

**Аннотация рабочей программы дисциплины «Информационная безопасность»
для специальности 38.05.01 Экономическая безопасность, специализация № 1
образовательной программы – Экономико-правовое обеспечение экономической
безопасности**

1. Цели и задачи освоения дисциплины

Цель дисциплины: заложить терминологический фундамент, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучить угрозы нарушения целостности, доступности, конфиденциальности информации и противодействия этим нарушениям.

Задачами дисциплины являются формирование знаний у студентов о современном состоянии проблемы обеспечения информационной безопасности при использовании компьютерных технологий, видах обеспечения информационной безопасности, методах и средствах защиты информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Вместе с другими дисциплинами ОП дисциплина «Информационная безопасность» обеспечивает формирование следующих компетенций:

способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12);

способностью проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности (ПК-32).

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

Знать: основные методы, способы и средства хранения, систематизации, обработки, передачи информации; задачи, методы, средства обеспечения и стандарты информационной безопасности; нормативные правовые акты в области защиты государственной тайны и информационной безопасности; методы и критерии оценки эффективности мероприятий по защите информации.

Уметь: различать правовые, организационные и технические мероприятия по защите информации; выявлять и классифицировать угрозы информационной безопасности предприятия; планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия; проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности; использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну, и иной служебной информации, рассчитывать эффективность мероприятий по защите информации

Владеть: навыками работы с различными источниками информации, информационными ресурсами и технологиями, навыками обеспечения защиты информации; современной терминологией в области информационной безопасности; навыками работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.

3. Содержание дисциплины

Актуальность проблемы обеспечения безопасности информации. Угрозы информационной безопасности. Вредоносное ПО. Компьютерные вирусы и средства защиты от них. Правовое обеспечение информационной безопасности. Организационные методы защиты информации. Основные программно-аппаратные меры.