МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Факультет среднего профессионального образования

«УТВЕРЖДАЮ»
Декан факультета СПО, к.т.н.
_____ С.Л. Поляков
«24» декабря 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

образовательной программы

09.02.11 «Разработка и управление программным обеспечением»

Объем дисциплины, часов	48
Учебные занятия, часов	40
в т.ч. лабораторно–практические занятия, часов	20
Самостоятельная работа, часов	8

Санкт-Петербург – 2025

Рабочая программа дисциплины разработана на основе ФГОС по специальности среднего профессионального образования

09.02.11 Разработка и управление программным обеспечением

код *наименование специальности*

РАССМОТРЕНА И ОДОБРЕНА
Цикловой комиссией
вычислительной техники и программирования
Протокол № 5 от 15.12.2025 г.
Председатель: _____/ Рохманько И.Л./

РЕКОМЕНДОВАНА
Методическим
советом факультета СПО
Протокол № 5 от 24.12.2025 г.
Председатель: _____/Шелешнева С.М./

Разработчики:

Попов И.Д., преподаватель первой квалификационной категории

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения рабочей программы

Рабочая программа дисциплины является составной частью программно-методического сопровождения образовательной программы (ОП) среднего профессионального образования (СПО) по специальности 09.02.11 «Разработка и управление программным обеспечением».

1.2. Место дисциплины в структуре ОП СПО

Дисциплина «Основы информационной безопасности» является дисциплиной общепрофессионального цикла.

1.3. Планируемые результаты освоения дисциплины

Код ПК, ОК	Умения	Знания
ОК 01, 02, 09 ПК 1.1, 1.4, 1.5, ПК 3.1-3.3, 3.5, 3.7	– планировать процесс поиска; – структурировать получаемую информацию; – выделять наиболее значимое в перечне информации; – оценивать практическую значимость результатов поиска; – оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; – использовать современное программное обеспечение; – использовать различные цифровые средства для решения профессиональных задач; – понимать тексты на базовые профессиональные темы; – шифрование данных и обеспечивает их конфиденциальность; – анализировать требования безопасности информационных систем; – разрабатывать и реализовывать меры безопасности;	– методы защиты баз данных от внешних угроз; – принципы криптографии и методов шифрования данных; – стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; – методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; – законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; – отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; – современный отечественный и зарубежный опыт в профессиональной деятельности; – принципы и методы обеспечения безопасности информационных систем; – принципы безопасности информационных систем; – современные методы и технологии в области безопасности информационных систем;

	– реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	– законодательные и нормативные акты в области безопасности информационных систем; – источники угроз информационной безопасности и меры по их предотвращению; – основные угрозы безопасности мобильных приложений; – принципы криптографии и шифрования данных; – стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; – законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; – основные принципы безопасности информации и методов ее защиты; – стандартные криптографические алгоритмы для шифрования данных; – принципы обеспечения безопасности передачи данных по сети; – основы безопасности приложений и инфраструктуры; – методы анализа на уязвимости и мониторинга безопасности; – знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; – понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; – знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем дисциплины	**48**
Объем учебных занятий	**40**
в том числе:	
теоретическое обучение	20
лабораторные и практические занятия	20
Самостоятельная учебная работа	**8**
Консультации	**-**
Промежуточная аттестация в форме дифференцированного зачета в 4 семестре	**-**

Практическая подготовка при реализации дисциплины организуется путем проведения практических занятий и (или) лабораторных работ и иных аналогичных видов учебной деятельности, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

2.2. Тематический план и содержание дисциплины ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов / в т.ч. в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
1	2		4
Раздел 1.	**Основы информационной безопасности**	**40/20**	ОК 01, 02, 09 ПК 1.1, 1.4, 1.5, ПК 3.1-3.3, 3.5, 3.7
Тема 1.1. Введение в информационную безопасность	**Содержание учебного материала**	2	
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности.		
Тема 1.2. Управление безопасностью информации	**Содержание учебного материала**	2	
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)		
Тема 1.3. Криптография	**Содержание учебного материала**	2	
	Основы криптографии: симметричные и асимметричные алгоритмы. Стеганография. Применение криптографии в приложениях. Хэширование и цифровые подписи.		
	Практические и лабораторные занятия	**6**	
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.		
Тема 1.4. Защита сетевой инфраструктуры	**Содержание учебного материала**	2	
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.). Использование VPN и межсетевых экранов.		
	Практические и лабораторные занятия	**8**	
	Организация защиты от атак. Организация работы VPN и межсетевого экрана.		
Тема 1.5. Безопасность приложений	**Содержание учебного материала**	2	
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.		
Тема 1.6. Защита данных	**Содержание учебного материала**	2	
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным.		
	Практические и лабораторные занятия	4	
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным.		
Тема 1.7. Безопасность облачных технологий	**Содержание учебного материала**	2	
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности.		
	Практические и лабораторные занятия	**2**	

	Изучение модели облачных услуг и их безопасности.		
Тема 1.8. Инциденты безопасности	**Содержание учебного материала**	2	
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика.		
Тема 1.9. Социальная инженерия и человеческий фактор	**Содержание учебного материала**	2	
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности.		
Тема 1.10. Будущее информационной безопасности	**Содержание учебного материала**	2	
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности.		
Самостоятельная работа обучающихся: 1. Изучение документации OpenSSL. 2. Установка ОС Kali Linux на виртуальную машину. 3. Изучение документации к разным межсетевым экранам.		**8**	ОК 01, 02, 09
Всего:		**48**	-

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Для реализации программы дисциплины предусмотрены следующие специальные помещения: лаборатория компьютерных сетей и основ информационной безопасности.

Оснащение учебных кабинетов и лабораторий установлено в соответствии с протоколом Методического совета факультета: Протокол № 5 от 24.12.2025 г.

3.2. Информационное обеспечение реализации программы

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники

1 Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ИНФРА-М, 2026. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-16-021164-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2207574

Дополнительные источники

1 Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340

2 Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580668

Электронные ресурсы

1 Интернет-версия журнала «Компьютерра». - URL: https://www.computerra.ru/

2 Сайт exponenta.ru. - URL: https://exponenta.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: методы защиты баз данных от внешних угроз; принципы криптографии и методов шифрования данных; стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; современный отечественный и зарубежный опыт в профессиональной деятельности; принципы и методы обеспечения безопасности информационных систем; принципы безопасности информационных систем; современные методы и технологии в области безопасности информационных систем; законодательные и нормативные акты в области безопасности информационных систем; источники угроз информационной безопасности и меры по их предотвращению; основные угрозы безопасности мобильных приложений; принципы криптографии и шифрования данных; стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Знания: – оценка по результатам устного опроса, – экспертное наблюдение за выполнением практических работ, – промежуточная аттестация. Умения: – экспертное наблюдение за выполнением практических работ.

основные принципы безопасности информации и методов ее защиты; стандартные криптографические алгоритмы для шифрования данных; принципы обеспечения безопасности передачи данных по сети; основы безопасности приложений и инфраструктуры; методы анализа на уязвимости и мониторинга безопасности; знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.		
Умения: планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач; понимать тексты на базовые профессиональные темы; шифрование данных и обеспечивает их конфиденциальность;		

анализировать требования безопасности информационных систем; разрабатывать и реализовывать меры безопасности; реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.		