

## АННОТАЦИЯ

Рабочая программа дисциплины «Основы информационной безопасности» является составной частью программно-методического сопровождения образовательной программы (ОП) среднего профессионального образования (СПО) по специальности 09.02.11 «Разработка и управление программным обеспечением».

Дисциплина «Основы информационной безопасности» является дисциплиной общепрофессионального цикла.

В результате освоения учебной дисциплины обучающийся должен уметь:

- 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.

В результате освоения учебной дисциплины обучающийся должен знать:

- 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

#### НІРАА;

- 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.

Количество часов на освоение программы дисциплины, часов - 48.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме дифференцированного зачета в 4 семестре.

Язык обучения по дисциплине: русский.