

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ»

ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»



УТВЕРЖДАЮ

Заместитель директора по УМР

Е.Ю. Кузнецов

«27» марта 2026 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

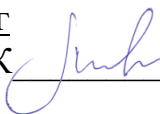
по специальности 09.02.11 Разработка и управление программным обеспечением

РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией

Протокол № 9

«26» марта 2026 г

Председатель ПЦК  Л.И. Логинова/

Рабочая программа учебной дисциплины ОП.05 Основы информационной безопасности разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением.

Разработчик:

Курасов Павел Александрович, преподаватель с ученой степенью кандидата технических наук, проектирования и производства электронно-вычислительных машин ФГБОУ ВО «Поволжский государственный технологический университет»

Рецензент (внутренний)

Кузнецов Е.Ю., преподаватель с ученой степенью кандидата технических наук, заместитель директора по УМР Высшего колледжа ПГТУ «Политехник»

Рецензент (внешний)

Савинов А.Н., преподаватель с ученой степенью кандидата технических наук, доцент кафедры информационно-вычислительных систем ФГБОУ ВО «Поволжский государственный технологический университет»

Рецензент (представитель работодателя)

Рыбаков А.Е., генеральный директор ООО «ОМЕГА-СОФТ»

СОДЕРЖАНИЕ

1. АННОТАЦИЯ
2. ОБЩАЯ ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ
3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
4. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. АННОТАЦИЯ

Рабочая программа учебной дисциплины ОП.05 Основы информационной безопасности является частью программы подготовки специалистов среднего звена (ППССЗ) по специальности среднего профессионального образования 09.02.11 Разработка и управление программным обеспечением.

Цель дисциплины – 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.

Общий объем учебной нагрузки по дисциплине составляет 46 часов, нагрузка во взаимодействии с преподавателем составляет 40 часов, самостоятельной работы – 6 часов.

Содержание дисциплины включает изучение следующих разделов/тем:

- Введение в информационную безопасность.
- Управление безопасностью информации.
- Криптография
- Защита сетевой инфраструктуры.
- Безопасность приложений.
- Защита данных
- Безопасность облачных технологий
- Инциденты безопасности
- Социальная инженерия и человеческий фактор
- Будущее информационной безопасности

В результате освоения учебной дисциплины ОП.05 Основы информационной безопасности обучающийся должен овладеть предусмотренными ФГОС умениями, знаниями, которые формируют следующие **компетенции**:

Код результата обучения	Результат обучения
1	2
Общие и профессиональные компетенции	
ОК.01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК.02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК.09	Пользоваться профессиональной документацией на государственном и иностранном языках.
ПК 1.1	Проектировать базы данных
ПК 1.4	Администрировать базы данных.
ПК 1.5	Защищать информацию в базе данных с использованием технологии защиты информации.
ПК 3.1	Собирать исходные данные для разработки проектной документации на информационную систему.
ПК 3.2	Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.
ПК 3.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.
ПК 3.5	Интегрировать информационную систему с существующими информационными системами заказчика.
ПК 3.7	Разрабатывать техническую документацию на эксплуатацию информационной системы.

Текущий контроль успеваемости осуществляется в процессе проведения теоретических и лабораторных занятий, обеспечивает оценивание хода освоения дисциплины. Формы текущего контроля успеваемости: тестирование, устный опрос, доклад, выполнение лабораторных работ, защита обучающимися индивидуальных заданий, проектов и др.

Форма промежуточной аттестации – дифференцированный зачет (3 семестр).

2. ОБЩАЯ ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Место дисциплины в структуре программы подготовки специалистов среднего звена:

Дисциплина ОП.05 Основы информационной безопасности входит в общепрофессиональный цикл профессиональной подготовки ППССЗ и реализуется в 3 семестре.

