ИНСТРУМЕНТЫ БЕЗОПАСНОСТИ

Нестандартные методы применения DLP-системы

СЕГОДНЯ DLP-СИСТЕМА – must have-инструмент в руках профессионалов ИБ-отрасли. Функциональность современных программных продуктов позволяет решать все больше задач, порой весьма нестандартных. Эксперт «Сёрчинформ» – компания входит в тройку ведущих разработчиков DLP-решений на рынке России и стран СНГ – рассказал о нетривиальных методах применения DLP-системы.

Некоторые нестандартные варианты применения DLP могут показаться рискованными, буквально «на грани фола», но результат способен компенсировать эти риски с лихвой. Конечно, отдельные методы используются с предварительного согласования с руководством.

Итак, для каких особенных задач может послужить уже привычный инструмент:

1. Выявление нелояльных сотрудников. Негативно настроенный работник – это «бомба замедленного действия». Он способен навредить компании самым неожиданным образом: оставить команду в ответственный момент, перейти к конкуренту, системно настраивать персонал против руководства. Чтобы выявить таких сотрудников, можно действовать по простому плану:

- Вбросить «дезу» (оформите приказ, который потенциально вызовет возмущение сотрудников).
- Настроить политики безопасности на слова-маркеры.

SHUTTERSTOCK.COM/ANTONBRAND

АЛЕКСЕЙ ПАРФЕНТЬЕВ,
ведущий аналитик «Сёрчинформ»

● Проанализировать трафик в день «вброса» (наши клиенты анализируют как переписку, так и переговоры сотрудников – с помощью инструмента MicrophoneSniffer).
● Взять «на контроль» негативно настроенных сотрудников.

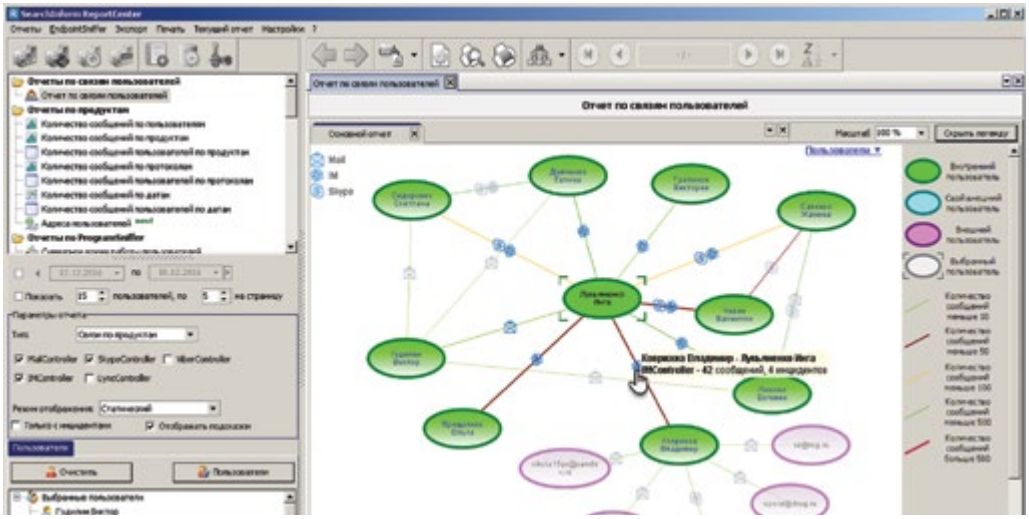
Провокационный приказ должен быть реалистичным, но вызывающим негодование в коллективе. Документ даст повод высказать возмущение, обменяться мнениями с коллегами, вызовет всплеск активности в переписке. Службе безопасности остается просто отследить, кто проявляет особое рвение. Для мониторинга негатива используются слова-маркеры, взятые из того самого фейк-приказа.

2. Выявление неформальных лидеров. Вброс дезинформации также может показать неформальных лидеров коллектива. Ведь зачастую от настроя этих людей зависит настрой существенной части персонала.

В повседневной работе выявить лидеров в команде можно с помощью специального отчета, показывающего кто, с кем и насколько активно общается. Нужно учесть, что анализ связей может вывести на первые места офис-менеджеров и секретарей, если они используются в качестве «перевалочных информационных пунктов». Этих специалистов можно исключить из анализа.

3. Обнаружение руководителей-самодуров. Большинство сотрудников не рассказывают высшему руководству о начальнике-самодуре из страха быть уволенными или от нежелания прослыть «доносчиками». Но анонимно изливать проблемы в сети не так рискованно, поэтому мы так часто видим негативные отзывы о компаниях. Даже если это в целом вредит имиджу работодателя.

