

Аннотация к рабочей программе дисциплины «Комплексная защита объектов информатизации»

Курс учебной дисциплины «Комплексная защита объектов информатизации» предназначен для обучения студентов направления 10.03.01 «Информационная безопасность», профиль «Комплексная защита объектов информатизации» и входит в состав базовых дисциплин учебного плана Б1.В.02.07.

Общая трудоемкость освоения дисциплины составляет 144 часов (4 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), лабораторные работы (36 час.), самостоятельная работа (36 час.), контроль качества обучения студентов по дисциплине (36 час.). Дисциплина реализуется на 4 курсе в 8 семестре. Форма контроля по дисциплине – экзамен, курсовая работа.

Дисциплина «Комплексная защита объектов информатизации» логически и содержательно связана с такими курсами, как «Основы информационной безопасности», «Основы проектной деятельности», «Информационная безопасность автоматизированных систем», «Моделирование объектов и систем защиты информации».

Содержание дисциплины охватывает следующий круг вопросов: принципы организации и этапы разработки КОЗИОИ, выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию, определение потенциальных каналов и методов несанкционированного доступа к информации, определение компонентов и условий функционирования КОЗИОИ, материально-техническое и нормативно-методическое обеспечение КСЗИ, принципы и методы планирования функционирования КОЗИОИ, характеристика подходов, методов и моделей к оценке эффективности систем.

Цель: формирование у обучаемых знаний в области теоретических и практических основ построения и реализации комплексной системы защиты

информации объекта информатизации (КОЗИОИ), методику и технологию ее организации, принципы и содержание управления системой, методы обеспечения ее надежности.

Задачи:

- формирование знаний, умений и навыков, позволяющих проводить самостоятельный анализ состояния комплексной информационной безопасности на предприятии;

- изучение основ построения и реализации комплексной системы защиты информации объекта информатизации (КОЗИОИ), методику и технологию ее организации, принципы и содержание управления системой, методы обеспечения ее надежности.

Для успешного изучения дисциплины «Комплексная защита объектов информатизации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

- способность к самосовершенствованию и саморазвитию в профессиональной сфере, к повышению общекультурного уровня (ОК-1);

- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-12);

- способность оценивать уязвимости информационных систем, разрабатывать требования и критерии оценки информационной безопасности, согласованных со стратегией развития информационных систем (ПК-10);

- способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе

защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объектов и локализации защищаемых элементов (ПСК-3.2);

- способность разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, проводить выбор необходимых технологий и технических средств, организовать внедрение и последующее сопровождение (ПСК-3.3).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-7) способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает	информационные ресурсы, подлежащие защите и возможные пути реализации угроз безопасности
	Умеет	определять информационные ресурсы, подлежащие защите
	Владеет	способностью анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
(ПК-3) способностью администрировать подсистемы информационной безопасности объекта защиты	Знает	вероятные угрозы и уровни развития технологий защиты информации
	Умеет	организовывать и поддерживать выполнение комплекса мер по информационной безопасности
	Владеет	навыками управления процессом защиты с учетом решаемых задач и организационной структуры объекта защиты
(ПК-8) способностью проводить анализ исходных данных для проектирования	Знает	основы информационной безопасности
	Умеет	принимать участие в эксплуатации подсистем управления информационной безопасностью

<p>подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</p>	<p>Владеет</p>	<p>навыками применения мер по защите информации</p>
--	----------------	---

Для формирования вышеуказанных компетенций в рамках дисциплины «Комплексная защита объектов информатизации» применяются следующие методы интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах. Используемые оценочные средства: собеседование (ОУ-1), конспект (ПР-7), лабораторные работы (ПР-6), курсовая работа (ПР-5).