2.2 Цель и планируемые результаты освоения дисциплины

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 (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; 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 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	использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные. применение механизмов хеширования для защиты паролей

		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	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
--	--	---	---

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Объем учебной дисциплины и виды учебной работы

Вид учебной деятельности	Объем в часах
Объем учебной дисциплины	46
Суммарная учебная нагрузка во взаимодействии с преподавателем	40
в том числе:	
лекционные занятия	20
лабораторные занятия	20
практические занятия <i>(если предусмотрены)</i>	-
контрольные работы <i>(если предусмотрены)</i>	-
курсовая работа (проект) <i>(если предусмотрена)</i>	-
Самостоятельная работа	6
Консультации	-
Промежуточная аттестация	-
<i>Итоговая форма контроля - дифференцированный зачет (3 семестр)</i>	

3.2 Тематический план и содержание учебной дисциплины ОП.05 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Формируемые компетенции
1	2	3	4
Тема 1.1 Введение в информационную безопасность	Содержание учебного материала	2	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	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	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	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	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.		
	Лабораторные работы	4	
	Работа с симметричными и асимметричными алгоритмами.		
	Хэширование и создание цифровой подписи сообщения.		
Тема 1.4 Защита сетевой инфраструктуры	Содержание учебного материала	2	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.		
	Лабораторные работы	4	
	Организация защиты от атак		
	Организация работы VPN и межсетевого экрана		
Тема 1.5 Безопасность приложений	Содержание учебного материала	2	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.		
	Лабораторные работы	2	
	Тестирование на проникновение и анализ уязвимостей.		
Тема 1.6 Защита данных	Содержание учебного материала	2	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным		
	Лабораторные работы	4	
	Выполнение резервного копирования и восстановления данных.		
	Управление доступом к данным		

	Самостоятельная работа обучающихся	2	
Тема 1.7 Безопасность облачных технологий	Содержание учебного материала	2	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности		
	Лабораторные работы	2	
	Изучение модели облачных услуг и их безопасности		
	Самостоятельная работа обучающихся	2	
Тема 1.8 Инциденты безопасности	Содержание учебного материала	2	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика		
	Лабораторные работы	2	
	Работа с инцидентами.		
Тема 1.9 Социальная инженерия и человеческий фактор	Содержание учебного материала	2	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности		
	Лабораторные работы	2	
	Разработка политики информационной безопасности		
	Самостоятельная работа обучающихся	2	
Тема 1.10 Будущее информационной безопасности	Содержание учебного материала	2	ОК.01, ОК.02, ОК.09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1-ПК 3.3, ПК 3.5, ПК 3.7
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности		
Всего		46	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

4.1. Материально-техническое обеспечение учебной дисциплины

Реализация программы дисциплины требует наличия:

Кабинет математических дисциплин

Комплект мебели для учебного процесса.

Мультимедийное оборудование: компьютеры-12 шт; АО "РАМЭК-ВС" Core i3 12100F/16Гб/512Гб SSD Apacer AS2280 P4U /NVIDIA Geforce RTX 3050 8Гб/кл. мышь, NVIDIA GeForce GT730 ПЗУ:- SSD 256 Гб 12 шт.; монитор 24" PHILIPS 243V c, 12 шт.

Программное обеспечение: 1С:Предприятие 8. Комплект для обучения (лицензия №8922961); Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); КОМПАС-3D; nanoCAD; СПДС 23.0; Яндекс Браузер; Draw.io, Git, Java SE Development Kit, Qt Designer, Visual Studio Code, Postman, MySQL Workbench.

Средства обучения: доска маркерная 120*240см, шкаф для хранения учебной и методической литературы.

Лаборатория компьютерных сетей и основ информационной безопасности

Комплект мебели для учебного процесса.

Мультимедийное оборудование: компьютеры- 12 шт: ПК Intel Core i3/GA-H310-D3H/DDRIV 16Gb/500Gb SATAIII/INWIN EAR003, монитор 24" Samsung S24F350FHI, клавиат., мышь; NVIDIA GeForce GT730 ПЗУ:- SSD 256 Гб 12 шт.;

Программное обеспечение: Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); Draw.io, Qt Designer, Visual Studio Code, Postman, MySQL Workbench.

Средства обучения: доска маркерная, шкаф для хранения учебной и методической литературы

Лаборатория алгоритмизации и программирования

Комплект мебели для учебного процесса.

Мультимедийное оборудование: компьютеры - 15 шт.: ПК H404,2 420W/Intel Core i3 540/клав., мышь, монит. 21,5" VA2248-LED; ПК RAY S902.4(клав. мышь оптич. пачкорд, ИДТО ,монитор 21,5 " View Sonic VA2248-LED; монитор 17" LCD PROVIEW VA-796KN; принтер струйный рулон. HP500 120*600.

