

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

С2.В.ОД.1 Информационная безопасность

Семестр: 8

Количество часов: 144

Количество зачетных единиц: 4

Промежуточная аттестация: -

Место дисциплины в структуре ООП:

Дисциплина «Информационная безопасность» относится к вариативной части математического и естественнонаучного цикла С2.В 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», «Информационные системы в экономике».

Цель и задачи освоения дисциплины:

Целью дисциплины «Информационная безопасность» является формирование у специалистов сведений и знаний о современном состоянии и проблемах обеспечения информационной безопасности компьютерных систем, существующих угрозах, основ правового регулирования отношений в информационной сфере, получение навыков работы в ложной сетевой информационной среде современного предприятия и механизмов их реализации.

Для достижения поставленной цели студентам необходимо решить следующие основные задачи:

- развить современный образ мышления в отношении значимости информации как объекта, подлежащего защите от посягательств со стороны злоумышленников;
- сформировать знания о средствах и методах защиты информации;
- приобрести практические навыки по применению изученных средств и методов защиты конфиденциальной информации.

Содержание дисциплины:

Понятие информационной безопасности в широком и узком смысле. Основные составляющие информационной безопасности. Информационные войны и информационное оружие. Связь информационной безопасности с другими сферами деятельности общества. Ценность информации. Информация как товар. Угрозы доступности, целостности и конфиденциальности информации.

Основные составляющие национальных интересов РФ в информационной сфере. Комплексное обеспечение информационной безопасности государства. Области и объекты обеспечения информационной безопасности и защиты информационной деятельности. Доктрина информационной безопасности РФ. Со-

временные подходы к технологиям и методам обеспечения информационной безопасности. Основные проблемы информационной безопасности в РФ.

Уровни обеспечения информационной безопасности. Структура государственной системы обеспечения информационной безопасности. Законодательный уровень информационной безопасности. Отечественные и международные нормативно-правовые акты обеспечения информационной безопасности.

Организационный уровень обеспечения информационной безопасности: правила построения системы защиты информации, методы и средства обеспечения информационной безопасности в системах переработки информации.

Политика безопасности. Уровни информационной безопасности: административный, процедурный, программно-технический уровень. Принципы архитектурной безопасности и критерии защищенности информационных систем. Управление рисками информационной безопасности. Аудит информационной безопасности предприятий.

Модели противодействия угрозам безопасности: модели предоставления прав, вероятностные модели, модели Биба, модели защиты информационной системы при отказе в обслуживании, модели анализа безопасности программного обеспечения.

Организация противодействия технической разведке. Методологические основы технического обеспечения защиты процессов переработки информации и контроля её эффективности. Криптографическая защита и программно-аппаратные средства защиты информации. Автоматизация технического контроля защиты потоков информации. Эффективность защиты и методология её расчета.

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-14 Способен реализовывать мероприятия по получению юридически значимой информации, анализировать и оценивать ее, эффективно использовать в интересах выявления рисков и угроз экономической безопасности, предупреждения, пресечения, раскрытия и расследования преступлений и иных правонарушений в сфере экономики (*знать* теоретические основы обеспечения информационной безопасности; понятие информационной безопасности; основные угрозы безопасности; виды противников или «нарушителей»; виды компьютерных

вирусов; *уметь* анализировать нарушения информационной безопасности; применять полученные знания для обеспечения информационной безопасности; *владеть* навыками получения юридически значимой информации, анализировать и оценивать ее).

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.