РИСУНОК 1. ВИЗУАЛИЗАЦИЯ СВЯЗЕЙ ПОЛЬЗОВАТЕЛЕЙ В DLP-СИСТЕМЕ



В силах службы безопасности используя слова-маркеры отслеживать негатив и работать с источником – недовольным сотрудником.

4. Инвентаризация ПО и оборудования. DLP-система облегчает задачу по отслеживанию съемного «железа» и устанавливаемых программ. Подменить оперативную память ноутбука на меньшую, установить нелицензионное ПО, грозящее штрафом организации, – сотрудники компаний нередко грешат этим. Например, «КИБ Сёрчинформ» позволит отследить нарушения:
● Агент DLP-системы фиксирует установку, удаление и наличие ПО на компьютерах, а также установку и снятие используемого оборудования.
● Система выдает отчеты, в которых наглядно отображаются все действия работников в отношении ПО и оборудования.

5. Контроль «гостей». Возможность убедиться в хороших (или плохих) намерениях гостей, пришедших в офис, – ценное подспорье для любого руководителя.

Посетители нередко используют Wi-Fi-сеть в чужой компании. А это источник дополнительной информации для специалиста по безопасности при условии, что он использует современную DLP-систему. Контроль ведется безотносительно личных каналов общения (например, личный Skype или Viber), но действия с корпоративными ресурсами фиксируются и анализируются.

К примеру, в практике нашего клиента есть история, когда служба безопасности обнаружила попытки аудиторов скачать архив контрагентов из корпоративной системы документооборота.

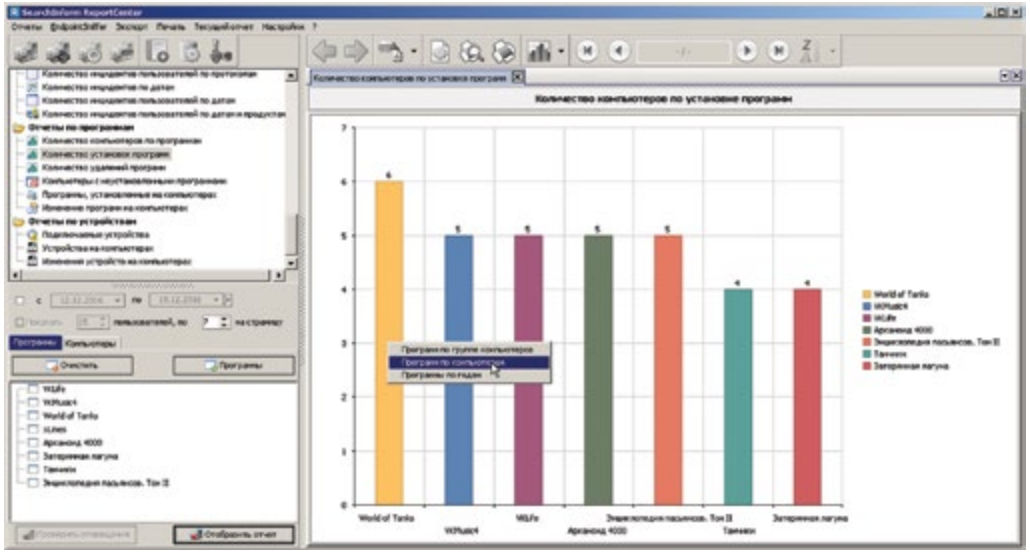
Другой пример – сотрудник аутсорсинговой компании был замечен за попытками установить программы слежения на ПК фирмы. В обоих случаях ИБ-служба оперативно предоставила данные об инцидентах руководству.

6. Мониторинг продуктивности сотрудников. Привычная проблема руководства компании любого масштаба – опоздания, прогулы, имитация работы персоналом. Если в организации работают 50 человек и половина из них 40 % времени тратит на развлечения и личные дела, то за год компания потеряет 98 рабочих дней в расчете на каждого.

