МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

РОСТОВСКОЙ ОБЛАСТИ

**«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ СВЯЗИ И ИНФОРМАТИКИ»**

**Рабочая программа дисциплины**

**ОП.05 Основы информационной безопасности**

программы подготовки специалистов среднего звена

по специальности

**09.02.11 Разработка и управление программным обеспечением**

**2025г.**

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  программирования  Протокол № 1 от 1 сентября. 2025 года  Председатель ЦК  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.Н. Сулавко | **УТВЕРЖДАЮ:**  Зам. директора по УМР  \_\_\_\_\_\_\_\_\_\_\_\_И.В. Подцатова  «2\_» сентября 2025 г. |

# Рабочая программа 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 (приказ Минпросвещения России от 24.02.2025 № 138).

**Разработчик:** государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики»

[СОДЕРЖАНИЕ ПРОГРАММЫ](#_Toc208139214)

[1. Общая характеристика рабочей программы учебной дисциплины](#_Toc208139215)

[1.1. Цель и место дисциплины в структуре образовательной программы](#_Toc208139216)

[1.2. Планируемые результаты освоения дисциплины](#_Toc208139217)

[2. Структура и содержание дисциплины](#_Toc208139218)

[2.1. Трудоемкость освоения дисциплины](#_Toc208139219)

[2.2. Содержание дисциплины](#_Toc208139220)

[3. Условия реализации дисциплины](#_Toc208139221)

[3.1. Материально-техническое обеспечение](#_Toc208139222)

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

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 (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 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 | использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные.  применение механизмов 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 | 60 | 20 |
| Лекционные занятия | 36 |  |
| Практические занятия | 24 | 20 |
| Самостоятельная работа | - | - |
| Промежуточная аттестация - дифференцированный зачет | ХХ | ХХ |
| Всего | **60** | **20** |

**2.1.1. Количество часов на освоение программы дисциплины (за счет объема времени обязательной и вариативной частей ППСС):**

- объем образовательной нагрузки –60 часов (из них 28 часов за счет объема времени вариативной части);

| **Дополнительные требования к результатам освоения ППССЗ** | |
| --- | --- |
| **Умения** | **Знания** |
| -классифицировать защищаемую информацию по видам;  - применять основные правила и документы системы защиты информации;  -классифицировать основные угрозы безопасности информации;  -составлять модель нарушителя;  -осуществлять способы защиты ПДн.  - осуществлять защиту информации с применением программных и программно-аппаратных СИЗ; | -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. |

– практическая подготовка – 20 часов;

в том числе:

– всего учебных занятий – 60 часа,

из них: – теоретическое обучение – 36 часов (из них 14 часов за счет объема времени вариативной части),

– практических (лабораторных) занятий - 24 часа (из них 14 часов за счет объема времени вариативной части).

Практическая подготовка при реализации учебной дисциплины ОП.05 Основы информационной безопасности по специальности 09.02.11 Разработка и управление программным обеспечением организуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

2.2. Содержание дисциплины

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование разделов и тем** | **Содержание учебного материала, практических и лабораторных занятий** | **Объем часов** | **Формируемые общие компетенции и профессиональ ные компетенции** |
| **Раздел 1. Основы информационной безопасности** | |  |  |
| **Тема 1.1. Введение в информационную безопасность** | **Содержание** | **2** |  |
| Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности | 2 | ОК.01  ОК.02  ОК.09 |
| **Тема 1.2. Управление безопасностью информации** | **Содержание** | **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.) | 4 | ОК.01  ОК.02  ОК.09  ПК.1.1 |
| **Тема 1.3. Криптография** | **Содержание** | **6** |  |
| Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография. | 4 | ОК.01  ОК.02  ОК.09  ПК.1.1  ПК.1.4 |
| **В том числе практических и лабораторных занятий** | **2** |  |
| **Практическое занятие № 1** Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения. | 2 | ПК.1.1  ПК.1.4 |
| **Тема 1.4. Защита сетевой инфраструктуры** | **Содержание** | **8** |  |
| Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов | 4 | ОК.01  ПК.1.1  ПК.1.4  ПК.1.5 |
| **В том числе практических и лабораторных занятий** | **4** |  |
| **Практическое занятие № 2** Организация защиты от атак | 2 | ПК.1.1  ПК.1.4  ПК.1.5 |
| **Практическое занятие № 3** Организация работы VPN и межсетевого экрана | 2 | ПК.1.1  ПК.1.4  ПК.1.5 |
| **Тема 1.5. Безопасность приложений** | **Содержание** | **6** |  |
| Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей. | 4 | ОК.02  ПК.3.1  ПК.3.2  ПК.3.3 |
| **В том числе практических и лабораторных занятий** | **2** |  |
| **Практическое занятие № 4** Тестирование на проникновение и анализ уязвимостей. | 2 | ОК.02  ПК.3.1  ПК.3.2  ПК.3.3 |
| **Тема 1.6. Защита данных** | **Содержание** | **6** |  |
| Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным | 2 | ОК.02  ПК.3.1  ПК.3.5  ПК.3.7 |
| **В том числе практических и лабораторных занятий** | **4** |  |
| **Практическое занятие № 5** Выполнение резервного копирования и восстановления данных. Управление доступом к данным | 4 | ОК.02  ПК.3.1  ПК.3.5  ПК.3.7 |
| **Тема 1.7. Безопасность облачных технологий** | **Содержание** | **8** |  |
| Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности | 4 | ОК.02  ПК.3.3  ПК.3.5  ПК.3.7 |
| **В том числе практических и лабораторных занятий** | **4** |  |
| **Практическое занятие № 6** Изучение модели облачных услуг и их безопасности | 4 | ОК.02  ПК.3.3  ПК.3.5  ПК.3.7 |
| **Тема 1.8. Инциденты безопасности** | **Содержание** | **8** |  |
| Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика | 4 | ОК.09  ОК.02  ПК.3.3  ПК.3.5  ПК.3.7 |
| **В том числе практических и лабораторных занятий** | **4** |  |
| **Практическое занятие № 7**  Работа с инцидентами. | 4 |  |
| **Тема 1.9. Социальная инженерия и человеческий фактор** | **Содержание** | **8** |  |
| Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности | 4 | ОК.09  ОК.02  ПК.3.3  ПК.3.5  ПК.3.7 |
| **В том числе практических и лабораторных занятий** | **4** |  |
| **Практическое занятие № 8** Разработка политики информационной безопасности | 4 | ОК.09  ОК.02  ПК.3.3  ПК.3.5  ПК.3.7 |
| **Тема 1.10. Будущее информационной безопасности** | **Содержание** | **2** |  |
| Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности | 2 | ОК.01  ОК.02  ПК.3.5  ПК.3.7 |
| **Промежуточная аттестация – дифференцированный зачет** | | **2** |  |
| **Всего часов** | | **60** |  |

3. Условия реализации ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Лаборатория «Информационной безопасности»:

Учебная мебель; мультимедийный проектор;

Автоматизированные рабочие места на 25 обучающихся с конфигурацией: процессор Core i5, 16 Гб ОЗУ, диагональ дисплея 23”, мышь, клавиатура;

программное обеспечение: Astra Linux; Visio; Adobe Photoshop; Microsoft Office 2007; Adobe Acrobat Reader DC; Яндекс. Баузер;

справочная правовая система Консультант Плюс; 7-Zip. Коммутаторы Cisco Catalyst 3650 24 Port PoE 4x1G Uplink IP Services;

коммутатор D-Link DGS-1024C/A1A;IP-телефон Cisco UC phone 7975; межсетевой экран Cisco ASA 5506 c лицензией Security Plus;

маршрутизатор CISCO2911/k9;

коммутатор Cisco WS-C2960-24TC-L;

маршрутизатор Cisco ISR 4321 (2GE,2NIM,4G FLASH,4G DRAM, IPB); маршрутизатор Cisco 2911

3.2. Учебно-методическое обеспечение

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

**3.2.1. Основные печатные и/или электронные издания**

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547 (дата обращения: 16.11.2024).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950 (дата обращения: 16.11.2024).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 16.11.2024)

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082 (дата обращения: 16.11.2024).

**3.2.2. Основные электронные издания:**

1. Основы информационной безопасности. Издательство: РИОР. Авторы: Баранова Елена Константиновна, Бабаш Александр Владимирович.

<https://znanium.ru/catalog/document?id=451828>

2. Основы информационной безопасности. Вид издания: Учебное пособие. Уровень образования: Среднее профессиональное образование. Издательство: НИЦ ИНФРА-М.Автор: Сычев Юрий Николаевич.

<https://znanium.ru/catalog/document?id=468550> .

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 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 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.  ***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 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. | 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 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 HIPAA;  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 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. | Экспертное наблюдение выполнения практических работ и видов работ по практике  Диагностика (тестирование, контрольные работы) |

Лист согласования

**Дополнения и изменения к рабочей программе на учебный год**

Дополнения и изменения к рабочей программе на \_\_\_\_\_\_\_\_\_\_ учебный год по дисциплине Наименование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В рабочую программу дисциплины «…» внесены следующие изменения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дополнения и изменения в рабочей программе дисциплины «…» обсуждены на заседании ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Протокол № \_\_\_от «\_\_\_\_» \_\_\_\_\_\_\_\_ 20\_\_г.

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_