

Аннотации модулей программы повышения квалификации «Большие данные в обеспечении кибербезопасности»

Содержание модуля 1

Тема 1.1. Сущность, специфика и источники больших данных

Теория и практика больших данных. Методики анализа больших данных. Аналитические инструменты больших данных. Рынки решений для управления большими данными. Платформы больших данных (BDP, Big Data Platform).

Тема 1.2. Основные процессы больших данных: Data Mining и Data Extraction

Использование априорных представлений об анализируемых данных. Наглядное представление результатов анализа (визуализация). Структуризация неструктурированных данных. Текстовая аналитика. Разметка текстов и медиафайлов. "Скрытые" знания. Описательные и прогностические задачи. Закономерности ("паттерны"). Алгоритмы поиска закономерностей. Аналитика больших данных. Поиск ассоциативных правил. Группировка объектов, кластерный анализ. Использование регрессионных моделей. Классификация объектов.

Тема 1.3. Аналитические инструменты больших данных, нейросети

Искусственный нейрон. Искусственная нейронная сеть. Однослойный персептрон. Многослойные нейронные сети. Обучение искусственной нейронной сети. Эффект переобученности сети. Экстраполяция данных с использованием искусственных нейронных сетей. Метод входного окна.

Механизмы анализа big data. Алгоритм построения деревьев решений. Файл имён переменных. Файл данных. Файл стоимости ошибки. Структура правила.

Оптимизация методом градиентного спуска. Генетические алгоритмы: суть, основные компоненты, алгоритм функционирования. Операторы генетических алгоритмов. Селекция. Скрещивание. Мутация. Применение генетических алгоритмов.

Содержание модуля 2

Тема 2.1. Теоретические основы кибербезопасности.

Понятие информационной безопасности. Составляющие информационной безопасности. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Модели безопасности. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408.

Тема 2.2. Анализ и управление рисками в сфере информационной безопасности.

Модель безопасности с полным перекрытием. Управление информационной безопасностью. Методики построения систем защиты информации. Модель Lifecycle Security. Модель многоуровневой защиты. Методика управления рисками, предлагаемая MS. Протоколы IPSec и трансляция сетевых адресов. Межсетевые экраны. Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей.

Тема 2.3. Технологии электронной цифровой подписи и блокчейна в решении задач кибербезопасности

Использование защищенных компьютерных систем. Методы криптографии. Основные понятия криптографии. Открытый текст. Шифротекст. Криптографический алгоритм. Шифр Цезаря. Вскрытие шифра методом лобовой атаки. Понятие надежности криптографического алгоритма. Дополнительные задачи криптографического алгоритма - аутентификация источника сообщения, целостность, неотрицание авторства.

Алгоритмы симметричного шифрования. Шифрование с общим ключом. Проблема секретности общего ключа. Шифрование блоками и потоком. Раунды циклического алгоритма и подключи. Сеть Фейштеля. Дифференциальный и линейный криптоанализ. Алгоритм DES.

Криптография с открытым ключом. Алгоритмы шифрования с открытым ключом. Открытый и закрытый ключ. Алгоритм RSA. Алгоритм DSS. Обмен сессионных ключей. Виды криптосистем: симметричные криптосистемы, криптосистемы с открытым ключом, гибридные криптосистемы.

Хеш-функции и аутентификация сообщений. Цифровая подпись. Цифровой сертификат

Закон РФ «Об электронной цифровой подписи». Требования к хеш-функциям. Простые и сложные хеш-функции. Хеш-функция MD-5. Цифровая подпись. Прямая и арбитражная цифровые подписи. Стандарт цифровой подписи DSS. Цифровые сертификаты. Доверительные центры.

Основные термины и понятия технологии блокчейна. Принципы работы блокчейн-технологии. Анализ сферы применения и интеграции в бизнес-процессы. Обзор платформ для разработки блокчейн-проекта. Архитектура блокчейн-проекта.

Блокчейн-технологии для развития бизнеса BusinessDevelopment. Аудит безопасности смарт-контрактов.

Содержание модуля 3

Тема 3.1. Большие данные как инструмент обеспечения кибербезопасности.

Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика.

Механизмы обеспечения информационной безопасности. Идентификация и аутентификация. Методы разграничение доступа. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).

Тема 3.2. Поддержка принятия решений в области кибербезопасности на основе больших данных.

Экспертные системы. Модели представления знаний. Типовая структура экспертной системы. Задачи, решаемые с помощью экспертных систем. Мировой опыт внедрения. Примеры экспертных систем.

Тема 3.3. Большие данные как объект защиты в рамках решения задач кибербезопасности.

Основные технологии построения защищённых информационных систем. Оценки стоимости проведения мероприятий по безопасности. Вопросы разработки и реализации политики безопасности. Управление доступом. Аудит систем. Системы отчетности по безопасности. Сканирование уязвимых мест информационных систем. Место информационной безопасности информационных систем в национальной безопасности страны.

Зам. директора

Смоленского филиала Финуниверситета



Мосийчук А.В.