Аннотация рабочей программы дисциплины «Информационная безопасность»

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Цель изучения дисциплины – сформировать знания о принципах и способах противодействия опасностям и угрозам, возникающим в процессе развития современного информационного общества в сфере информационной безопасности.

1.2 Задачи учебной дисциплины:

- ознакомить студентов с современными технологиями, применяемыми в решении задач информационной безопасности, моделями возможных угроз, нормативными документами, терминологией и основными понятиями теории защиты информации;
- приобрести практические навыки анализа и выбора методов и средств защиты компьютерной информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

2.1. Цикл (раздел) ООП:

Дисциплина «Информационная безопасность» относится к базовой части дисциплин профессионального цикла (М2.Б).

2.2. Взаимосвязь дисциплины с другими дисциплинами ООП

Дисциплина тесно связана с такими курсами, как: «Базы данных», «Теория систем и системный анализ», «Вычислительные системы, сети и телекоммуникации». Основные положения дисциплины могут быть использованы в дальнейшем при изучении следующих дисциплин: «Управление информационными системами», «Проектирование информационных систем», «Информационный менеджмент» и др.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

Компетенции обучающегося, формируемые в результате освоения дисциплины:

Код соответствующей компетенции по ГОС	Наименование компетенций	Результат освоения (знать, уметь, владеть)
ОПК-1	способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий	**Знать:** - нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий. **Уметь:** - использовать нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий для организации защиты информации. **Владеть:** - международными и отечественными стандартами в области обеспечения

		безопасности информационных систем и технологий.
ОПК-3	способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности	**Знать:** - основы защиты информации. **Уметь:** - реализовывать меро-приятия для обеспечения на предприятии (в организации) деятельности в области защиты информации. **Владеть:** - навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях.
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** - виды угроз ИС и методы обеспечения информационной безопасности. **Уметь:** - применять методы анализа прикладной области на концептуальном, логическом, и алгоритмическом уровнях с целью выявления угроз безопасности. **Владеть:** - способностью блокировать угрозы безопасности ИС предприятия с помощью методов обеспечения защиты информации.
ПК-7	способностью эксплуатировать и сопровождать ИС и сервисы	**Знать:** - принципы эксплуатации и сопровождения информационных систем и сервисов с точки зрения обеспечения защиты от вредоносного ПО. **Уметь:** - эксплуатировать и сопровождать информационные системы и сервисы с точки зрения их защиты от вредоносного ПО.. **Владеть:**

		- принципами эксплуатации и сопровождения информационных систем и сервисов с точки зрения их защиты от вредоносного ПО.
ПК-10	способностью принимать участие в организации ИТ-инфраструктуры в управлении информационной безопасностью	**Знать:** - типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду. **Уметь:** - использовать типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду. **Владеть:** - навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях.
ПК-12	способностью осуществлять и обосновывать выбор проектных решений по видам обеспечения информационных систем	**Знать:** - принципы и методы разработки политики безопасности на предприятии. **Уметь:** - разрабатывать документы определяющие политику безопасности на предприятии. **Владеть:** - технологиями разработки и реализации политики безопасности на предприятии.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Технологии и методы обеспечения ИБ

Тема 1.1 Основные понятия ИБ. ИБ в системе национальной безопасности России.

Тема 1. 2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба.

Тема 1. 3. Угрозы информационной безопасности.

Тема 1.4 Политика безопасности и формирование организационной структуры системы защиты

информации на предприятии
Тема 1.5. Технологии защиты от вредоносных программ и спама.
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность.
Тема 1.7. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия.
Тема 1.8. Основные принципы и методы в области технической защиты информации
Тема 1.9. Противодействие несанкционированному доступу к конфиденциальной информации
Тема 1.10. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ.
Тема 1.11. Международные стандарты информационной безопасности. COBIT
Тема 1.12. Практические аспекты безопасности ИС.
Тема 1.13. Обеспечение безопасности ОС. Безопасность Windows 7.
Тема 1.14. Криптографические методы защиты информации. Классификация криптографических методов защиты.
Тема 1.15. Симметричные криптографические алгоритмы
Тема 1.16. Ассиметричные криптографические алгоритмы
Тема 1.17. Цифровая электронная подпись (ЭЦП)
Тема 1.18. Технологии аутентификации

Раздел 2. Информационная безопасность ИС и сетей
Тема 2.1 Проблемы информационной безопасности сетей
Тема 2.2 Угрозы и уязвимости проводных корпоративных сетей
Тема 2.3 Технология защиты межсетевого обмена данными. Брандмауэры.
Тема 2.4 Технологии VPN
Тема 2.5 ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP
Тема 2.6 Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне.
Тема 2.7 Защита на сетевом уровне — протокол IPSec. Инфраструктура защиты на прикладном уровне

5. ОБРАЗОВАТЕЛЬНЫЕТЕХНОЛОГИИ

Традиционные технологии (лекция, практическое занятие, консультация, зачет); репродуктивный, продуктивный, активный методы обучения; информационно-коммуникационные технологии.

Разработчики рабочей программы:
***Семичастный И.Л.** , к.т.н., доцент кафедры информационных технологий*