Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«**Колледж автоматизации производственных процессов и прикладных информационных систем**»

ПРИНЯТО
Педагогическим советом
Протокол № 9 от 14.06.2024

УТВЕРЖДЕНО
Приказом
СПб ГБПОУ «Колледж автоматизации производства»
от 17.06.2024 № 580

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

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

Квалификация специалиста	техник по защите информации
Форма обучения	очная
Уровень образования, необходимый для приема на обучение по ППССЗ	основное общее образование
Срок получения СПО по ППССЗ	3 года 10 месяцев
Год начала подготовки	2024

Санкт-Петербург – 2024

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности 10.02.01 «Организация и технология защиты информации» (утв. приказом Министерства образования и науки Российской Федерации от 28.07.2014 № 805)

Организация-разработчик: Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Колледж автоматизации производственных процессов и прикладных информационных систем»

Программу составил Обухова А.С., преподаватель СПб ГБПОУ «Колледж автоматизации производственных процессов и прикладных информационных систем»

Программа рассмотрена и одобрена на заседании методической комиссии, протокол № 10 от 10.05.2024.

Заведующий отделом СОП А.Ф. Жмайло

С О Д Е Р Ж А Н И Е

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	– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – применять основные правила и документы системы сертификации Российской Федерации; – классифицировать основные угрозы безопасности информации.	– 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.

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

№ п/п	Вид учебной работы	Объем часов
1.	**Объем работы обучающихся во взаимодействии с преподавателем**	92
2.	**В форме практической подготовки**	92
в *том числе во взаимодействии с преподавателем:*		
	– теоретическое обучение	50
	– практические занятия	42
	– консультации	-
	– промежуточная аттестация в форме экзамена	6
3.	**Самостоятельная внеаудиторная работа обучающихся**	4
Всего по дисциплине в рамках образовательной программы		102

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	
Тема 1. Информационная безопасность в системе национальной безопасности РФ	**Содержание учебного материала**	**8**	**2**	**8**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	1.1. Место информационной безопасности в системе национальной безопасности РФ. Направления государственной политики в области информационной безопасности.	2		2	
	1.2. Источники и содержание угроз в информационной сфере.	2		2	
	1.3. Юридические аспекты защиты информации в РФ.	2		2	
	Практические занятия	**2**	**2**	**2**	
	Практическое занятие № 1. «Изучение Указов Президента РФ № 683 и № 646».	2	2	2	
Тема 2. Критическая информационная инфраструктура (КИИ) РФ	**Содержание учебного материала**	**10**	**2**	**10**	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. Реестр значимых объектов КИИ. Система безопасности значимого объекта КИИ	2		2	
	2.4. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры				
	Практические занятия	**2**	**2**	**2**	
	Практическое занятие № 2. «Использование справочно-правовой системы в ИБ».	2	2	2	
	Содержание учебного материала	**18**	**10**	**18**	ОК 03,

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	
Тема 3. Сущность и понятие информационной безопасности (ИБ), характеристика составляющих ИБ	3.1. Сущность и понятие ИБ. Основные термины и определения. Концептуальная модель ИБ	2		2	ОК 06, ОК 09, ОК 10, ПК 2.4
	3.2. Понятие угрозы, виды угроз. Банк данных угроз безопасности информации ФСТЭК России	2		2	
	3.3. Объекты воздействия угроз. Информационные ресурсы организации. Источники угроз, цели угроз.	2		2	
	3.4. Понятие уязвимости. Виды уязвимостей	2		2	
	Практические занятия	**10**	**10**	**10**	
	Практическое занятие № 3 «Определение угроз ИБ для различных объектов»	2	2	2	
	Практическое занятие № 4 «Работа с официальным сайтом ФСТЭК России»	2	2	2	
	Практическое занятие № 5 «Классификация угроз информационной безопасности»	2	2	2	
	Практическое занятие № 6 «Определение характеристик уязвимости с использованием банка данных уязвимостей»	2	2	2	
	Практическое занятие № 7 «Основные понятия ИБ»	2	2	2	
Тема 4. Информация как объект защиты	**Содержание учебного материала**	**10**	**6**	**10**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4 2
	4.1. Свойства информации с точки зрения ИБ. Виды информации в зависимости от категории доступа.	2		2	
	4.2. Конфиденциальная информация. Жизненный цикл конфиденциальной информации в процессе ее создания, обработки, передачи.	2		2	
	Практические занятия	**6**	**6**	**6**	

