**«Установка, настройка и эксплуатация программного комплекса Ankey SIEM NG»**

**Цель обучения:**приобретение теоретических знаний в области защиты информации в части применения программного комплекса Ankey SIEM NG, изучение функциональных возможностей компонентов комплекса; а также практических навыков: установка, настройка и эксплуатация ПК Ankey SIEM NG.

**Для кого этот курс?**

- администраторы безопасности;

- администраторы корпоративных сетей; IT-специалисты;

- аудиторы информационной безопасности; консультанты и инженеры, ответственные за построение процессов мониторинга и аудита информационной безопасности.

**Профессиональный стандарт**: 06.032 Специалист по безопасности компьютерных систем и сетей 14.09.2022

**Срок обучения:**32 академических часа (4 учебных дня)

**Формат**: очный/дистанционный, с отрывом от работы.

**Режим занятий**: 8 академических часов в день

**Структура курса**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №№  п.п. | Наименование разделов и тем | Всего часов | В том числе | | Форма контроля |
|  |  |  | Лекции | Практ. занятия |  |
| **1** | **Введение. Назначение Ankey SIEM NG.** | **8** | **8** |  | **Мини-тест** |
| 1.1. | Назначение Ankey SIEM NG.  Меры защиты ФСТЭК и действующие сертификаты.  Актуальные релизы Ankey SIEM NG и их ключевые различия.  Преимущества на рынке РФ. | 2 | 2 |  |  |
| 1.2. | Компоненты ПК Ankey SIEM NG и их функциональные возможности.  Основные компоненты:  компонент Ankey SIEM NG Agent (сервер сбора данных);  компонент Ankey SIEM NG Agent (сервер сбора и предварительной обработки «SIEM Light»);  компонент Ankey SIEM NG Core (сервер управления): приложение Management and configuration, приложение SIEM, приложение Knowledge Base.  компонент Ankey SIEM NG Server (сервер обработки);  компонент Ankey SIEM NG Event Storage (сервер хранения).  Дополнительные компоненты:  Ankey SIEM NG Vulnerability management (база данных уязвимостей);  Ankey SIEM NG Retro Correlator (сервер ретроспективной корреляции);  Ankey SIEM NG Event Broker (брокер данных);  Ankey SIEM NG Update and Configuration Service (модуль распределенного поиска событий).  Схема взаимодействия компонентов ПК Ankey SIEM NG. | 2 | 2 |  |  |
| 1.3. | Обзор конфигураций ПК Ankey SIEM NG.  Варианты архитектур ПК Ankey SIEM NG.  Аппаратные и программные требования. Технологический стек и рекомендации для выбора правильной конфигурации ПК Ankey SIEM NG. | 2 | 2 |  |  |
| 1.4. | Проектирование, расчеты, лицензирование и масштабирование ПК Ankey SIEM NG. | 2 | 2 |  |  |
| **2.** | **Установка, настройка и эксплуатация ПК Ankey SIEM NG** | **22** |  | **22** | **Мини-тест** |
| 2.1. | Подготовительные операции перед установкой.  Установка и настройка компонентов ПК Ankey SIEM NG.  Особенности администрирования. | 2 |  | 2 |  |
| 2.2. | Компоненты и функции веб-консоли ПК Ankey SIEM NG:  -    обзор приложения Management and configuration;  -    обзор приложения SIEM;  -    обзор приложения Knowledge Base.  Работа в веб-интерфейсе SIEM-системы. | 4 |  | 4 |  |
| 2.3. | Подготовка приложения Knowledge Base к установке библиотеки ресурсов.  Обзор содержимого приложения Knowledge Base:  -    базовые модули – стандартные коннекторы;  -    базовые модули - стандартный контент;  -    дополнительные модули – доп. коннекторы;  дополнительные модули – доп. контент. | 4 |  | 4 |  |
| 2.4. | Обзор функционала для мониторинга состояния ПК Ankey SIEM NG (платформа, сбор данных, корреляция):  -    управление системой;  -    контроль состояния лицензии и версий компонентов;  -    контроль состояния механизмов сбора событий;  контроль работы правил корреляции. | 4 |  | 4 |  |
| 2.5. | Резервное копирование и восстановление данных ПК Ankey SIEM NG:  -    резервное копирование конфигурации ПК Ankey SIEM NG;  -    настройка архивирования событий ИБ. | 4 |  | 4 |  |
| 2.6. | Обновление ПК Ankey SIEM NG:  -    обновление компонентов платформы;  -    обновление коннекторов;  -    обновление контента. | 4 |  | 4 |  |
|  | **Всего:** | **30** | **8** | **22** |  |
|  | **Итоговый контроль знаний** | **2** |  | **2** | **Итоговый тест** |
|  | **Итого:** | **32** | **8** | **24** |  |