

ПРАКТИКА ПРИМЕНЕНИЯ DLP-СИСТЕМ

[учебный онлайн-курс]

6 апреля, 11.00.

Контроль удаленной работы. Консоль аналитика. Отчеты и веб-отчеты. Для чего нужна каждая из групп. Правила эффективности. Коэффициенты. Как ProgramController учитывает время работы.

7 апреля, 11.00.

Два пути развития DLP-систем и их влияние на поисковые алгоритмы.

Движение информации в DLP-системе. Плюсы и минусы сетевого и агентского перехвата. Что такое индекс и для чего он нужен. Разница между индексом и базой данных. Интеграция сторонних систем с КИБ на примере ABBYY и распознавания голоса.

8 апреля, 11.00.

Блокировки: контекстные и контентные. Как работают, в чем отличия, где настраиваются. Как прослушать смартфоны сотрудников и не сесть в тюрьму. Юридические аспекты.

9 апреля, 11.00.

Что нужно знать и уметь аналитику в консолях администрирования DLP-системы: NetworkController, EndpointController, SearchServer, DataCenter. Контроль командировочных. Морфология. Очереди на агентах. Опрос конфигурации ПО. Настройка Файлового аудитора. Индексация облачных хранилищ. Настройка Индексации рабочих станций. Импортирование почтовых архивов. Бэкапы индексов. Постановка индексов на паузу. Настройка детекторов в SearchServer. Непрерывная индексация. Стоп-слова и стоп-символы. Ролевая модель доступа.

10 апреля, 11.00.

Консоль аналитика. Онлайн-инструменты. Основные и продвинутое инструменты вкладки «Поиск» для ручного поиска. Работа с поисковой выдачей. Работа с экспортом. ID и UIN. Алиасы и источники данных. Работа с фразовым поиском.

13 апреля, 11.00.

Консоль аналитика. Виды поиска. По словарю, по атрибутам, по регулярным, по базам данных, по цифровым отпечаткам. Поиск похожих.

14 апреля, 11.00.

Как работает AlertCenter. Некоторые нюансы поиска. Поиск синонимов. Как создать политику безопасности. Разбор политик безопасности.

15 апреля, 11.00.

Файловый аудитор. Настройка. Использование.

16 апреля, 11.00.

Профайлинг: что это, как работать. Практическая характерология. Работа с карточкой. Работа с динамикой. Методика по кадровым рискам, устанавливающая связь между профайлингом и DLP.

17 апреля, 11.00.

Социальная инженерия. Риторика как инструмент специалиста по безопасности.

20 апреля, 11.00.

Мотивы инсайдера. Как выявляются. Работа по раннему определению инсайдера. Конфликтология.

Старт: 6 апреля, 11.00 (Мск).

Преподаватель: начальник отдела информационной безопасности «СёрчИнформ» Алексей Дрозд.

[Регистрация.](#)