



Автономная некоммерческая образовательная организация  
профессионального образования  
«Санкт-Петербургская академия милиции имени Н.А. Щёлокова»  
(АНОО ПО «СПб АМ им. Н.А. Щёлокова»)

ИНН 7801152738/ОГРН 1037800006276

190005, г. Санкт-Петербург, ул. 7-я Красноармейская, д.26, лит. Б

тел. 8 (812) 490-24-85, 8 (812) 316-49-53, 8 (812) 316-03-88

<https://police-college.ru/> \* e-mail: [ipc-info@yandex.ru](mailto:ipc-info@yandex.ru)

Принято на заседании  
Педагогического Совета  
Протокол № 6 от 28.12.2023г.

Утверждаю  
Директор АНОО ПО  
«СПб АМ им. Н.А. Щёлокова»  
О.В. Ярухин  
Приказ №105У от «28» декабря 2023 г.



**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ  
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

по программе подготовки специалистов среднего звена по специальности

**10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

на базе среднего общего образования.

Форма обучения: Очная

Санкт-Петербург

2023

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (утв. приказом Министерства образования и науки Российской Федерации от 28.07.2014 № 805)

Организация-разработчик: Автономная некоммерческая образовательная организация профессионального образования «Санкт-Петербургская академия милиции имени Н.А. Щёлокова».

**С О Д Е Р Ж А Н И Е**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ .....	5
2.1. Объем учебной дисциплины и виды учебной работы.....	5
2.2. Тематический план и содержание учебной дисциплины.....	6
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	12

**1. ОБЩАЯ ХАРАКТЕРИСТИКА  
РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ  
ОП.01. «Основы информационной безопасности»**

**1.1. Область применения рабочей программы**

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

**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 конфиденциальности;</li> <li>– применять основные правила и документы системы сертификации Российской Федерации;</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>– источники угроз информационной безопасности и меры по их предотвращению;</li> <li>– жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;</li> <li>– современные средства и способы обеспечения информационной безопасности.</li> </ul>

В результате освоения образовательной программы у выпускника должны быть сформированы общие и профессиональные компетенции:

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

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

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.

**2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ****2.1. Объем учебной дисциплины и виды учебной работы**

<b>№ п/п</b>	<b>Вид учебной работы</b>	<b>Объем часов</b>
<b>1.</b>	<b>Объем работы обучающихся во взаимодействии с преподавателем</b>	92
<b>2.</b>	<b>В форме практической подготовки</b>	92
<i>в том числе во взаимодействии с преподавателем:</i>		
	– теоретическое обучение	50
	– практические занятия	42
	– промежуточная аттестация в форме экзамена	
<b>3.</b>	<b>Самостоятельная внеаудиторная работа обучающихся</b>	12
<b>Всего по дисциплине в рамках образовательной программы</b>		<b>104</b>

## 2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов, в т.ч.			Коды компетенций, формированию которых способствует элемент программы
		всего	практические занятия	в форме практической подготовки	
<b>Тема 1. Информационная безопасность в системе национальной безопасности РФ</b>	<b>Содержание учебного материала</b>	<b>8</b>		<b>8</b>	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	1.1. Место информационной безопасности в системе национальной безопасности РФ.	2		2	
	1.2. Направления государственной политики в области информационной безопасности.	2		2	
	1.3. Источники и содержание угроз в информационной сфере	2		2	
	1.4. Юридические аспекты защиты информации в РФ	2		2	
<b>Тема 2. Критическая информационная инфраструктура (КИИ) РФ</b>	<b>Содержание учебного материала</b>	<b>10</b>		<b>10</b>	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	2.1. Понятие КИИ. Компоненты КИИ.	2		2	
	2.2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ	2		2	
	2.3. Категорирование объектов КИИ	2		2	
	2.4. Реестр значимых объектов КИИ. Система безопасности значимого объекта КИИ	2		2	
	2.5. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	2		2	
<b>Тема 3. Сущность и понятие информационной безопасности (ИБ), характеристика составляющих ИБ</b>	<b>Содержание учебного материала</b>	<b>18</b>	<b>6</b>	<b>18</b>	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	3.1. Сущность и понятие ИБ. Основные термины и определения.	2		2	
	3.2. Концептуальная модель ИБ	2		2	
	3.3. Понятие угрозы, виды угроз. Банк данных угроз безопасности информации ФСТЭК России	2		2	

