Б1.Б.15 Основы управления информационной безопасностью

Объем дисциплины (модуля) **4 ЗЕТ (144 час)**

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Цель дисциплины: Изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии. Задачи дисциплины: Приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации в управлении информационной безопасностью. Формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ
УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
УК-2.1: Формулирует в рамках поставленной цели проекта совокупность задач, обеспечивающих ее достижение
УК-2.2: Определяет потребности в ресурсах для решения задач профессиональной деятельности
УК-2.3: Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-5.2: Применяет нормативные правовые акты и нормативные методические документы по информационной безопасности в профессиональной деятельности
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;
ОПК-10.1: Знает требования к формированию политики информационной безопасности и управлению информационной безопасностью на объекте защиты
ОПК-10.2: Классифицирует информационную систему по требованиям защиты информации
ОПК-10.3: Определяет угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети
ОПК-10.4: Формирует комплекс мер по противодействию угрозам информационной безопасности, организовывает и поддерживает его выполнение
ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;
ОПК-12.2: Анализирует, проверяет достоверность, полноту, актуальность и непротиворечивость данных и содержательно интерпретирует полученные результаты для технико-экономического обоснования проектных решений
ОПК-2.1: Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;
ОПК(п)-2.1.2: Выявляет источники информационных угроз, их возможные цели, пути реализации
ОПК(п)-2.1.1: Знает функциональные процессы и информационные составляющие объектов защиты
ОПК(п)-2.1.3: Оценивает предполагаемый ущерб от реализации информационных угроз
ОПК-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ОПК(п)-2.3.2: Знает и применяет международные и национальные стандарты в области информационной безопасности

В результате освоения дисциплины обучающийся должен

Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы организации информационных систем в соответствии с требованиями по защите информации; основные нормативные правовые акты в области информационной безопасности и защиты информации.
Уметь: анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации; формулировать и настраивать политику безопасности распространенных операционных систем, а также вычислительных сетей, построенных на их основе.
Владеть: навыками работы с нормативными правовыми актами; навыками работы с нормативными документами; методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; методами организации и управления деятельностью служб защиты информации на предприятии; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
Раздел 1. Введение в системы управления информационной безопасностью
Раздел 2. Управление информационными рисками как базовый процесс системы управления информационной безопасностью
Раздел 3. Управление информационной безопасностью в отдельных классах информационных систем