Санкт-Петербургское государственное бюджетное профессиональноеобразовательное учреждение

«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО
На заседании педагогического совета Протокол № 3
«05» июля 2022г

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ ИНФОРМАТИКА

для специальности

10.02.01 «Организация и технология защиты информации»

(базовой подготовки)

Санкт-Петербург – 2022 год

ОДОБРЕНА

Цикловой комиссией

Общетехнических дисциплин

и компьютерных технологий

Протокол № 9

от 24.05.2022 г.

Председатель ЦК

 Андреев В.В.

РАССМОТРЕНА

Методическим советом

СПБ ГБПОУ «АУГСГиП»

Протокол № 6

от «28» июня 2022г.

Рабочая программа учебной дисциплины «Основы информационной безопасности» разработана на основе Федерального государственного образовательного стандарта по специальности 10.02.01 «Организация и технология защиты информации» среднего профессионального образования.

Разработчики:

Андреев В.В., преподаватель СПб ГБПОУ «Академия управления городской средой, градостроительства и печати»

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 «Основы информационной безопасности» является частью программы подготовки специалистов среднего звена (далее – ППССЗ) по специальности 10.02.01 Организация и технология защиты информации.

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;
- 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 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 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразование, осознанно планировать повышение квалификации

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

Формируемые личностные результаты:

ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 9	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 14	Проявляющий сознательное отношение к непрерывному образованию как условию успешно профессиональной и общественной деятельности
ЛР 15	Проявляющий гражданское отношение к профессиональнойдеятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

– максимальной учебной нагрузки обучающегося **147** часов, в том числе:
  - обязательной аудиторной учебной нагрузки обучающегося **98** часов;
  - самостоятельной работы обучающегося **49** 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)	**147**
Обязательная аудиторная учебная нагрузка (всего)	**98**
в том числе:	
– практические занятия	30
Самостоятельная работа обучающегося (всего)	**49**
Промежуточная аттестация в форме **дифференцированного зачета**	

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 часов	Коды формируемых компетенций (ОК,ПК) и личностных результатов (ЛР)
Тема 1. Информационная безопасность в системе национальной безопасности РФ	**Содержание учебного материала**	**6**	ОК1-ОК5;ОК8- ОК9; ПК1.6,ПК1.4,ПК 1.8,ПК2.3,ПК3.1,ПК3. 2,ЛР1,ЛР2,ЛР4,ЛР9,Л Р10,ЛР14,ЛР15
	1.1. Место информационной безопасности в системе национальной безопасности РФ.	2	
	1.2. Направления государственной политики в области информационной безопасности.	2	
	1.3. Источники и содержание угроз в информационной сфере	2	
Тема 2. Критическая информационная инфраструктура (КИИ) РФ	**Содержание учебного материала**	**10**	ОК1-ОК5;ОК8- ОК9; ПК1.6,ПК1.4,ПК 1.8,ПК2.3,ПК3.1,ПК3. 2,ЛР1,ЛР2,ЛР4,ЛР9,Л Р10,ЛР14,ЛР15
	2.1. Понятие КИИ. Компоненты КИИ.	2	
	2.2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ	2	
	2.3. Категорирование объектов КИИ	2	
	2.4. Реестр значимых объектов КИИ. Система безопасности значимого объекта КИИ	2	
	2.5. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	2	
Тема 3. Сущность и понятие информационной безопасности (ИБ), характеристика составляющих ИБ	**Содержание учебного материала**	**20**	ОК1-ОК5;ОК8- ОК9; ПК1.6,ПК1.4,ПК 1.8,ПК2.3,ПК3.1,ПК3. 2,ЛР1,ЛР2,ЛР4,ЛР9,Л Р10,ЛР14,ЛР15
	3.1. Сущность и понятие ИБ. Основные термины и определения. Концептуальная модель ИБ	2	
	3.2. Понятие угрозы, виды угроз. Банк данных угроз безопасности информации ФСТЭК России	2	
	3.3. Объекты воздействия угроз. Информационные ресурсы организации.	2	
	3.4. Источники угроз, цели угроз.	2	
	3.5. Понятие уязвимости. Виды уязвимостей	2	
	Практические занятия	**10**	

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Коды формируемых компетенций (ОК,ПК) и личностных результатов (ЛР)
	Практическое занятие № 1 «Работа с официальным сайтом ФСТЭК России»	2	
	Практическое занятие № 2 «Классификация угроз информационной безопасности»	4	
	Практическое занятие № 3 «Определение характеристик уязвимости с использованием банка данных уязвимостей»	4	
Тема 4. Информация как объект защиты	**Содержание учебного материала**	**8**	ОК1-ОК5;ОК8- ОК9; ПК1.6,ПК1.4,ПК 1.8,ПК2.3,ПК3.1,ПК3. 2,ЛР1,ЛР2,ЛР4,ЛР9,Л Р10,ЛР14,ЛР15
	4.1. Свойства информации с точки зрения ИБ. Виды информации в зависимости от категории доступа.	2	
	4.2. Конфиденциальная информация.	2	
	4.3. Жизненный цикл конфиденциальной информации в процессе ее создания, обработки, передачи.	2	
	Практические занятия	**2**	
	Практическое занятие № 4 «Классификация информации по видам тайн и степеням конфиденциальности»	2	
Тема 5. Меры по предотвращению угроз. Современные средства и способы обеспечения информационной безопасности	**Содержание учебного материала**	**26**	ОК1-ОК5;ОК8- ОК9; ПК1.6,ПК1.4,ПК 1.8,ПК2.3,ПК3.1,ПК3. 2,ЛР1,ЛР2,ЛР4,ЛР9,Л Р10,ЛР14,ЛР15
	5.1. Направления защиты: правовая, организационная, техническая.	2	
	5.2. Подходы к обеспечению ИБ.	2	
	5.3. Физическая защита информации	2	
	5.4. Техническая защита информации	2	
	5.5. Криптографическая защита информации	2	
	5.6. Понятие и виды НСД.	2	
	5.7. Защита от НСД к информации.	2	