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов, в т.ч.			Коды компетенций, формирование которых способствует элемент программы
		всего	практические занятия	в форме практической подготовки	
	3.4. Объекты воздействия угроз. Информационные ресурсы организации.	2		2	
	3.5. Источники угроз, цели угроз.	2		2	
	3.6. Понятие уязвимости. Виды уязвимостей	2		2	
	<b>Практические занятия</b>	<b>6</b>	<b>6</b>	<b>6</b>	
	<b>Практическое занятие № 1 «Работа с официальным сайтом ФСТЭК России»</b>	2	2	2	
	<b>Практическое занятие № 2 «Классификация угроз информационной безопасности»</b>	2	2	2	
	<b>Практическое занятие № 3 «Определение характеристик уязвимости с использованием банка данных уязвимостей»</b>	2	2	2	
<b>Тема 4. Информация как объект защиты</b>	<b>Содержание учебного материала</b>	<b>8</b>	<b>2</b>	<b>8</b>	
	4.1. Свойства информации с точки зрения ИБ. Виды информации в зависимости от категории доступа.	2		2	
	4.2. Конфиденциальная информация.	2		2	
	4.3. Жизненный цикл конфиденциальной информации в процессе ее создания, обработки, передачи.	2		2	
	<b>Практические занятия</b>	<b>2</b>	<b>2</b>	<b>2</b>	
	<b>Практическое занятие № 4 «Классификация информации по видам тайн и степеням конфиденциальности»</b>	2	2	2	
<b>Тема 5. Меры по предотвращению угроз.</b>	<b>Содержание учебного материала</b>	<b>26</b>	<b>4</b>	<b>26</b>	
	5.1. Направления защиты: правовая, организационная, техническая.	2		2	

ОК 03,  
ОК 06,  
ОК 09,  
ОК 10,  
ПК 2.4  
2

ОК 03,  
ОК 06,  
ОК 09,

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов, в т.ч.			Коды компетенций, формирование которых способствует элемент программы
		всего	практические занятия	в форме практической подготовки	
Современные средства и способы обеспечения информационной безопасности	5.2. Подходы к обеспечению ИБ.	2		2	ОК 10, ПК 2.4
	5.3. Физическая защита информации	2		2	
	5.4. Техническая защита информации	2		2	
	5.5. Криптографическая защита информации	2		2	
	5.6. Понятие и виды НСД.	2		2	
	5.7. Защита от НСД к информации.	2		2	
	5.8. Идентификация и аутентификация.	2		2	
	5.9. Управление доступом. Модели доступа	2		2	
	5.10. Защита от вредоносного программного обеспечения	2		2	
	5.11. Системы обнаружения вторжений (СОВ). Требования к СОВ	2		2	
	<b>Практические занятия</b>	<b>4</b>	<b>4</b>	<b>4</b>	
	<b>Практическое занятие № 5 «Работа с моделями доступа, определение степени конфиденциальности информации».</b>	2	2	2	
<b>Практическое занятие № 6 «Сравнительный анализ средств антивирусной защиты»</b>	2	2	2		
Тема 6. Защита от внутренних угроз. DLP-системы	<b>Содержание учебного материала</b>	<b>6</b>	<b>2</b>	<b>6</b>	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	6.1. Понятие DLP-системы. Структура, назначение, функции DLP-системы.	2		2	
	6.2. Обзор рынка DLP-систем	2		2	
	<b>Практические занятия</b>	<b>2</b>	<b>2</b>	<b>2</b>	
	<b>Практическое занятие № 7 «Определение внутренних угроз информационной безопасности»</b>	2	2	2	

