САИБ

Практика применения систем контроля сотрудников и защиты от утечек информации

+7 (383) 255 32 55 info@saib.biz saib.biz

САИБ

Практика применения систем контроля сотрудников и защиты от утечек информации

saib.biz
info@saib.biz
+7 (383) 255 32 55

Аннотация

На сегодняшний день в комплексных системах защиты информации применяются различные классы средств защиты, направленных на уменьшение рисков, связанных с техническими угрозами.

Вместе с тем актуальными остаются угрозы, возникающие из-за человеческого фактора. Среди них особо следует отметить угрозу утечки конфиденциальной информации по вине внутреннего нарушителя (инсайдера).

Целью инсайдера может быть продажа информации конкурентам, публикация в открытом доступе и т.д.

В курсе рассматриваются основные вопросы, связанные с применением систем класса DLP (англ. Data Leak Prevention – предотвращение утечек данных), осуществляющих контроль сотрудников и защиту от утечек:

- **По каким каналам может произойти утечка информации?**
- **Как определить критичные классы информации, обрабатываемой в организации?**
- **Какие возможности предоставляют системы класса DLP?**
- **Какие инциденты можно выявить при помощи систем класса DLP?**
- **Как организовать сбор доказательной базы для расследования инцидентов?**

saib.biz
info@saib.biz
+7 (383) 255 32 55

Содержание курса

Характеристики основных каналов утечки информации

В этом разделе вы познакомитесь с основными характеристиками мест обработки корпоративной информации и особенностями основных каналов утечки и работы с ними.

Методы сбора необходимой информации об организации

В этом разделе вы узнаете, как определить степень критичности обрабатываемой информации и какую информацию необходимо собрать для планирования защиты критичной информации.

Основные функции и возможности систем класса DLP

В этом разделе вы познакомитесь с системами класса DLP и с их основными возможностями: методами перехвата информации и их базовой настройкой, а также узнаете о том, как спланировать внедрение DLP-системы и оценить эффективность её применения.

Разбор интересных кейсов выявления потенциальных каналов утечки информации

В этом разделе рассматриваются сценарии использования DLP-систем, которые могут быть интересны для дальнейшего анализа.

Примеры создания доказательной базы по выявленным инцидентам нарушения конфиденциальности информации

В этом разделе вы узнаете, по каким признакам можно выявить инцидент, как составлять автоматические правила генерации инцидентов, какими методами производится сбор доказательной базы, а также познакомитесь с нюансами внедрения системы хранения инцидентов, составления отчётов и сценариями ликвидации инцидентов.


САИБ