Информационная безопасность

1 Цель дисциплины:

Овладение знаниями по основным уровням информационной безопасности, происхождению угроз, развитие умений применения современных методов и технологий защиты информации на ПК и в сетях, антивирусного программное обеспечение, методов шифрования информации; развитие творческих навыков при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности личности, общества и государства.

Задачи дисциплины:

- развить и дополнить знания студентов, полученных в результате изучения других предметов, по основам защиты информации;
- рассмотреть понятие внешних и внутренних угроз, направленных на компьютерную систему;
- рассмотреть уровни безопасности компьютерных систем и дать представление об современных методах защиты информации на соответствующих уровнях;
- рассмотреть понятие вируса и его функциональные возможности;
- изучить антивирусное программное обеспечение и получить навыки работы с ним;
- рассмотреть современные технологии шифрования информации.
- рассмотреть вопросы обеспечения информационной безопасности личности, общества и государства;

2 Место дисциплины в структуре ООП:

Дисциплина «Информационная безопасность» относится к специальным дисциплинам профессионального цикла (Б1.Б.12).

Для освоения дисциплины «Информационная безопасность» обучающиеся используют знания, умения, навыки и установки, сформированные в ходе изучения дисциплин «Информатика и программирование», «Вычислительные системы, сети и телекоммуникации», «Операционные системы», «Информационные системы и технологии».

Освоение дисциплины «Информационная безопасность» не является необходимой основой для последующего изучения каких-либо дисциплин.

Междисциплинарные связи разделов и (или) тем дисциплины с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	Наименование разделов (темы) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин				
		Информационные угрозы и уровни обеспечения информационной безопасности.	Информационные угрозы и уровни обеспечения информационной безопасности.	Информационные угрозы и уровни обеспечения информационной безопасности.	Информационные угрозы и уровни обеспечения информационной безопасности.	Информационные угрозы и уровни обеспечения информационной безопасности.
1	Информатик		+			+

	а и программирование					
2	Вычислительные системы, сети и телекоммуникации		+	+	+	+
3	Операционные системы		+		+	+
4	Информационные системы и технологии	+	+	+	+	+

3 Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-4 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

В результате изучения дисциплины студент должен:

Знать:

- основные угрозы безопасности компьютерным системам; законодательство в информационной сфере; основные средства и приемы борьбы с угрозами возникающие в компьютерных системах, основные методы криптографической защиты информации;

- цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства; основные термины по проблематике информационной безопасности; правовые аспекты обеспечения информационной безопасности; методологию создания систем защиты информации; перспективные направления развития систем и методов защиты информации; современные подходы к построению систем защиты информации; компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

Уметь:

- выявлять и классифицировать угрозы информационной безопасности; разрабатывать модели злоумышленников, схемы решения проблем безопасности в компьютерных системах; создавать препятствия проникновению в компьютер и сеть нежелательной информации; находить и использовать новые средства защиты информации в условиях появления новых угроз; разрабатывать политики информационной безопасности организации, обосновывать организационно-технические мероприятия по защите информации в ИС; реализовывать защиту информационных систем от компьютерных вирусов и других вредоносных программ; применять методы и средства защиты конфиденциальной информации, включая криптографические средства; оформлять необходимую документацию.

Владеть:

- навыками установки и эксплуатации антивирусного программного обеспечения; работы с криптографическим программным обеспечением; установки электронных средств компьютерной защиты; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую

тайну, а также персональных данных; работы с инструментальными средствами защиты информации.

4 Общая трудоемкость дисциплины составляет 3 зачетных единиц.