

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет инфокоммуникаций

Кафедра защиты информации

**СИСТЕМА ПРОТИВОДЕЙСТВИЯ УТЕЧКЕ ДАННЫХ
«КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
SEARCHINFORM»**

*Рекомендовано УМО по образованию в области
информатики и радиоэлектроники в качестве пособия
для специальности 1-98 80 01 «Информационная безопасность»*

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	4
1. ОБЩИЕ СВЕДЕНИЯ О DLP-СИСТЕМАХ.....	6
1.1. Назначение DLP-систем и принципы их функционирования.....	6
1.2. Технические возможности получения информации об активности работников.....	8
1.3. Виды перехвата информации.....	10
1.4. Состав и взаимосвязь компонентов DLP-систем на примере программного комплекса «Контур информационной безопасности SearchInform».....	11
2. СЕРВЕРНЫЕ КОМПОНЕНТЫ ПРОГРАММНОГО КОМПЛЕКСА «КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SEARCHINFORM».....	16
2.1. Платформа SearchInform NetworkSniffer: особенности реализации сетевого перехвата трафика.....	16
2.2. Платформа SearchInform NetworkSniffer: особенности реализации перехвата почтовых сообщений путем интеграции с почтовыми серверами и/или SMTP-интеграции.....	40
2.3. Платформа SearchInform NetworkSniffer: особенности реализации контроля журналов событий Active Directory.....	53
2.4. Платформа SearchInform EndpointSniffer: особенности реализации агентского перехвата трафика.....	56
2.5. Управление индексами и базами данных компонентов программного комплекса «Контур информационной безопасности SearchInform» при помощи средств SearchInform DataCenter.....	135
3. ПОИСК, ПРОСМОТР И АНАЛИЗ ПЕРЕХВАЧЕННЫХ ДАННЫХ.....	158
3.1. Поиск по перехваченным документам при помощи приложения SearchInform Client.....	158
3.2. Автоматический мониторинг информационных потоков при помощи приложения SearchInform AlertCenter.....	193
3.3. Формирование отчетов об активности пользователей и инцидентах при помощи приложения SearchInform ReportCenter.....	233
3.4. Ведение полноформатного расследования в рамках консоли IncidentCenter.....	272
ЗАКЛЮЧЕНИЕ.....	280
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	282