

Аннотация к рабочей программе дисциплины

Автор: Урбан В.А., доцент, канд.техн.наук

Наименование дисциплины: Б1.В.02 Аудит информационной безопасности

Цель освоения дисциплины: заключается в освоении дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе организации и проведения аудита информационной безопасности.

1. Требования к результатам освоения дисциплины:

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	Этап 1: риск утечки конфиденциальной информации	Этап 1: анализировать риски информационной безопасности, которые напрямую связаны с возможностью осуществления угроз безопасности для предприятия в отношении ресурсов информационной системы	Этап 1: навыками определения основных видов угроз безопасности, рассматриваемыми при проведении аудита информационной безопасности
ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	Этап 2: оценку информационной системы предприятия на предмет соответствия существующим стандартам и нормативно-правовым документам в области информационной безопасности	Этап 2: исследовать локальные вычислительные системы	Этап 2: постановкой задачи аудита информационной безопасности
ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	Этап 3: принципы организации информационных систем в соответствии с требованиями по защите информации	Этап 3: правильно формулировать требования к программам для решения системных задач	Этап 3: методами формализации информационных процессов объекта и связей между ними
ПК-4 Способен оценивать	Этап 4: требования	Этап 4: проводить анализ и	Этап 4: навыками

последствия от реализации угроз безопасности информации в автоматизированной системе	стандартов и другой нормативной документации в области информационной безопасности	давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня технических средств защиты информации	применения комплексного подхода к обеспечению информационной безопасности объекта защиты
ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Этап 1: методы проведения аттестации объектов информатизации по требованиям стандартов и другой нормативной документации	Этап 1: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 1: навыками организации и проведении контрольных проверок работоспособности и эффективности применяемых средств защиты информации
ПК-6 Способен проводить анализ рисков информационной безопасности автоматизированной системы	Этап 1: риск распространения дискредитирующей во внешней среде информации	Этап 1: работать с основными средствами защиты информации	Этап 1: навыками использования математических методов и моделей для решения задач

2. Содержание дисциплины:

Тема 1. Понятие аудита безопасности

Тема 2. Методы анализа данных при аудите информационной безопасности

Тема 3. Анализ и управление рисками информационной безопасности

Тема 4. Нормативная база аудита информационной безопасности исполнительных органов государственной власти органов местного самоуправления субъектов Российской Федерации

Тема 5. Методика проведения аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации

Тема 6. Лицензирование и сертификация деятельности в области защиты информации

Тема 7. Стандарты, применяемые для оценки информационной безопасности

Тема 8. Методики проведения аудит информационной безопасности

Тема 9. Применение программных средств для аудита информационной безопасности

3. Общая трудоемкость дисциплины: 3 ЗЕ