В.

Программа одобрена на заседании Педагогического совета и рекомендована к использованию в учебном процессе.

Протокол № 1 от 30 августа 2022

**СОДЕРЖАНИЕ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ  
УЧЕБНОЙ ДИСЦИПЛИНЫ
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

## 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 1.1. Место дисциплины в структуре основной профессиональной образовательной программы:

Дисциплина *ОП.01 Основы информационной безопасности* входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

### 1.2. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК	Умения	Знания
ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4	<ul style="list-style-type: none"> <li>– классифицировать защищаемую информацию по видам тайны и степеням секретности;</li> <li>– классифицировать основные угрозы безопасности информации;</li> </ul>	<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 безопасности;</li> </ul>

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
<b>Обязательная учебная нагрузка</b>	51
в том числе:	
-теоретическое обучение	31
-практические занятия	18
- лабораторные занятия	-
- самостоятельная работа	-
- консультации	-
- промежуточная аттестация 4 семестр – <b>дифференциальный зачет</b>	<b>2</b>

Вариативная часть в объеме **17** часа направлена на углубление изучения материала для подготовке обучающегося к освоению видов деятельности

## 2.2. Тематический план и содержание учебной 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>38</b>	
<b>Тема 1.1.</b> Основные понятия и задачи информационной безопасности	<b>Содержание учебного материала</b>	<b>6</b>	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.		
<b>Тема 1.2.</b> Основы защиты информации	<b>Содержание учебного материала</b>	<b>18</b>	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.	12	
	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>Практические занятия</b>	<b>6</b>	
	Определение объектов защиты на типовом объекте информатизации.		
	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.		
<b>Тема 1.3.</b> Угрозы безопасности	<b>Содержание учебного материала</b>	<b>14</b>	ОК 3, ОК 6, ОК 9, ПК.2.4
	Понятие угрозы безопасности информации	10	

Наименование разделов и тем	Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	4
защищаемой информации.	Системная классификация угроз безопасности информации.		
	Каналы и методы несанкционированного доступа к информации		
	Уязвимости. Методы оценки уязвимости информации		
	<b>Практическое занятие</b>	<b>4</b>	
	Определение угроз объекта информатизации и их классификация		
<b>Раздел 2. Методология защиты информации</b>		<b>26</b>	
<b>Тема 2.1.</b> Методологические подходы к защите информации	<b>Содержание учебного материала</b>	<b>6</b>	ОК 3, ОК 6, ОК 9, ПК 2.4
	Анализ существующих методик определения требований к защите информации.	6	
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.		
	Виды мер и основные принципы защиты информации.		
<b>Тема 2.2.</b> Нормативно правовое регулирование защиты информации	<b>Содержание учебного материала</b>	<b>10</b>	ОК 3, ОК 6, ОК 9, ОК 10
	Организационная структура системы защиты информации	6	
	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>Практическое занятие</b>		
<b>Тема 2.3.</b> Защита информации в автоматизированных (информационных)	<b>Содержание учебного материала</b>	<b>10</b>	ОК 3, ОК 6, ОК 9, ОК 10
Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	8		
		Программные и программно-аппаратные средства защиты информации	

Наименование разделов и тем	Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	4
системах	Инженерная защита и техническая охрана объектов информатизации		
	Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.		
	<b>Практическое занятие</b>	<b>2</b>	
	Выбор мер защиты информации для автоматизированного рабочего места		
<i>Промежуточная аттестация по учебной дисциплине- Дифференциальный зачет</i>		<b>2</b>	
<b>Всего</b>		<b>51</b>	

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:**

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.

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

##### **1.2.1. Основные печатные источники:**

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2019.

##### **1.2.2. Дополнительные печатные источники:**

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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 безопасности.</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>
<p><b>Умения:</b></p> <ul style="list-style-type: none"> <li>– классифицировать защищаемую информацию по видам тайны и степеням секретности;</li> <li>– классифицировать основные угрозы безопасности информации;</li> </ul>	<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>