АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

С.2. ДВ Криптографические методы
защиты информации

Семестр: 7
Количество часов: 72
Количество зачетных единиц: 2
Промежуточная аттестация: зачет

Место дисциплины в структуре ООП:

Дисциплина «Криптографические методы защиты информации» относится к дисциплинам по выбору математического и естественнонаучного цикла С.2.ДВ учебного плана подготовки специалиста по специальности 38.05.01 *Экономическая безопасность* специализация «Экономико-правовое обеспечение экономической безопасности».

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении дисциплин: «Информатика», «Математика», «Информационные системы в экономике».

Цель и задачи освоения дисциплины:

Целью дисциплины «Криптографические методы защиты информации» является формирование у специалистов представления о современных методах обработки, преобразования и защиты информации в современных компьютерных системах, о современных способах борьбы с несанкционированным блокированием, доступом, копированием, изменением и сбором информации; развитие способностей и профессиональных навыков, связанных с организацией систем обеспечения информационной безопасности посредством шифрования данных, изучения общих подходов к криптоанализу, алгоритмов шифрования и дешифрования.

Для достижения поставленной цели студентам необходимо решить следующие основные задачи:

- сформировать знания о средствах и методах криптоанализа и защиты информации;
- развить способности и профессиональные навыки, связанные с организацией систем обеспечения информационной безопасности;
- приобрести практические навыки по применению изученных средств и алгоритмов шифрования и дешифрования.

Содержание дисциплины:

Предмет и задачи криптографии. Основные определения. Требования к криптографическим системам защиты информации. Реализация криптографических методов. Сведения из истории криптографии. Криптографические атаки. Криптографический протокол.

Общая схема симметричного шифрования. Методы замены: одноалфавитная замена, пропорциональные шифры, многоалфавитные

подстановки, методы гаммирования. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Требования к блочному алгоритму шифрования. Сеть Фейштеля.

Основные сведения. Шифрование. Расшифрование. Двухкратный DES и атака «встреча посередине». Трехкратный DES. Алгоритм Rijndael. Режимы работы блочных алгоритмов. Структура раунда ГОСТ 28147-89. Процедуры шифрования и расшифрования. Основные режимы шифрования. Отличия алгоритмов шифрования по ГОСТ 28147-89 и DES.

Понятие хеш-функции. Использование блочных алгоритмов шифрования для формирования хеш-функции. Поточные шифры. Принципы использования генераторов псевдослучайных чисел при потоковом шифровании. Линейный конгруэнтный генераторы псевдослучайных чисел. Метод Фибоначчи с запаздыванием. Генератор псевдослучайных чисел на основе алгоритма BBS. Генераторы псевдослучайных чисел на основе сдвиговых регистров с обратной связью. Использование режимов OFB и CTR блочных шифров для получения псевдослучайных чисел. Алгоритм RC4. Управление секретными ключами.

Односторонние функции. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с открытым ключом. Формирование секретных ключей с использованием асимметричных алгоритмов. Требования к алгоритмам шифрования с открытым ключом.

В результате освоения учебной дисциплины обучающийся должен обладать следующими общекультурными (ОК) и профессиональными (ПК) компетенциями**:**

ОК-16 Способен работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, применять в профессиональной деятельности автоматизированные информационные системы, используемые в экономике, автоматизированные рабочие места, проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач (*знать* методы и средства получения, хранения и поиска информации; *уметь* использовать их в своей профессиональной деятельности; *владеть* современными методиками обработки и передачи информации.

ПК-16 Способен осуществлять расследование экономических преступлений в форме дознания (*знать* мероприятия по получению юридически значимой информации, анализировать и оценивать ее; *уметь* давать оценку профессиональной ситуации в контексте анализа общих социально-экономических проблем; *владеть* навыками предупреждения, пресечения, раскрытия и расследования преступлений и иных правонарушений в сфере экономики.

ПК-23 Способен соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности (*знать* основные нормативные руководящие документы, касающиеся государственной тайны; *уметь* применять полученные знания для

обеспечения информационной безопасности; *владеть* навыками разработки стратегии защиты от преступников и предотвращения компьютерных преступлений.

ПК-46 Способен принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов (*знать* основные понятия и концепцию информационной безопасности; основные средства и способы защиты информации; *уметь* выявлять и классифицировать основные угрозы безопасности информации; *владеть* средствами средства защиты информации от разглашения, разрушения, несанкционированного доступа и т.д).

Образовательные технологии:

Дисциплина предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий в зависимости от вида и цели учебного занятия: компьютерные симуляции, деловые и ролевые игры, мастер-классы, разбор конкретных ситуаций.

Теоретический материал излагается на лекционных занятиях в форме проблемно-ориентированных лекций.

Лабораторные занятия ориентированы на закрепление теоретического материала, изложенного на лекционных занятиях, а также на приобретение дополнительных знаний, умений и практических навыков осуществления аналитической и профессиональной деятельности с применением интерактивных форм обучения (моделирование деловых ситуаций, подготовка презентаций, групповые дискуссии).

С целью формирования и развития профессиональных навыков студентов предлагается использовать проектную технологию, портфолио, визуальные презентации теоретического материала.

Составитель: К. С. Смолич, к. т. н, доцент кафедры прикладной информатики.