АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Наименование дисциплины	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Направление подготовки	162001 Эксплуатация воздушных судов и организация воздушного движения
Направленность программы (профиль)	Организация авиационной безопасности
Квалификация выпускника	Специалист
Форма обучения	Очная
Цели освоения дисциплины	Целями освоения дисциплины «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» являются формирование у студентов знаний по основам информационной безопасности, формирование умений и навыков применения полученных знаний в повседневной профессиональной деятельности.
Семестр (курс), в (на) котором изучается дисциплина	Очная форма – в 9 семестре
Наименование части (блока) ОПОП ВО, к которой относится дисциплина	Дисциплина относится к базовой части
Компетенции обучающегося, формируемые в результате освоения дисциплины	ПК-14; ПК-15; ПК-21; ПК-27; ПК-28; ПК-30; ПК-75; ПК-84
Трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 академических часа.
Содержание дисциплины. Основные разделы (темы)	Тема 1. Основные определения и составляющие информационной безопасности. Единые критерии безопасности информационных систем Тема 2. Нормативные акты, руководящие документы Российской Федерации в области информационной безопасности. Нормативные акты Российской Федерации в области информационной безопасности. Руководящие документы по техническому и экспортному контролю. Тема 3. Обзор и сравнительный анализ стандартов информационной безопасности. Обзор и сравнительный анализ стандартов информационной безопасности. Практические недостатки стандартов и рекомендаций по информационной безопасности. Тема 4. Информационное противоборство. Ее психологическая и техническая составляющие. Информационное противоборство. Ее психологическая и техническая составляющие. Тема 5. Угрозы информационной безопасности. Антивирусная защита. Угрозы информационной безопасности. Классификация угроз. Общие принципы функционирования компьютерных вирусов, их классификация и борьба с ними. Тема 6. Построение систем защиты от угроз информации в информационных системах.

	Принципы построения систем защиты от угроз нарушения конфиденциальности, целостности, доступности информации в информационных системах. Тема 7. Криптографические методы защиты информации. Симметричные и асимметричные криптографические методы защиты информации. Электронная цифровая подпись. Тема 8. Уязвимости компьютеров и компьютерных сетей. Угрозы и причины их реализации. Уязвимости архитектуры клиент-сервер. Уязвимости системных утилит. Сетевые вирусы. Тема 9. Основные виды атак на компьютерные системы. Удаленные атаки. Типичные атаки и уровни атак. Методы нападения и проникновения. Тема 10. Сетевые средства экранирования. Типы межсетевых экранов. Основные компоненты сетевых экранов. Схемы подключения. Тема 11. Системы анализа защищенности Аудит и мониторинг информационной безопасности. Классификация. Сетевые сканеры. Системные сканеры. Тема 12. Системы обнаружения и предотвращения вторжений. Тема 13. Обеспечение сохранности данных и защита ПЭВМ. Информационная безопасность систем управления базами данных. Тема 14. Политика безопасности. Принципы построения. Тема 15. СКЗИ Secret Net и Сфера. Особенности, правила использования.
Форма промежуточной аттестации по итогам освоения дисциплины	Экзамен