

Аннотация к рабочей программе дисциплины

Автор: Антонова О.В., старший преподаватель

Наименование дисциплины: Б1.О.35 Автоматизированные системы обработки информации

Цели освоения дисциплины:

изучение основных направлений развития исследований в области автоматизированных систем обработки информации и наиболее значительных перспективных проектов

1. Требования к результатам освоения дисциплины:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1 Организует и поддерживает выполнение комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации	<i>Знать:</i> задачи программно-технического обеспечения информационной безопасности в организации и политику безопасности в автоматизированных системах. <i>Уметь:</i> выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации. Умеет организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности на защищаемом объекте. <i>Владеть:</i> навыками формирования и реализации политики информационной безопасности на защищаемом объекте. Владеет навыками разработки и применения системы безопасности, прикладными и инструментальными средствами создания систем информационной безопасности.

<p>ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах</p>	<p>ОПК-4.1.2 Обеспечивает блокирование возможных каналов утечки информации через технические средства с помощью специальных устройств</p>	<p><i>Знать:</i> принципы устройства и функционирования средств криптографической и технической защиты информации. Знает принципы организации информационной безопасности автоматизированных систем в соответствии с требованиями по защите информации.</p> <p><i>Уметь:</i> интегрировать средства криптографической и технической защиты информации в автоматизированные системы при решении задач профессиональной деятельности.</p> <p><i>Владеть:</i> методами установки и настройки криптографических и технических средств защиты информации.</p>
<p>ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах</p>	<p>ОПК-4.1.3 Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности в автоматизированных системах</p>	<p><i>Знать:</i> базовый понятийный аппарат в области информационной безопасности, структуру политики безопасности и основные законодательно-правовые положения защиты информации, виды и состав угроз информационной безопасности и меры их предотвращения.</p> <p><i>Уметь:</i> классифицировать угрозы информационной безопасности. применительно к объектам защиты, грамотно применять основные законы и нормативные документы в области информационной безопасности.</p> <p><i>Владеть:</i> навыками анализировать состояние информационной безопасности на конкретном объекте защиты, способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.</p>

<p>ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем</p>	<p>ОПК-4.4.1 Способен диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции систем защиты автоматизированных систем</p>	<p><i>Знать:</i> особенности и способы применения программных и программно-аппаратных средств защиты информации автоматизированных систем. <i>Уметь:</i> обеспечивать работоспособность, обнаруживать и устранять неисправности. <i>Владеть:</i> навыками тестирования, диагностики и настройки компонентов систем защиты информации автоматизированных систем</p>
<p>ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем</p>	<p>ОПК-4.4.2 Способен осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации</p>	<p><i>Знать:</i> типовые средства и методы ведения аудита, средств и способов защиты информации автоматизированных систем. <i>Уметь:</i> осуществлять регистрацию основных событий в автоматизированных (информационных) системах <i>Владеть:</i> навыками работы с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе.</p>
<p>ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем</p>	<p>ОПК-4.4.3 Применяет типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа</p>	<p><i>Знать:</i> типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. <i>Уметь:</i> устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации. <i>Владеть:</i> навыками мониторинга и регистрации сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.</p>

2. Содержание дисциплины:

- Тема 1. Введение в предметную область проектирования систем
- Тема 2. Общая характеристика процесса проектирования АСОИУ
- Тема 3. Разработка функциональной модели
- Тема 4. Разработка модели и защита данных
- Тема 5. Создание модели в стандарте IDEF0
- Тема 6. Разработка модели АСОИУ
- Тема 7. Защита данных в АСОИУ
- Тема 8. Разработка пользовательского интерфейса
- Тема 9. Дизайн пользовательского интерфейса
- Тема 10. Разработка алгоритмов
- Тема 11. Метод грубой силы
- Тема 12. Метод декомпозиции
- Тема 13. Логический анализ структур АСОИ
- Тема 14. Процесс анализа системы
- Тема 15. Управление проектом АСОИ
- Тема 16. Графическое представление планирования
- Тема 17. Инструментальные средства проектирования АСОИ
- Тема 18. Архитектура компонентов РНР для доступа к БД
- Тема 19. Средства РНР для организации форм ввода данных

3. Общая трудоёмкость дисциплины: 3 ЗЕ.