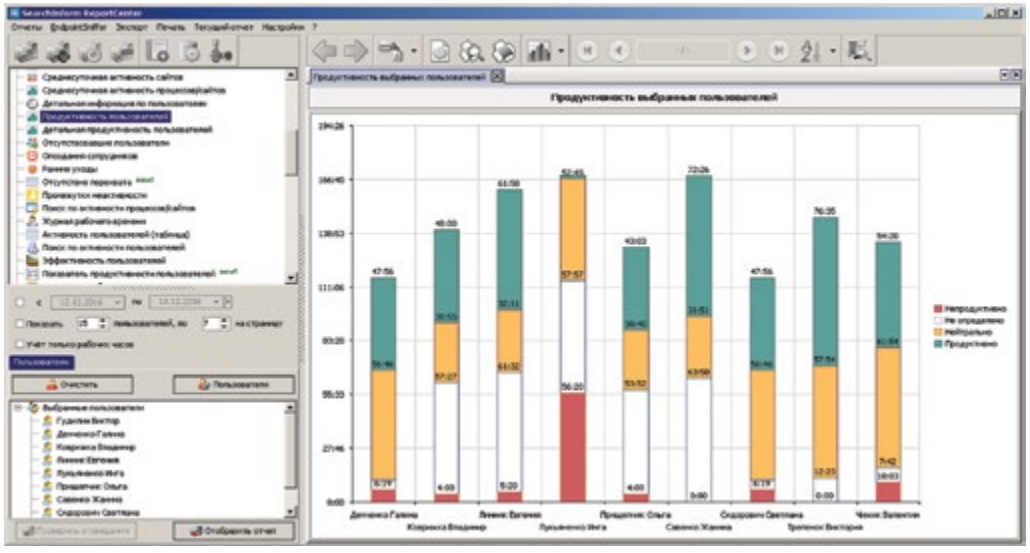
Обнаружить проблемы с трудовой дисциплиной – уже полдела. Но DLP-система соберет данные об эффективности сотрудников, сформирует отчет, на основе которого руководитель сможет исправить ситуацию – оптимизирует численность, установит санкции за нарушения и прочее.

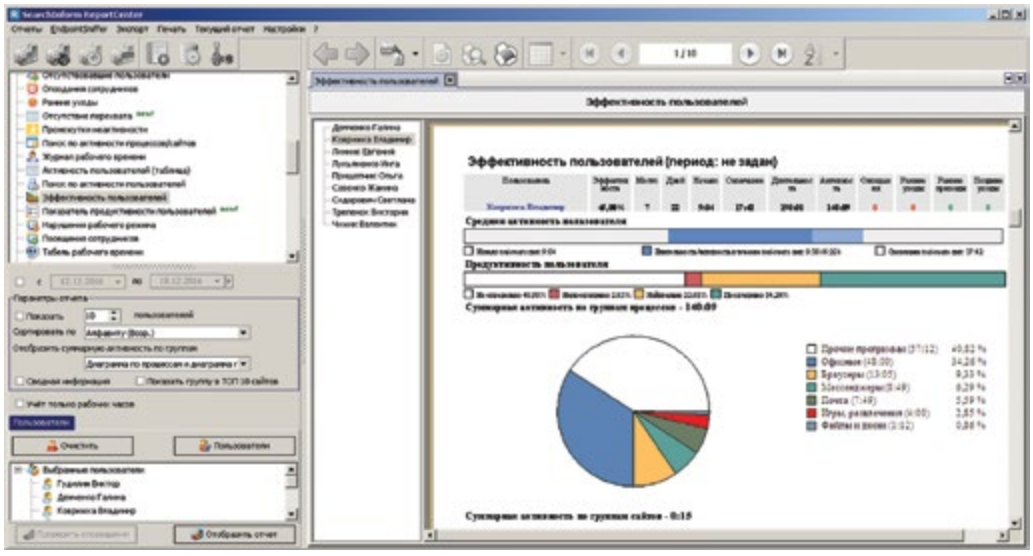
7. Мониторинг качества обслуживания клиентов. Может применяться

РИСУНОК 2. ОТЧЕТ ПО ДЕЙСТВИЯМ В ОТНОШЕНИИ ПО



РИСУНКИ 3–4. ОТЧЕТЫ ПО ПРОДУКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ





как к цифровым каналам (скайп, соцсети), так и к аудиопотоку (телефония в call-центрах, микрофонная запись в офисах продаж). Принцип действия таков: в DLP вносятся политики, срабатывающие на негативную лингвистику, и аудитор видит отчет обо всех неоднозначных фактах общения с клиентами. Применять ИБ-политики к аудиофайлам позволяет интеграция с решением центра речевых технологий – оно преобразует аудиофайлы в текст, а дальше действует аналитика DLP-системы.

Выводы

За 11 лет работы в ИБ-сфере мы разработали политики безопасности для организаций из всех секторов экономики, обработали множество кейсов и решили вместе с клиентами немало нетривиальных задач. Главный вывод, который можно сделать из всей этой работы, – сфера ИБ никогда не стоит на месте.

Поэтому мы поставили перед собой задачу не только разрабатывать продукт для ИБ-профессионалов, но и способствовать обмену опытом между нашими заказчиками. Мы агрегируем кейсы, практические приемы и экспертные мнения в блоге на сайте searchinform.ru (там же можно подписаться на дайджест-рассылку полезных материалов), дважды в год проводим серию конференций Road Show SearchInform в городах России и СНГ, а также рассказываем о новостях в специализированном телеграм-канале для ИБ-специалистов telegram.me/searchinform. ●