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов, в т.ч.			Коды компетенций, формирование которых способствует элементу программы
		всего	практические занятия	в форме практической подготовки	
<b>Тема 7. Нарушитель ИБ</b>	<b>Содержание учебного материала</b>	<b>4</b>	<b>2</b>	<b>4</b>	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	7.1. Понятие нарушителя ИБ. Модели нарушителя ИБ	2		2	
	<b>Практические работы</b>	<b>2</b>	<b>2</b>	<b>2</b>	
	<b>Практическое занятие № 8</b> «Определение характеристик нарушителя ИБ в зависимости от угрозы информационной безопасности»	2	2	2	
<b>Тема 8. Сертификация и лицензирование</b>	<b>Содержание учебного материала</b>	<b>14</b>	<b>4</b>	<b>14</b>	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	8.1. Система сертификации средств защиты информации.	2		2	
	8.2. Порядок сертификации. Правила и документы сертификации. Государственный реестр сертифицированных средств защиты информации	2		2	
	8.3. Лицензирование в области защиты информации.	2		2	
	8.4. Аттестация объектов информатизации по требованиям защиты информации.	4		2	
	<b>Практические занятия</b>	<b>4</b>	<b>4</b>	<b>4</b>	
	<b>Практическое занятие № 9</b> «Применение правил и документов системы сертификации РФ»	2	2	2	
	<b>Практическое занятие № 10</b> «Заполнение заявления на сертификацию средства защиты информации»	2	2	2	
<b>Самостоятельная работа</b> Заполнение рабочей тетради в СДО на платформе Moodle	<b>12</b>			ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4	
				ОК 09, ОК 10, ПК 2.4	
<b>Промежуточная аттестация</b>		6			
<b>Всего</b>		<b>104</b>			

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Оборудование кабинета: рабочие места по количеству обучающихся; рабочее место преподавателя комплект учебно-наглядных пособий, в т.ч. на электронных носителях.

Технические средства обучения: компьютер с лицензионным программным обеспечением на рабочем месте преподавателя.

#### **3.2. Информационное обеспечение реализации программы**

Для реализации программы библиотечный фонд колледжа располагает печатными и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе

##### **3.2.1. Основные источники**

1. Баранова, Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учеб. Пособие. - 3-е изд, перераб. И доп. - Москва: РИОР: ИНФРА-М, 2016 - 322 с. - (Высшее образование).

##### **3.2.2. Электронные издания (электронные ресурсы)**

1. Баранова, Е. К. Основы информационной безопасности: учебник/ Е.К. Баранова, А.В. Бабаш. - Москва: РИОР: ИНФРА-М, 2021. — 202 с. — (Среднее профессиональное образование). — DOI: <https://doi.org/10.29039/01806-4>. - ISBN 978-5-369-01806-4.

##### **3.2.3. Дополнительные источники**

1. Воронцова, С.В. Обеспечение информационной безопасности в банковской сфере: монография / С.В. Воронцова. - 2-е изд., стер. - Москва: КНОРУС, 2020. - 160 с. - (Ligitimate legen et ordinem).

2. Шаханова, М.В. Современные технологии информационной безопасности: учебно-методический комплекс. - Москва: Проспект, 2020. - 216 с.

3. Ищейнов, В.Я., Мецатунян М.В. Основные положения информационной безопасности: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. -Москва: ФОРУМ: ИНФРА- М, 2021. - 208 с. - (Профессиональное образование).

4. Нестеров, С.А. Основы информационной безопасности: Учебное пособие. - 2-е изд., стер. - Санкт-Петербург: Издательство "Лань", 2020. - 324 с. - (Учебник для вузов. Специальная литература).

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

Результаты обучения	Критерии оценки	Методы оценки
<p>Перечень знаний, осваиваемых в рамках дисциплины: сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; источники угроз информационной безопасности и меры по их предотвращению; жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности.</p>	<p>Полнота ответов, точность формулировок, не менее 75% правильных ответов. Не менее 75% правильных ответов.</p>	<p><b>Текущий контроль при проведении:</b> - устных зачетов; - понятийных диктантов;</p> <p><b>Промежуточная аттестация</b> в форме экзамена</p>
<p>Перечень умений, осваиваемых в рамках дисциплины: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; применять основные правила и документы системы сертификации Российской Федерации; Классифицировать основные угрозы безопасности информации.</p>	<p>Правильность, полнота выполнения заданий, точность формулировок, точность расчетов. Адекватность, оптимальность выбора способов действий, методов, техник, последовательностей действий и т.д. Точность оценки, самооценки выполнения. Соответствие требованиям инструкций, регламентов Рациональность действий и т.д.</p>	<p><b>Текущий контроль при проведении:</b> - практических работ; - оценки результатов самостоятельной работы</p>