ОГЛАВЛЕНИЕ

Предисловие 3
Введение 7
1. Что такое DLP? 11
1.1. Общие сведения 11
1.2. Трансформация задач 12
1.3. DLP в концепциях People-Centric Security и Data-Centric Security 18
1.4. Восток-Запад: два пути развития DLP 19
1.5. От DLP к MLP 22
1.6. ИБ-аутсорсинг 23
1.7. Место DLP среди других решений на рынке 24
Конкуренция
1.8. Ближайшее будущее DLP 26
2. КИБ СёрчИнформ 29
2.1. Портфель продуктов компании СёрчИнформ 29
2.2. Движение информации в DLP 30
2.3. «Ромашка» КИБ. Описание модулей 35
2.4. Профайлинг 59
2.5. Преимущества КИБ 61
3. Виды поиска 65
3.1. Фразовый поиск 67
3.2. Поиск по словарю 76
3.3. Пару слов о синонимах 78
3.4. Поиск похожих 81
3.5. Поиск по атрибутам 83
3.6. Поиск нераспознанных 85
3.7. Поиск по регулярным выражениям 88

3.8. Поиск по цифровым отпечаткам ... 91
3.9. Сложный запрос ... 95
3.10. Поиск по базам данных ... 98
3.11. Статистические запросы ... 99
3.12. Поиск по формам ... 100
4. AnalyticConsole: ручной и автоматический анализ информации ... 102
4.1. Вкладка «Поиск» ... 102
4.2. Вкладка «Текущая активность» ... 118
4.3. Вкладка «Отчеты» ... 118
4.4. Вкладка «Карточки пользователей» ... 143
4.5. Вкладка «Файловый аудитор» ... 150
4.6. Вкладка «Профайл центр» ... 150
4.7. Вкладка «Карантин» ... 150
4.8. Вкладка «Task Management» ... 159
5. AlertCenter: автоматический мониторинг информационных потоков ... 163
5.1. Внешний вид ... 163
5.2. Создание политики ... 163
5.3. Метки ... 168
5.4. Шаблоны ... 170
6. Блокировка информации в КИБ СёрчИнформ ... 177
6.1. Общий принцип блокировки в DLP-системах ... 177
6.2. Блокировка: настройка правил ... 179
6.3. Блокировка на уровне сети ... 191
6.4. Блокировка на уровне агента ... 192
6.5. Блокировка почты на уровне рабочей станции или почтового сервера (агент) ... 208
7. FileAuditor СёрчИнформ: аудит операций в файловой системе и прав доступа к файлам ... 211
7.1. Что не так с контролем «данных в покое» при помощи DLP-системы? ... 211
7.2. О технологии DCAP ... 211
7.3. Рынок DCAP-систем ... 213
7.4. «FileAuditor СёрчИнформ»: назначение и решаемые задачи ... 214

7.5. Настройка правил поиска конфиденциальных документов в модуле FileAuditor в консоли EndpointController ... 215
7.6. Просмотр файлов, контролируемых модулем FileAuditor, в AnalyticConsole ... 229
7.7. Отличия FileAuditor от ИРС ... 235
8. Профайл центр: оценка рисков, связанных с человеческим фактором ... 236
8.1. AnalyticConsole: вкладка «Профайл центр» ... 237
8.2. Принцип работы ... 239
8.3. Несколько слов о психотипах ... 241
8.4. Блок «Базовые ценности» ... 245
8.5. Блок «Потенциальные криминальные тенденции» ... 245
8.6. Блок «Уровень амбиций» ... 248
8.7. Блок «Потенциальные риски и рекомендации» ... 248
8.8. Блок «Сильные и слабые стороны» ... 248
8.9. Блок «Индекс личностных качеств» ... 249
8.10. Динамика профиля ... 250
8.11. Расширенный отчёт ... 254
8.12. Поиск по характеристикам пользователя ... 255
8.13. Рейтинги пользователей ... 256
8.14. Связь ProfileCenter и КИБ ... 259
ЛАБОРАТОРНЫЙ ПРАКТИКУМ ... 260
Лабораторная работа № 1. Основные компоненты программного комплекса «СёрчИнформ КИБ» и разграничение прав доступа ... 260
1.1. Порядок выполнения работы ... 260
1.2. Задания к лабораторной работе ... 260
1.3. Содержание отчета ... 261
1.4. Теоретические сведения ... 261
1.5. Ход выполнения работы ... 271
1.6. Вопросы для самоконтроля ... 297
Лабораторная работа № 2. Основные принципы и приемы использования DLP-системы для мониторинга утечек конфиденциальной информации (на примере программного комплекса «СёрчИнформ КИБ») ... 297
2.1. Порядок выполнения работы ... 297

2.2. Задания к лабораторной работе 297
2.3. Содержание отчета 298
2.4. Теоретические сведения 298
2.5. Ход выполнения работы 299
2.6. Вопросы для самоконтроля 312
Лабораторная работа № 3. Осуществление контроля переписки и действий пользователей при помощи различных видов поиска (на примере программного комплекса «СёрчИнформ КИБ») 313
3.1. Порядок выполнения работы 313
3.2. Задания к лабораторной работе 313
3.3. Содержание отчета 315
3.4. Теоретические сведения 315
3.5. Ход выполнения работы 315
3.6. Вопросы для самоконтроля 337
Лабораторная работа № 4. Проведение расследований с использованием возможностей программного комплекса «СёрчИнформ КИБ» 339
4.1. Порядок выполнения работы 339
4.2. Задания к лабораторной работе 339
4.3. Содержание отчета 340
4.4. Теоретические сведения 340
4.5. Ход выполнения работы 341
4.6. Вопросы для самоконтроля 359
Заключение 360
Литература 363