Программа обучения «Практика применения DLP-систем»

Цель: овладение слушателями навыками использования современных DLP-систем в профессиональной деятельности в сфере информационной безопасности.

Формы проведения обучения: лекции, анализ ситуаций (case-study), практические занятия, тренинги.

Категория слушателей: руководители и сотрудники служб информационной безопасности предприятий и организаций.

День 1

10.00 – 10.15 **Организационное собрание**

10.15 – 10.45 **Презентация слушателей** (тренинг знакомства)

10.45 – 11.45 **Информационная безопасность: введение в проблему**

Утечка информации как социальное явление. Виды утечек информации. Риски, связанные с утечками информации, и их оценка. Экономическая эффективность различных методик оценки рисков, связанных с утечками информации.

Практическое применение методики оценки рисков, связанных с утечками информации. Расчет экономического эффекта от внедрения DLP-систем.

11.45 – 12.00 **Перерыв**

12.00 – 14.00 **Основы работы DLP-систем**

Технические возможности получения информации об активности работников. Проблема перехвата трафика, различные подходы к технической реализации перехвата трафика. Достоинства и недостатки блокирующих и контролирующих систем. Инструментарий сотрудника службы информационной безопасности. Основные характеристики современных DLP-систем.

Психологические аспекты использования DLP-систем. Психология инсайдера, типы инсайдеров. Популярные техники социальной инженерии. Теория конфликтов.

Практическое определение психологических характеристик автора по содержанию переписки.

14.00 – 15.00 **Обед**

15.00 – 16.45 **Развертывание и администрирование DLP-системы**

Что необходимо знать перед развертыванием DLP-системы. Доменная структура Windows. Учетные записи и права. Этапы развертывания DLP-системы. Администрирование DLP-системы. Требование соблюдения конфиденциальности установки DLP-системы в организации. Необходимость контроля всех используемых каналов передачи информации.

Практическая работа по составлению типового перечня возможных каналов передачи информации в организации.

16.45 – 17.00 **Перерыв**

17.00 – 19.00 **Инструменты аналитики в DLP-системах**
Автоматизированный поиск; мониторинг; статистический, семантический и др. анализ; системы отчетности.
Практическая работа, направленная на сравнение достоинств и недостатков различных способов работы с перехваченными данными.

Круглый стол по теме «Группа риска: кого ловить и как идентифицировать?»

День 2

10.00 – 11.45 **Практическое использование DLP-системы** (практическое занятие)
Отработка и закрепление полученных знаний. Формирование базовых навыков работы с DLP-системой.

11.45 – 12.00 **Перерыв**

12.00 – 14.00 **Способы и примеры анализа информации, получаемой при помощи DLP-систем**
Выявление неформальных лидеров и нелояльных сотрудников. Прогнозирование инцидентов. Угрозы информационной безопасности: уволенные сотрудники пенсионного возраста, люди с нетрадиционной сексуальной ориентацией, лица, употребляющие наркотики, сектанты, переманивание сотрудников, мобильные устройства работников и др.
Практическая работа по составлению типовой карты угроз информационной безопасности в организации.

14.00 – 15.00 **Обед**

15.00 – 16.45 **Способы и примеры анализа информации, получаемой при помощи DLP-систем** (практическое занятие)
Создание и использование политик безопасности.
Формирование политик безопасности, ориентированных на контроль документов.
Формирование политик, ориентированных на анализ содержания документа.
Формирование политик, ориентированных на анализ тематики документа.

16.45 – 17.00 **Перерыв**

17.00 – 19.00 **Способы и примеры анализа информации, получаемой при помощи DLP-систем** (практическое занятие – продолжение)
Контроль передачи информации при помощи использования метода «поиск похожих документов». Виды поиска: поиск документа целиком, поиск на основе списка ключевых слов. Резюме, важные документы, даты, списки сотрудников, подставные фирмы и другие основания поиска. Анализ используемой работниками лексики: грубость, «мат» в

общении между собой, а также с клиентами; негативные характеристики руководства и деятельности организации и т.п.

Круглый стол по теме «Юридические аспекты: периоды Pre- и Post-DLP».

День 3

10.00 – 11.45 **Способы и примеры анализа информации, получаемой при помощи DLP-систем** (практическое занятие – продолжение)
Составление тематических словарей и работа с ними. Поиск технических, бухгалтерских, юридических и др. документов по словарям. Поиск лиц, имеющих долги и кредиты; азартных игроков; людей, страдающих алкогольной зависимостью и различными заболеваниями.

11.45 – 12.00 **Перерыв**

12.00 – 14.00 **Способы и примеры анализа информации, получаемой при помощи DLP-систем** (практическое занятие – продолжение)
Фразовый поиск. Поиск документов с грифом, налоговых деклараций, смет, логинов и паролей. Регулярные выражения и поиск по регулярным выражениям. Поиск номеров кредитных карт и персональных данных. Анализ нераспознанных документов.

14.00 – 15.00 **Обед**

15.00 – 16.45 **Способы и примеры анализа информации, получаемой при помощи DLP-систем** (практическое занятие – продолжение)
Поиск по атрибутам (интернет-казино, сайты знакомств, онлайн просмотр фильмов, онлайн-игры). Совместное использование различных видов поиска. Формирование сложных запросов. Комплексный подход к мониторингу информации. Отработка и закрепление полученных навыков работы с DLP-системой по сценариям: несанкционированное использование внешних носителей информации; перехват FTP-трафика; перехват HTTP-трафика; перехват сообщений интернет-пейджеров; перехват электронной почты; контроль содержимого рабочих станций пользователей; перехват голосовых и текстовых сообщений Skype; перехват документов, отправленных на печать.

16.45 – 17.00 **Перерыв**

17.00 – 19.00 **Способы и примеры анализа информации, получаемой при помощи DLP-систем** (практическое занятие – завершение)
Отработка и закрепление полученных навыков работы с DLP-системой по сценариям: поиск работников, проявляющих наибольшую активность в социальных сетях и интернет-пейджерах; нерациональное использование принтера; несанкционированное использование личного ящика электронной почты; поиск сотрудником другого места работы; общение с конкурентами; общение с уволенным работником; несанкционированная загрузка файлов в интернет; подозрительная активность. Выдача сертификатов.