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	
	Практическое занятие № 8 «Определение класса ИС персональных данных для организации**»**	2	2	2	
	Практическое занятие № 9 «Составление практических рекомендаций по информационной безопасности**»**	2	2	2	
	Практическое занятие № 10 «Классификация информации по видам тайн и степеням конфиденциальности»	2	2	2	
Тема 5. Меры по предотвращению угроз. Современные средства и способы обеспечения информационной безопасности	**Содержание учебного материала**	**24**	**10**	**24**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	5.1. Направления защиты: правовая, организационная, техническая. Подходы к обеспечению ИБ.	2		2	
	5.2. Правовая защита информации.	2		2	
	5.3. Физическая защита информации. Техническая защита информации. Криптографическая защита информации	2		2	
	5.4. Понятие и виды НСД. Защита от НСД к информации. Защита от вредоносного программного обеспечения	2		2	
	5.5. Идентификация и аутентификация.	2		2	
	5.6. Управление доступом. Модели доступа	2		2	
	5.7. Системы обнаружения вторжений (СОВ). Требо-вания к СОВ	2		2	
	Практические занятия	**10**	**10**	**10**	
	Практическое занятие № 11 «Решение ситуационных задач».	2	2	2	
	Практическое занятие № 12 «Работа с моделями доступа, определение степени конфиденциальности информации»	2	2	2	

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	
	Практическое занятие № 13 «Сравнительный анализ средств антивирусной защиты**»**	2	2	2	
	Практическое занятие № 14 «Использование антивирусного программного обеспечения».	2	2	2	
	Практическое занятие № 15 «Анализ существующих вирусов»	2	2	2	
Тема 6. Защита от внутренних угроз. DLP-системы	**Содержание учебного материала**	**6**	**4**	**6**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	6.1. Понятие DLP-системы. Структура, назначение, функции DLP-системы. Обзор рынка DLP-систем	2		2	
	Практические занятия	**4**	**4**	**4**	
	Практическое занятие № 16 «Закрепление материала по теме «DLP-системы»	2	2	2	
	Практическое занятие № 17 «Определение внутренних угроз информационной безопасности»	2	2	2	
Тема 7. Нарушитель ИБ	**Содержание учебного материала**	**4**	**2**	**4**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	7.1. Понятие нарушителя ИБ. Модели нарушителя ИБ	2		2	
	Практические работы	**2**	**2**	**2**	
	Практическое занятие № 18 «Определение характеристик нарушителя ИБ в зависимости от угрозы информационной безопасности»	2	2	2	
Тема 8. Сертификация и лицензирование	**Содержание учебного материала**	**12**	**6**	**12**	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
	8.1. Система сертификации средств защиты информации. Порядок сертификации. Правила и документы сертификации. Государственный реестр сертифицированных средств защиты информации	2		2	

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	
	8.2. Лицензирование в области защиты информации. Аттестация объектов информатизации по требованиям защиты информации.	2		2	
	Практические занятия	**6**	**6**	**6**	
	Практическое занятие № 19 «Применение правил и документов системы сертификации РФ»	2	2	2	
	Практическое занятие № 20 «Заполнение заявления на сертификацию средства защиты информации»	2	2	2	
	Практическое занятие № 21 «Закрепление материала по теме «Сертификация и лицензирование»	2	2	2	
Самостоятельная работа Заполнение рабочей тетради в СДО на платформе Moodle		**4**			ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4
Промежуточная аттестация		6			
Всего		**102**			

.

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, 2022 - 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 профессионааьное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1209579 (дата обращения: 05.11.2020). – Режим доступа: по подписке.

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. - (Ligitimitate 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 : Тздательство "Лань", 2020. - 324 с. - (Учебник для вузов. Специальная литература).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
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.	Полнота ответов, точность формулировок, не менее 75% правильных ответов. Не менее 75% правильных ответов.	**Текущий контроль при проведении:** - устных зачетов; - понятийных диктантов;
		Промежуточная аттестация в форме экзамена
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.	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.	**Текущий контроль при проведении:** - практических работ; - оценки результатов самостоятельной работы