Программное обеспечение: «Адепт: Управление строительством» (контракт № А-859); Autodesk AutoCAD (регистрация на сайте производителя); Autodesk ReCap (регистрация на сайте производителя); CREDO DAT 5.2 (лицензия №1249.28749.28.08-13); MapInfo Professional (лицензионный договор №32/2014-У); Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); Draw.io, Qt Designer, Visual Studio Code, Postman, MySQL Workbench; P7-Графика; Git; Anaconda3; PyCharm Professional Edition, Eclipse IDE for Java, Postman; комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); справочная правовая система «Консультант Плюс» (контракт №2025_СВ_2 от 04.12.2024 г); Renga (лицензия №ДЛ-19-00224); SCAD Office s64 (лицензия № 15417); STARK ES 2019 (лицензия №066700); ГИС "Карта 2011" (сетевой USB-ключ); КОМПАС-3D V19 (лицензия №Вг-20-00154); ЛИРА-САПР 2018 PRO (сублицензионный контракт № 3641/ЙО от 21.09.2018 г.); Смета-Багира 4.0 (лицензия №4475).

Средства обучения: источник бесп.питания APC Smart UPS 1000VA USB 2U 230V; коммутатор Cisco Catalyst WS C2960-24 PC-L; коммутатор Cisco Catalyst WS - C2960-48 TC-L; коммутатор WS-C2960-48TT с конвертором, шкаф для хранения учебной и методической литературы.

4.2. Информационное обеспечение учебной дисциплины

Основная и дополнительная литература

№ п/ п	Список используемой литературы (печатные издания, электронные издания за последние 5 лет)	Количество экземпляров, имеющихся в библиотеке, или ссылка на ЭБС
ОСНОВНАЯ ЛИТЕРАТУРА		
1	Бубнов, А. А. Основы информационной безопасности: учебное издание / Бубнов А. А., Пржегорлинский В. Н., Савинкин О. А. - Москва : Академия, 2024. - 256 с. (Специальности среднего профессионального образования). – ISBN 978-5-0054-1646-9 URL: https://academia-moscow.ru/catalogue/5549/792068/ (дата обращения: 10.06.2026)	Электронный ресурс
2	Белов, Е. Б. Основы информационной безопасности: Учебное пособие для вузов / Е.Б. Белов и др. - Москва : Гор. линия-Телеком, 2011. - 558 с.: ил.; . - (Специальность; Учебное пособие для высших учебных заведений). ISBN 5-93517-292-5, 100 экз. - Текст: электронный. - URL: https://znanium.ru/catalog/product/405159 (дата обращения: 10.06.2026)	Электронный ресурс
Дополнительная литература		
1.	Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст: электронный. - URL: https://znanium.ru/catalog/product/1189328 (дата обращения: 10.06.2026)	Электронный ресурс

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в форме текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по дисциплине за период обучения. Форма промежуточной аттестации – дифференцированный зачет.

Текущий контроль успеваемости осуществляется в процессе проведения лабораторных работ, обеспечивает оценивание хода освоения дисциплины.

Формы текущего контроля успеваемости: тестирование, устный опрос, доклады, выполнение лабораторных работ.

Результаты обучения	Показатели освоённости 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 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;	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 информатизации; Может применять современные средства и устройства информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; Владеет лексическим	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

- 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; - основные принципы безопасности информации и методов ее защиты; - стандартные криптографические алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети;	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 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	
---	---	--

- 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 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	НПРАА; Владеет основными принципами безопасности информации и методов ее защиты; 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; 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	
--	--	--

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.	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; 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.	
---	--	--

Критерии оценивания результатов обучения по дисциплине, шкала оценивания

Критерии оценивания:

- усвоение программного теоретического материала (объем знаний, глубина усвоения);
- умение излагать программный материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания на практике.

Шкала оценивания:

Результаты сдачи дифференцированного зачета оцениваются по шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, который глубоко и прочно усвоил программный материал, проявляет знание основной и дополнительной литературы, грамотно, логически стройно и аргументировано излагает материал, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с практическими заданиями.

Оценка «хорошо» выставляется обучающемуся, твердо знающему программный материал, который излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, не испытывает затруднений с ответами на вопросы.

Оценка «удовлетворительно» выставляется обучающемуся, который имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

Дополнения и изменения к рабочей программе на учебный год

Дополнения и изменения к рабочей программе на _____ учебный год по дисциплине _____

В рабочую программу внесены следующие изменения:

Дополнения и изменения в рабочей программе обсуждены на заседании ПЦК

«_____» _____ 20____ г. (протокол № _____).

Председатель ПЦК _____ / _____ /