**Аннотация к рабочей программе учебной дисциплины**

**Основы криптографии**

**Специальность**: 38.05.01 Экономическая безопасность

**Специализация**: Экономико-правовое обеспечение экономической безопасности

1. **Компетенции, формируемые в результате освоения дисциплины:**

**ПСК-2 –** способностью применять в обеспечении безопасности экономической деятельности средства и методы предупреждения недобросовестной конкуренции, в том числе навыки подготовки и реализации оперативных комбинаций с соблюдением требований конспирации;

**ПК-15 –** способностью применять в профессиональной деятельности теоретические основы раскрытия и расследования преступлений, использовать в целях установления объективной истины по конкретным делам технико-криминалистические методы и средства, тактические приемы производства следственных действий, формы организации и методику раскрытия и расследования отдельных видов и групп преступлений;

**ПК-16 –** способностью использовать при решении профессиональных задач особенности тактики проведения оперативно-служебных мероприятий в соответствии со спецификой будущей профессиональной деятельности.

**2. Содержание учебной дисциплины**

|  |  |
| --- | --- |
| **№ п/п** | **Разделы учебной дисциплины** |
| 1 | Понятие криптографии. История и основные направления развития современной защитой информации. Место и роль криптографии в системах обеспечения экономической безопасности.  |
| 2 | Криптография с открытым и секретным ключами. Модели передачи информации в криптосистемах с открытым и секретным ключами. Построение криптосистем на основе арифметики на эллиптических кривых. |
| 3 | Основы криптоанализа. Криптографическая устойчивость информационных систем. Дифференциальный криптоанализ. |
| 4 | Понятие стеганографии. Модель передачи скрытых сообщений. Первые стеганографические системы. Защита авторского права. Цифровые водяные знаки. Цифровые отпечатки пальцев.  |
| 5 | Теория и практика кодирования. Ошибки при передаче сообщений. Проверочная и порождающая матрицы. |

**3. Форма контроля –** экзамен.