Ильина Любовь Николаевна
Подписано: Ильина Любовь Николаевна
DN: cn=Ильина Любовь Николаевна, c=RU, o=ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ", email=ilina@chels.ranepa.ru
Дата: 2026.06.04 12:12:03 +03'00'

Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 Основы информационной безопасности

09.02.11 Разработка и управление программным обеспечением
(код, наименование направление подготовки)

Веб-разработка
(Направленность)

Программист
(квалификация)

Очная
(форма обучения)

Год набора – 2026

Чебоксары

Автор-составитель:
Александрова И.Н., преподаватель Чебоксарского филиала РАНХиГС.

Председатель ЦК:
Александрова И.Н., дисциплин профессиональной подготовки по специальности 09.02.07 Информационные системы и программирование.

Рабочая программа учебной дисциплины одобрена на заседании цикловой комиссии протокол №6 от «21» февраля 2026 г.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4

1.1. Цель и место дисциплины в структуре образовательной программы 4
1.2. Планируемые результаты освоения дисциплины 4

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7

2.1. Трудоемкость освоения дисциплины 7
2.2. Содержание дисциплины 8

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ 9

3.1. Материально-техническое обеспечение 9
3.2. Учебно-методическое обеспечение 9

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ 10

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.05 Основы информационной безопасности»

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «Основы информационной безопасности»: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Дисциплина «Основы информационной безопасности» включена в обязательную часть общепрофессионального цикла образовательной программы.

1.2. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ПОП).

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
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	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	-

	(самостоятельно или с помощью наставника)		
ОК.02	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	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; 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	-
		современный отечественный и зарубежный опыт в 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	применение современных методов и технологий 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	использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные. применение механизмов

		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	хеширования для защиты паролей пользователей от несанкционированного доступа. обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS соблюдение законодательства и регуляций в области защиты данных

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	Объем в часах	В т.ч. в форме практ. подготовки

Учебные занятия	32	16
Самостоятельная работа	10	-
Промежуточная аттестация	-	-
Всего	**32**	**16**

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторных занятий
Раздел 1. Основы информационной безопасности (32 часа)	
Тема 1.1. Введение в информационную безопасность	**Содержание**
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности
	В том числе самостоятельная работа обучающихся
Тема 1.2. Управление безопасностью информации	**Содержание**
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)
	В том числе самостоятельная работа обучающихся
Тема 1.3. Криптография	**Содержание**
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.
	В том числе лабораторных занятий
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.
	В том числе самостоятельная работа обучающихся
Тема 1.4. Защита сетевой инфраструктуры	**Содержание**
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов
	В том числе лабораторных занятий
	Организация защиты от атак
	Организация работы VPN и межсетевого экрана
	В том числе самостоятельная работа обучающихся
Тема 1.5. Безопасность приложений	**Содержание**
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.
	В том числе лабораторных занятий
	Тестирование на проникновение и анализ уязвимостей.
	В том числе самостоятельная работа обучающихся
Тема 1.6. Защита данных	**Содержание**
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным
	В том числе лабораторных занятий
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным
	В том числе самостоятельная работа обучающихся
Тема 1.7. Безопасность	**Содержание**

облачных технологий	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности
	В том числе лабораторных занятий
	Изучение модели облачных услуг и их безопасности
	В том числе самостоятельная работа обучающихся
Тема 1.8. Инциденты безопасности	**Содержание**
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика
	В том числе лабораторных занятий
	Работа с инцидентами.
	В том числе самостоятельная работа обучающихся
Тема 1.9. Социальная инженерия и человеческий фактор	**Содержание**
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности
	В том числе лабораторных занятий
	Разработка политики информационной безопасности
	В том числе самостоятельная работа обучающихся
Тема 1.10. Будущее информационной безопасности	**Содержание**
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности
	В том числе самостоятельная работа обучающихся
Промежуточная аттестация	
Всего 32 часа	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Лаборатория «Основы информационной безопасности», оснащенная в соответствии с приложением 3 ПОП.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. 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

2. 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, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458

3. 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, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587457

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. - М. : ИНФРА-М , 2024. - 416 с. - (Среднее профессиональное образование)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоенности компетенций	Методы оценки
Знает: - 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	Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить; Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте; Знает алгоритмы выполнения работ в профессиональной и смежных областях; Знает методы работы в профессиональной и смежных сферах; Знает структуру плана для решения задач; Может произвести оценку результатов решения задач профессиональной деятельности Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности; Знает приемы структурирования информации; Знает формат оформления результатов поиска информации, современные средства и устройства	– Компьютерное тестирование на знание терминологии по теме – Тестирование – Самостоятельная работа – Наблюдение за выполнением лабораторной работы (деятельностью студента) – Оценка выполнения практического задания – Зачет с оценкой

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 источники информации, необходимые для	информатизации; Может применять современные средства и устройства информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности; Знает принципы безопасности хранения данных; Владеет методами защиты баз данных от внешних угроз Знает принципы криптографии и методов шифрования данных; Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.; Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной	

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	деятельности; Знает современный отечественный и зарубежный опыт в профессиональной деятельности; Владеет принципами и методами обеспечения безопасности информационных систем; Знает принципы безопасности информационных систем; Владеет современными методами и технологиями в области безопасности информационных систем; Знает законодательные и нормативные акты в области безопасности информационных систем; Знает источники угроз информационной безопасности и меры по их предотвращению; Имеет представление об основных угрозах безопасности мобильных приложений; Ориентируется в принципах криптографии и шифрования данных; Знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; Владеет основными принципами безопасности информации и методов ее защиты;	

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. ***Умеет:*** -распознавать задачу и/или проблему в профессиональном и/или социальном контексте; -анализировать задачу и/или проблему и выделять её составные части; - определять этапы	Знает стандартные криптографические алгоритмы для шифрования данных; Имеет представление о принципах обеспечения безопасности передачи данных по сети; Знает основы безопасности приложений и инфраструктуры; Знает методы анализа на уязвимости и мониторинга безопасности; Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Анализирует задачу и/или проблему и может выделить её составные части; Умеет 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;	решения задачи; Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; Составляет план действия; Может определять необходимые ресурсы; Владеет актуальными методами работы в профессиональной и смежных сферах; Может реализовывать составленный план; Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника); Умеет определять задачи для поиска информации; Умеет определять необходимые источники информации; Планирует процесс поиска; Умеет структурировать получаемую информацию; Может выделить наиболее значимое в перечне информации; Умеет оценивать практическую значимость результатов поиска; Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач; Может 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.	Может использовать различные цифровые средства для решения профессиональных задач; Понимает тексты на базовые профессиональные темы; Умеет шифровать данные и обеспечивать их конфиденциальность; Умеет анализировать требования безопасности информационных систем; Может разрабатывать и реализовывать меры безопасности; Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	