МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ивангородский гуманитарно-технический институт (филиал)
федерального государственного автономного образовательного учреждения высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»
Центр среднего профессионального и дополнительного образования

УТВЕРЖДАЮ
Директор ИФ ГУАП, д.ю.н.

_____В.М. Чибинёв
«25» июня 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

образовательной программы

09.02.11 «Разработка и управление программным обеспечением»

Объем учебного предмета, часов	48
Учебные занятия, часов	40
в т.ч. лабораторно-практические занятия, часов	10
Самостоятельная работа, часов	8

Ивангород – 2026

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

09.02.11 Разработка и управление программным обеспечением ,

код *наименование специальности (ей)*

РАССМОТРЕНА И ОДОБРЕНА
Цикловой комиссией
по специальности «Информационные системы и программирование»
Протокол №6 от 09.06.2026 г.

РЕКОМЕНДОВАНА
Методическим советом
Центра СПиДО ИФ ГУАП

Протокол №7 от 23.06.2026 г.

Председатель:_____ / Сорокин А.А. Председатель:_____ / Ламерт О.В.

Разработчики:

Дагаев А.В., доцент, к.т.н., доцент

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	– распознавать задачу и/или проблему в профессиональном и/или социальном контексте; – анализировать задачу и/или проблему и выделять её составные части; – определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; – составлять план действия; определять необходимые ресурсы; – владеть актуальными методами работы в профессиональной и смежных сферах; – реализовывать составленный план; – оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	– актуальный профессиональный и социальный контекст, в котором приходится работать и жить; – основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; – алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; – структуру плана для решения задач; – порядок оценки результатов решения задач профессиональной деятельности
ОК 02	– определять задачи для поиска информации; – определять необходимые источники информации; – планировать процесс поиска; – структурировать получаемую информацию;	– номенклатура информационных источников, применяемых в профессиональной деятельности; – приемы структурирования информации;

	– 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	– формат оформления результатов поиска информации, современные средства и устройства информатизации; – порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.
ОК 09	– понимать тексты на базовые профессиональные темы	– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности
ПК 1.1	-	– принципы безопасности хранения данных
ПК 1.4	-	– методы защиты баз данных от внешних угроз
ПК 1.5	– шифровать данные и обеспечивать их конфиденциальность	– 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.
ПК 3.1	-	– отраслевая нормативная техническая документация; – источники информации, необходимой для профессиональной деятельности
ПК 3.2	-	– принципы и методы обеспечения безопасности информационных систем
ПК 3.3	– анализ требований безопасности информационных систем	– принципов безопасности информационных систем; – современных методов и технологий в области безопасности информационных систем; – законодательных и нормативных актов в области безопасности информационных систем
ПК 3.5	-	– источники угроз информационной безопасности и меры по их предотвращению

ПК 3.7	– разрабатывать и реализовывать меры безопасности; – реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	– 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 учебного предмета	**48**
Объем учебных занятий	**40**
в том числе:	
теоретическое обучение	30
лабораторно-практические занятия	10
Самостоятельная учебная работа (всего)	**8**
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*	*3*	*4*
Семестр 4		*48/10*	
Раздел 1	**Основы информационной безопасности**	**36/10**	ОК 01 ОК 02 ОК 09 ПК 1.1 ПК 1.4 ПК 1.5 ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 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**	4	
	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. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.		
	Практические занятия	2	
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.		
Тема 1.4. Защита сетевой инфраструктуры	**Содержание учебного материала**	4	
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов		
	Практические занятия	2	
	Организация защиты от атак Организация работы VPN и межсетевого экрана		
Тема 1.5. Безопасность приложений	**Содержание учебного материала**	4	
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.		
	Практическое занятие	1	
	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 занятия	2	
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным		
	Содержание учебного материала	4	

1	*2*	*3*	*4*
Тема 1.7. Безопасность облачных технологий	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности		
	Практическое занятие	1	
	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		
	Практическое занятие	1	
	Работа с инцидентами		
Тема 1.9. Социальная инженерия и человеческий фактор	**Содержание учебного материала**	2	
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности		
	Практическое занятие	1	
	Разработка политики 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 Основные понятия и история информационной безопасности. Актуальные угрозы и риски в информационной безопасности. Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Основы криптографии: симметричные и асимметричные алгоритмы, хэширование. Основы сетевой безопасности и защита от атак. Уязвимости веб-приложений и безопасное программирование. Резервное копирование, восстановление данных и управление доступом.		8	
Дифференцированный зачет		2	
Всего:		**48**	-

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения: лаборатория Вычислительной техники, архитектуры персонального компьютера и периферийных устройств.

Оборудование в соответствии с Распоряжением директора ИФ ГУАП №7 от 17.05.2022.

3.2. Информационное обеспечение реализации программы

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для СПО / А. Н. Баланов. — 3-е изд., стер. — Санкт-Петербург : Лань, 2026. — 84 с. — ISBN 978-5-507-55006-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/515089 — Режим доступа: для авториз. пользователей.

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для СПО / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 284 с. — ISBN 978-5-507-52953-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/463001 — Режим доступа: для авториз. пользователей.

3. Нестеров, С. А. Основы информационной безопасности : учебник для СПО / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2026. — 324 с. — ISBN 978-5-507-56692-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/518575 — Режим доступа: для авториз. пользователей.

Дополнительные источники:

1. Прохорова, О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 7-е изд., стер. — Санкт-Петербург : Лань, 2026. — 124 с. — ISBN 978-5-507-56325-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/515187 — Режим доступа: для авториз. пользователей.

2. Баранова, Е. К. Основы информационней безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2026. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-

01806-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2233508 – Режим доступа: по подписке.

3. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2026. — 337 с. — (Среднее профессиональное образование). - ISBN 978-5-16-019432-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2221361 – Режим доступа: по подписке.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: – актуальный профессиональный и социальный контекст, в котором приходится работать и жить; – основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; – алгоритмы выполнения работ в профессиональной и смежных областях; – методы работы в профессиональной и смежных сферах; – структуру плана для решения задач; – порядок оценки результатов решения задач профессиональной деятельности – номенклатуру информационных источников, применяемых в профессиональной деятельности; – приемы структурирования информации; – формат оформления результатов поиска информации, современные средства и устройства информатизации; – порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; – лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; – принципы безопасности хранения данных; – 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	«Отлично» - теоретическое содержание курса освоено полностью, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но без существенных упущений, 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.

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; – 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: – распознавать задачу и/или проблему в профессиональном и/или социальном контексте;		

– анализировать задачу и/или проблему и выделять её составные части; – определять этапы решения задачи; – выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; – составлять план действия; – определять необходимые ресурсы; – владеть актуальными методами работы в профессиональной и смежных сферах; – реализовывать составленный план; – оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); – определять задачи для поиска информации; – определять необходимые источники информации; – 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.		