Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО

на заседании педагогического совета

Протокол № 2

«26» декабря 2023 г.

УТВЕРЖДАЮ

Директор СПб ГБПОУ «АУГСГиП»

_____ А.М. Кривоносов

«26» декабря 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация: Техник по защите информации

Санкт-Петербург
2023 год

Рабочая программа учебной дисциплины ОП.01 Основы информационной безопасности разработана на основе Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки России от 09.12.2016 № 1553.

Программа рассмотрена на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Программа одобрена на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «Основы информационной безопасности»

1.1. Область применения программы

Рабочая программа учебной дисциплины Организационно-правовое обеспечение информационной безопасности является вариативной частью программы подготовки специалистов среднего звена по специальности **10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**, входящей в состав укрупненной группы специальностей **10.00.00. «Информационная безопасность»**

1.2. Место дисциплины в структуре ППССЗ

Учебная дисциплина «Основы информационной безопасности» относится к профессиональному циклу ППССЗ.

1.3. Цели и задачи дисциплины — требования к результатам освоения дисциплины

В результате освоения дисциплины, обучающийся должен **знать**:

— сущность и понятие информационной безопасности, характеристику ее составляющих;

— 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 дисциплины обучающийся должен **уметь**:

— классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

— применять основные правила и документы системы сертификации Российской Федерации;

— классифицировать основные угрозы безопасности информации.

Техник по защите информации должен обладать **общими и профессиональными компетенциями,** включающими в себя способность:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

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

стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

– максимальной учебной нагрузки обучающегося **84** часа, в том числе:
  - обязательной аудиторной учебной нагрузки обучающегося **68** часов;
  - самостоятельной работы обучающегося **10** часов,
  - экзамен 6 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ «Основы информационной безопасности»

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов*
Максимальная учебная нагрузка (всего)	**84**
Обязательная аудиторная учебная нагрузка (всего)	**68**
в том числе:	
– практические занятия	20
Самостоятельная работа обучающегося (всего)	**10**
Промежуточная аттестация в форме **экзамена**	

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем в часах
Тема 1. Критическая информационная инфраструктура (КИИ) РФ	**Содержание учебного материала**	**8**
	1.1. Понятие КИИ. Компоненты КИИ.	2
	1.2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ	2
	1.3. Категорирование объектов КИИ. Реестр значимых объектов КИИ. Система безопасности значимого объекта КИИ	2
	1.4. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	2
Тема 2. Сущность и понятие информационной безопасности (ИБ), характеристика составляющих ИБ	**Содержание учебного материала**	**10**
	2.1. Сущность и понятие ИБ. Основные термины и определения.	2
	2.2. Концептуальная модель ИБ. Понятие угрозы, виды угроз.	2
	2.3. Банк данных угроз безопасности информации ФСТЭК России. Объекты воздействия угроз. Информационные ресурсы организации.	2
	2.4. Источники угроз, цели угроз.	2
	2.5. Понятие уязвимости. Виды уязвимостей	2
	Практические занятия	**6**
	Практическое занятие № 1 «Работа с официальным сайтом ФСТЭК России»	2
	Практическое занятие № 2 «Классификация угроз информационной безопасности»	2
	Практическое занятие № 3 «Определение характеристик уязвимости с использованием банка данных уязвимостей»	2
Тема 3. Информация как объект защиты	**Содержание учебного материала**	**4**
	3.1. Свойства информации с точки зрения ИБ. Виды информации в зависимости от категории доступа.	2
	3.2. Конфиденциальная информация. Жизненный цикл конфиденциальной информации в процессе ее создания, обработки, передачи.	2

