**Аннотация к рабочей программе дисциплины**
**«Аудит и мониторинг безопасности»**

Рабочая программа дисциплины «Аудит и мониторинг безопасности» разработана для студентов, обучающихся по направлению 10.03.01 - «Информационная безопасность» по профилю подготовки «Комплексная защита объектов информатизации». Дисциплина «Аудит и мониторинг безопасности» относится к дисциплинам выбора вариативной части учебного плана.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы (144 часа). Учебным планом предусмотрены лекционные занятия (36 часов), практическая работа (18 часов), лабораторная работа студента (36 часов) и самостоятельная работа студента (54 часа) в том числе на подготовку к экзамену (27 часов).

Содержание курса охватывает следующий круг вопросов, связанных с организационными задачами и функциями службы защиты информации; технологическими задачами и функциями службы защиты информации.

Дисциплина «Аудит и мониторинг безопасности» логически и содержательно связана с такими курсами как «Основы управления информационной безопасностью», «Программно-аппаратные средства защиты информации», «Документоведение», «Информационная безопасность автоматизированных систем».

**Целью** дисциплины «Аудит и мониторинг безопасности» является изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ).

**Задачи** дисциплины:

- формирование требований к системе управления ИБ конкретного

объекта;

- проектирование системы управления ИБ конкретного объекта;
- эффективное управление ИБ конкретного объекта.

Для успешного изучения дисциплины у студентов должны быть сформированы предварительные компетенции:

- способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);
- способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5).

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

| **Код и формулировка компетенции** | **Этапы формирования компетенции** | |
|---|---|---|
| (ПК-6) способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации | Знает | методы сбора первичной информации |
| | Умеет | проводить экспертизу собранной информации |
| | Владеет | навыками формализации требований пользователей заказчика |
| (ПК-7) способностью разрабатывать программы и методики испытаний программных, программно-аппаратных и | Знает | методы и программно-аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации |
| | Умеет | настраивать каналы безопасного обмена |

| | | |
|---|---|---|
| технических средств и систем обеспечения информационной безопасности | | информацией в локальных и распределенных автоматизированных системах |
| | Владеет | программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах |
| (ПК-9) способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов | Знает | основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, федеральной службы по техническому и экспортному контролю в данной области |
| | Умеет | пользоваться нормативными и техническими документами по защите информации |
| | Владеет | навыками работы с нормативными правовыми актами, способностью оформлять рабочую техническую документацию |
| (ПК-12) способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности | Знает | организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации |
| | Умеет | разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации |
| | Владеет | методами формирования требований по защите информации |
| (ПК-19) способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по | Знает | первоочередные мероприятия по обеспечению безопасности информации АС организации |
| | Умеет | пользоваться нормативными документами по защите информации |
| | Владеет | методиками проверки защищенности объектов информации на соответствие требований нормативных документов |

| | | |
|---|---|---|
| техническому и экспортному контролю | | |
| (ПСК-3.1) способностью проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств с целью определения возможных источников информационных угроз, их вероятных целей и тактики | Знает | возможные источники информационных угроз |
| | Умеет | проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств |
| | Владеет | способностью анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты |

Для формирования вышеуказанных компетенций в рамках дисциплины «Аудит и мониторинг безопасности» применяются следующие методы активного/ интерактивного обучения: лекция – беседа, лекция – пресс-конференция.