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Коды формируемых компетенций (ОК,ПК) и личностных результатов (ЛР)
	5.8. Идентификация и аутентификация.	2	
	5.9. Управление доступом. Модели доступа	2	
	5.10. Защита от вредоносного программного обеспечения	2	
	5.11. 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 6. Защита от внутренних угроз. DLP-системы	**Содержание учебного материала**	**6**	ОК1-ОК5;ОК8- ОК9; ПК1.6,ПК1.4,ПК 1.8,ПК2.3,ПК3.1,ПК3. 2,ЛР1,ЛР2,ЛР4,ЛР9,Л Р10,ЛР14,ЛР15
	6.1. Понятие DLP-системы. Структура, назначение, функции DLP-системы.	2	
	6.2. Обзор рынка DLP-систем	2	
	Практические занятия	**2**	
	Практическое занятие № 7 «Определение внутренних угроз информационной безопасности»	2	
Тема 7. Нарушитель ИБ	**Содержание учебного материала**	**4**	ОК1-ОК5;ОК8- ОК9; ПК1.6,ПК1.4,ПК 1.8,ПК2.3,ПК3.1,ПК3. 2,ЛР1,ЛР2,ЛР4,ЛР9,Л Р10,ЛР14,ЛР15
	7.1. Понятие нарушителя ИБ. Модели нарушителя ИБ	2	
	Практические работы	**2**	
	Практическое занятие № 8 «Определение характеристик нарушителя ИБ в зависимости от угрозы информационной безопасности»	4	
Тема 8. Сертификация и лицензирование	**Содержание учебного материала**	**16**	
	8.1. Система сертификации средств защиты информации.	2	ОК1-ОК5;ОК8- ОК9; ПК1.6,ПК1.4,ПК 1.8,ПК2.3,ПК3.1,ПК3.
	8.2. Порядок сертификации. Правила и документы сертификации. Государственный реестр сертифицированных средств защиты информации	2	

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Коды формируемых компетенций (ОК,ПК) и личностных результатов (ЛР)
	8.3. Лицензирование в области защиты информации.	2	2,ЛР1,ЛР2,ЛР4,ЛР9,ЛР10,ЛР14,ЛР15
	8.4. Аттестация объектов информатизации по требованиям защиты информации.	2	
	Практические занятия	**8**	
	Практическое занятие № 9 «Применение правил и документов системы сертификации РФ»	4	
	Практическое занятие № 10 «Заполнение заявления на сертификацию средства защиты информации»	4	

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, 2016 - 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: 05.11.2020). – Режим доступа: по подписке.
2. Воронцова, С.В. Обеспечение информационной безопасности в банковской сфере : монография / С.В. Воронцова.- 2-е изд., стер. - Москва : КНОРУС, 2017. - 160 с. - (Ligitimitate legen et ordinem).
3. Шаханова, М.В. Современные технологии информационной безопасности : учебно-методический комплекс. - Москва : Проспект, 2017. - 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, 2017. - 208 с. - (Профессиональное образование).
5. Нестеров, С.А. Основы информационной безопасности : Учебное пособие. - 2-е изд., стер. - Санкт-Петербург : Тздательство "Лань", 2016. - 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
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;	

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Обеспечивать технику безопасности при проведении организационно-технических мероприятий	Соблюдение техники безопасности при проведении организационно-технических мероприятий	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Наблюдения при выполнении практических работ.
Применять программно-	Подбор средств	Текущий контроль в

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
аппаратные и технические средства защиты информации на защищаемых объектах	антивирусной защиты на основе сравнительного анализа	форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов. Наблюдения при выполнении практических работ.
Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов	Применение правил и документов системы сертификации РФ	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов.
Проводить регламентные работы и фиксировать отказы средств защиты	Подготовка отчетной и учетной документации	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов. Наблюдения при выполнении практических работ.
Выявлять и анализировать возможные угрозы информационной безопасности объектов	Классификация угроз информационной безопасности, определение характеристик уязвимости с использованием банка данных уязвимостей	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов. Наблюдения при

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
		выполнении практических работ.

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности	проявление интереса к будущей профессии в процессе теоретического обучения, производственной практики	Проверка качества выполнения практических работ, проверка отчетной документации по практике
Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	выбор и применение эффективных методов и способов решения профессиональных задач в профессиональной области; собственная оценка эффективности и качества выполнения заданий.	Анализ результатов практических работ
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	решение стандартных и нестандартных профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	эффективный поиск необходимой информации; использование различных источников, включая электронные	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Использовать информационно-коммуникационные технологии в профессиональной деятельности	работа с различными прикладными программами	Анализ результатов практических работ
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
повышение квалификации		
Ориентироваться в условиях частой смены технологий в профессиональной деятельности	Анализ инноваций в сфере защиты информации; работа с различными прикладными программами	Анализ результатов практических работ