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем в часах
	Практические занятия	**2**
	Практическое занятие № 4 «Классификация информации по видам тайн и степеням конфиденциальности»	2
Тема 4. Меры по предотвращению угроз. Современные средства и способы обеспечения информационной безопасности	**Содержание учебного материала**	**16**
	4.1. Направления защиты: правовая, организационная, техническая. Подходы к обеспечению ИБ.	2
	4.2. Физическая защита информации	2
	4.3. Техническая защита информации	2
	4.4. Криптографическая защита информации	2
	4.5. Понятие и виды НСД. Защита от НСД к информации.	2
	4.6. Управление доступом. Модели доступа. Идентификация и аутентификация.	2
	4.7. Защита от вредоносного программного обеспечения	2
	4.8. Системы обнаружения вторжений (СОВ). Требования к СОВ	2
	Практические занятия	**4**
	Практическое занятие № 5 «Работа с моделями доступа, определение степени конфиденциальности информации».	2
	Практическое занятие № 6 «Сравнительный анализ средств антивирусной защиты»	2
Тема 5. Защита от внутренних угроз. DLP-системы	**Содержание учебного материала**	**2**
	5.1. Понятие DLP-системы. Структура, назначение, функции DLP-системы.	2
	Практические занятия	**2**
	Практическое занятие № 7 «Определение внутренних угроз информационной безопасности»	2
Тема 6. Нарушитель ИБ	**Содержание учебного материала**	**2**
	6.1. Понятие нарушителя ИБ. Модели нарушителя ИБ	2

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем в часах
	Практические работы	**2**
	Практическое занятие № 8 «Определение характеристик нарушителя ИБ в зависимости от угрозы информационной безопасности»	2
Тема 7. Сертификация и лицензирование	**Содержание учебного материала**	**6**
	7.1. Система сертификации средств защиты информации. Лицензирование в области защиты информации.	2
	7.2. Порядок сертификации. Правила и документы сертификации. Государственный реестр сертифицированных средств защиты информации	2
	7.3. Аттестация объектов информатизации по требованиям защиты информации.	2
	Практические занятия	**4**
	Практическое занятие № 9 «Применение правил и документов системы сертификации РФ»	2
	Практическое занятие № 10 «Заполнение заявления на сертификацию средства защиты информации»	2
Самостоятельная работа Заполнение рабочей тетради в СДО на платформе Moodle		**10**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета информационной безопасности.

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 обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:

Основная литература

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).

Дополнительная литература

1. Баранова, Е. К. Основы информационной безопасности : учебник/ Е.К. Баранова, А.В. Бабаш. - Москва : РИОР : ИНФРА-М, 2021. — 202 с. — (Среднее про-фессионааьное 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: 05.11.2023). – Режим доступа: по подписке.
2. Воронцова, С.В. Обеспечение информационной безопасности в банковской сфере : монография / С.В. Воронцова.- 2-е изд., стер. - Москва : КНОРУС, 2023. - 160 с. - (Ligitimitate legen et ordinem).
3. Шаханова, М.В. Современные технологии информационной безопасности : учебно-методический комплекс. - Москва : Проспект, 2022. - 216 с.
4. 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).
5. Нестеров, С.А. Основы информационной безопасности : Учебное пособие. - 2-е изд., стер. - Санкт-Петербург : Тздательство "Лань", 2023. - 324 с. - (Учебник для вузов. Специальная литература).

1. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;	Выполнение практических работ
применять основные правила и документы системы сертификации Российской Федерации;	
классифицировать основные угрозы безопасности информации;	
Знания:	
сущность и понятие информационной безопасности, характеристику ее составляющих;	Устные зачеты Устные ответы на экзамене
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;	

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	выбор и применение эффективных методов и способов решения профессиональных задач в профессиональной области; собственная оценка эффективности и качества выполнения заданий.	Проверка качества выполнения практических работ, проверка отчетной документации по практике
Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	эффективный поиск необходимой информации; использование различных источников, включая	Анализ результатов практических работ

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
	электронные	
Планировать и реализовывать собственное профессиональное и личностное развитие	Эффективное планирование профессионального и личного развития	Анализ результатов практических работ
Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	взаимодействие с обучающимися, преподавателями в ходе обучения работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	взаимодействие с обучающимися, преподавателями в ходе обучения	Анализ результатов практических работ
Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Соблюдение режима труда и отдыха, здоровьесберегающих технологий в процессе решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Использовать информационные технологии в профессиональной деятельности	Анализ инноваций в сфере защиты информации; работа с различными прикладными программами	Анализ результатов практических работ

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
Пользоваться профессиональной документацией на государственном и иностранном языках	работа с различными источниками информации	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Анализ результатов практических работ
Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	Использование приемов предпринимательской деятельности в процессе решения профессиональных задач	Анализ результатов практических работ

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проверка технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ;
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Установка и настройка отдельных программных, программно-аппаратных средств защиты информации.	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ;
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ;

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Эксплуатация технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ;