Министерство образования Красноярского края

краевое государственное бюджетное профессиональное образовательное учреждение

«Красноярский колледж радиоэлектроники и информационных технологий»

****

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**«ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

для студентов специальности:

09.02.11 Разработка и управление программным обеспечением

Красноярск, 2025

Составлена в соответствии с федеральным государственным образовательным стандартом СПО по специальности 09.02.11 Разработка и управление программным обеспечением

|  |  |
| --- | --- |
| ОДОБРЕНО  старший методист  \_\_\_\_\_\_\_\_\_\_ Т.В. Клачкова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025г. | УТВЕРЖДАЮ  Заместитель директора  по учебной работе  \_\_\_\_\_\_\_\_\_\_\_\_\_\_М.А. Полютова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025г. |

РАССМОТРЕНО

на заседании цикловой комиссии укрупненной группы09.00.00

Информационная и вычислительная техника №1

Протокол от «\_\_\_» \_\_\_\_\_\_\_2025г № \_\_\_

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.А. Ивашова

АВТОР: Методический совет КГБПОУ ККРИТ

ПРОВЕРЕНО

Методист

\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.И. Макарова

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025г

СОДЕРЖАНИЕ ПРОГРАММЫ

[СОДЕРЖАНИЕ ПРОГРАММЫ 44](#_Toc208139544)

[1. Общая характеристика ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 45](#_Toc208139545)

[1.1. Цель и место дисциплины в структуре образовательной программы 45](#_Toc208139546)

[1.2. Планируемые результаты освоения дисциплины 45](#_Toc208139547)

[2. Структура и содержание ДИСЦИПЛИНЫ 48](#_Toc208139548)

[2.1. Трудоемкость освоения дисциплины 48](#_Toc208139549)

[2.2. Примерное содержание дисциплины 49](#_Toc208139550)

[3. Условия реализации ДИСЦИПЛИНЫ 50](#_Toc208139551)

[3.1. Материально-техническое обеспечение 50](#_Toc208139552)

[3.2. Учебно-методическое обеспечение 50](#_Toc208139553)

[4. Контроль и оценка результатов освоения ДИСЦИПЛИНЫ 51](#_Toc208139554)

1. Общая характеристика ПРИМЕРНОЙ 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[[1]](#footnote-1):

|  |  |  |  |
| --- | --- | --- | --- |
| **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

|  |  |
| --- | --- |
| **Вид учебной работы** | **Объем в часах** |
| **Обязательная учебная нагрузка** | 49 |
| в том числе: | |
| теоретическое обучение | 15 |
| практические занятия (если предусмотрено) | 30 |
| Самостоятельная работа | 8 |
| **Консультации** | **4** |
| **Дифференцированный зачет 2 семестр** |  |

* 1. Тематический план и содержание учебной дисциплины

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование разделов и тем** | **Содержание учебного материала и формы организации деятельности обучающихся** | **Объем часов** | **Коды компетенций, формированию которых способствует элемент программы** |
| 1 | 2 | 3 | 4 |
| **Раздел 1. Основы информационной безопасности** | | ***49*** |  |
| **Тема 1.1. Введение в информационную безопасность** | **Содержание учебного материала** | ***1*** |  |
| Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности | 1 | 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 |
| **В том числе практических и лабораторных занятий** |  |
| **Самостоятельная работа** |  |
| **Тема 1.2. Управление безопасностью информации** | **Содержание учебного материала** | ***1*** |  |
| Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.) | 1 | 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 |
| **В том числе практических и лабораторных занятий** |  |
| **Самостоятельная работа** |  |
| **Тема 1.3. Криптография** | **Содержание учебного материала** | ***7*** |  |
| Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография. | 1 | 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 |
| **В том числе практических и лабораторных занятий**  Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения. | 6 |
| **Самостоятельная работа** | 1 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Тема 1.4. Защита сетевой инфраструктуры** | **Содержание учебного материала** | ***7*** |  |
| Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов | 1 | 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 |
| **В том числе практических и лабораторных занятий**  Организация защиты от атак  Организация работы VPN и межсетевого экрана | 6 |
| **Самостоятельная работа** | 1 |
| **Тема 1.5. Безопасность приложений** | **Содержание учебного материала** | ***5*** |  |
| Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей. | 2 | 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 |
| **В том числе практических и лабораторных занятий**  Тестирование на проникновение и анализ уязвимостей. | 3 |
| **Самостоятельная работа** | 1 |
| **Тема 1.6. Защита данных** | **Содержание учебного материала** | ***5*** |  |
| Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным | 2 | 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 |
| **В том числе практических и лабораторных занятий**  Выполнение резервного копирования и восстановления данных. Управление доступом к данным | 3 |
| **Самостоятельная работа** | 1 |
| **Тема 1.7. Безопасность облачных технологий** | **Содержание учебного материала** | ***4*** |  |
| Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности | 1 | 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 |
| **В том числе практических и лабораторных занятий**  Изучение модели облачных услуг и их безопасности | 3 |
| **Самостоятельная работа** | 1 |
| **Тема 1.8. Инциденты безопасности** | **Содержание учебного материала** | ***7*** |  |
| Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика | 1 | 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 |
| **В том числе практических и лабораторных занятий**  Работа с инцидентами. | 6 |
| **Самостоятельная работа** | 1 |
| **Тема 1.9. Социальная инженерия и человеческий фактор** | **Содержание учебного материала** | ***5*** |  |
| Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности | 2 | 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 |
| **В том числе практических и лабораторных занятий**  Разработка политики информационной безопасности | 3 |
| **Самостоятельная работа** | 1 |
| **Тема 1.10. Будущее информационной безопасности** | **Содержание учебного материала** | ***2*** |  |
| Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности | 2 | 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 |
| **В том числе практических и лабораторных занятий** |  |
| **Самостоятельная работа** | 1 |
| **Консультация** | | **4** |  |
| **Дифференцированный зачет** | | 2 | 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 |
| **Всего** | | 57/49 |  |

1. Условия реализации ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Лаборатория «Компьютерных сетей и основ информационной безопасности», оснащенная:

- посадочных мест учащихся, рабочее место преподавателя, маркерная доска, ПО (Linux KUbuntu, onlyoffice, 7-zip, Яндекс Браузер, OBS Studio, Proxmox, Node.js, Git, Visual Studio Code,Postman), в соответствии с содержанием дисциплины: авторский электронный учебник, учебно-методический комплекс дисциплины, модуля. Технические средства обучения: персональный компьютер (процессор Core i3, оперативная память объемом 8 Гб) с выходом в Интернет, МФУ, интерактивная доска, справочные пособия, медиатека (мультимедиа разработки и презентации к урокам).

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 электронные издания**

1. Бабаш, А. В., Информационная безопасность. Лабораторный практикум + еПриложение : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КноРус, 2025. — 131 с. — (электронный учебник ЭБС)
2. Елин, В. М., Организационное и правовое обеспечение информационной безопасности : учебное пособие / В. М. Елин, А. К. Жарова. — Москва : КноРус, 2025. — 207 с. — (электронный учебник ЭБС)
3. Записной, Д. В., Английский язык в сфере информационной безопасности. Практикум по устной речи : учебное пособие / Д. В. Записной. — Москва : КноРус, 2025. — 189 с. — (электронный учебник ЭБС)
4. Литвиненко, В.И. Основы информационной безопасности : Учебное пособие / В.И. Литвиненко, Е.С. Козлов — Москва : КноРус, 2026. — 199 с. — (электронный учебник ЭБС)
5. Медведев, В. А., Информационная безопасность. Введение в специальность + еПриложение:Тесты : учебник / В. А. Медведев. — Москва : КноРус, 2024. — 143 с. — (электронный учебник ЭБС)
6. Пестунова, Т. М., Информационная безопасность и защита информации: краткое введение и практикум : учебное пособие / Т. М. Пестунова, А. А. Перов. — Москва : Русайнс, 2025. — 132 с. — (электронный учебник ЭБС)

**3.2.2. Дополнительные печатные и 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)

# **3.3. Общие требования к организации образовательного процесса в том числе и для обучающихся с ОВЗ и инвалидностью**

Теоретическую часть учебной дисциплины и практические занятия планируется проводить в учебных аудиториях, лабораториях и учебных мастерских, участие в организации производственной деятельности структурного подразделения.

Корректировка содержания общеобразовательной дисциплины для **обучающихся инвалидов и лиц с ОВЗ** проводиться в соответствиисразработанными Методическими рекомендациями для преподавателей по работе с обучающимися-инвалидами и обучающимися с ограниченными возможностями здоровья <https://disk.yandex.ru/i/l5hSPg7_FH3-VQ>

Образование обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья, а именно освоения данной дисциплины может быть организовано как совместно с другими обучающимися, так и по индивидуальному учебному плану, в том числе с использованием дистанционных образовательных технологий. В этом случае каждый преподаватель предусматривает специальные условия для реализации его особых образовательных потребностей. Вариант реализации адаптированной образовательной программы для конкретного обучающегося инвалида или обучающегося с ограниченными возможностями здоровья определяется в соответствии с рекомендациями, данными по результатам медико-социальной экспертизы или психолого-медико-педагогической комиссии, а также специальными условиями, созданными в колледже. При обучении инвалидов и обучающихся с ограниченными возможностями здоровья уделяется внимание **индивидуальной работе**, направленной на установление контакта между преподавателем и обучающимися. Индивидуальное обучение позволяет полностью индивидуализировать содержание, методы и темпы учебной деятельности инвалида, следить за каждым его действием и операцией при решении конкретных задач, вносить вовремя необходимые коррекции как в деятельность студента-инвалида, так и в деятельность преподавателя. Также обучение обучающихся инвалидов и обучающихся с ОВЗ может **осуществляться и с применением дистанционных технологий**. Дистанционное обучение позволяет обеспечивать возможности коммуникаций не только с преподавателем, но и с другими обучаемыми, сотрудничество в процессе познавательной деятельности. Важно проводить учебные мероприятия, способствующие сплочению группы, направленные на совместную работу, обсуждение, принятие группового решения. Эффективной формой работы является проведение **онлайн-занятий** (вебинары), которые используются для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы. Учебные материалы, предназначенные для обучающихся-инвалидов и обучающихся с ОВЗ размещены на сайте колледжа в СДО Moodle по каждой дисциплине, а также, на Академия Медиа 3.5, Google Classroom. При этом подбор и разработка учебных материалов производится преподавателем с учетом того, чтобы студенты с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально с использованием специальных программ и технических средств, перечисленных в рабочих программах дисциплин. При проведении учебных занятий преподаватели используют мультимедийные комплексы, электронные учебники и учебные пособия, адаптированных к ограничениям здоровья обучающихся:

- для лиц с нарушениями зрения: − в печатной форме увеличенным шрифтом; − в форме электронного документа; − в форме аудиофайла; − в печатной форме на языке Брайля;

- для лиц с нарушениями слуха: − в печатной форме; − в форме электронного документа; − в форме видеофайла (при условии сопровождения титрами или сурдопереводом);

- для лиц с нарушениями опорно-двигательного аппарата: - в печатной форме; − в форме электронного документа; − в форме аудио- или видеофайла.

При реализации программ среднего профессионального образования с применением электронного обучения и дистанционных образовательных технологий преподавателям рекомендуется своевременно отвечать на вопросы обучающихся инвалидов и обучающихся с ОВЗ и регулярно оценивать работу с использованием различных возможностей для взаимодействия друг с другом. Подбор и разработка учебных материалов производиться с учетом возможности предоставления материала в различных формах, обеспечивающих обучающимся с нарушениями слуха получение информации визуально, с нарушениями зрения - аудиально.

3.4. Кадровое обеспечение образовательного процесса

Реализация образовательной программы обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, и имеющими стаж работы в данной профессиональной области не менее трех лет.

Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах (при наличии).

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, не реже одного раза в три года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее трех лет в организациях, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, в общем числе педагогических работников, реализующих программы профессиональных модулей образовательной программы, должна быть не менее 25 процентов.

* 1. Обучение с применением элементов электронного обучения и дистанционных образовательных технологий

Изучение дисциплины ОП.05 Основы информационной безопасности возможно с применением элементов электронного обучения и ДОТ. Электронный учебно-методический комплекс данной дисциплины разработан и размещен на платформах по ссылке:

1. 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) |

1. *Берутся сведения, указанные по данному виду деятельности в п. 4.2.* [↑](#footnote-ref-1)