

### **Цели освоения дисциплины (модуля) / практики**

Целью освоения дисциплины является формирование общепрофессиональной компетенции, заключающееся в способности анализировать правила управления безопасностью вычислительных систем и компьютерных сетей, проводить комплексный подход к обеспечению безопасности, анализировать и структурировать угрозы безопасности, оформлять и представлять аналитические обзоры рисков безопасности, изучать методы и средства обеспечения безопасности вычислительных систем и компьютерных сетей с обоснованными выводами и рекомендациями.

### **Компетенции, формируемые в результате освоения дисциплины (модуля)/практики.**

#### **Индикаторы достижения компетенций**

ОПК-3 Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями;

ОПК-3.1 Анализирует профессиональную информацию, направленную на безопасность и защиту информации, и представляет её в виде аналитических обзоров

ОПК-3.2 Оформляет и представляет научно-техническую информацию в соответствии со сложившимся академическим этикетом

#### **В результате освоения дисциплины (модуля)/практики обучающийся должен**

##### **Знать:**

основные положения законодательства в области современного авторского права и защиты информации;  
основные методы и средства защиты конфиденциальной информации;  
состав и организацию систем информационной безопасности, методы криптографических преобразований;  
основные стандарты и протоколы шифрования и электронной подписи;  
методы и средства обеспечения информационной безопасности компьютерных систем;  
современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования;  
современные подходы к построению систем защиты информации.

##### **Уметь:**

определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий;  
использовать современные программные средства для защиты информации;  
принимать адекватные решения при выборе средств защиты информации на основе анализа угроз;  
разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности;  
обоснованно выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты.

##### **Владеть:**

навыками разработки защищенных приложений;  
навыками создания защищенной среды с помощью аппаратно-программных средств защиты;  
навыками самостоятельного проектирования систем защиты информации;  
методами оценки эффективности систем защиты информации в компьютерных системах.

Трудоёмкость дисциплины/практики: 4 ЗЕ.