Ростелеком
Солар

Исследование «Топ 5 разочарований пользователей DLP-систем».

Декабрь 2019

МОСКВА, 2019

Содержание

1. Ключевые цифры

- Самым критичным недостатком современных DLP-систем **65%** компаний назвали **отсутствие** или некорректную работу **заявленной функциональности.** В то же время чуть менее половины респондентов отметили перегруженность современных DLP-систем избыточным функционалом.
- В **53%** случаев ИБ-службам компаний не хватило функционала внедренной DLP-системы для решения своих задач.
- **29%** опрошенных заказчиков сетуют на отсутствие на рынке общей концепции работы с системами защиты от утечек.
- При этом большинство респондентов (**82%**) подчеркнули, что **не отказались бы от использования DLP-систем**, если бы заранее знали о выявившихся после внедрения недостатках.

2. Методология

- Данное исследование проведено методом устного опроса, а также письменного анкетирования руководителей и специалистов служб информационной безопасности российских компаний.
- В опросе приняли участие представители предприятий, относящихся к сегменту среднего бизнеса (SMB), а также к крупным предприятиям уровня Enterprise.
- В отраслевой ландшафт опрошенных компаний вошли следующие сегменты: ВПК, производство, судостроение, телеком, ТЭК, транспорт, финансы.
- Для целей исследования были проинтервьюированы пользователи ключевых DLP-систем, представленных на российском рынке.
- В процессе опроса респондентам предлагалось выбрать от одного до пяти вариантов ответов из десятка перечисленных в анкете недостатков DLP-систем или же предложить не более трех собственных вариантов.

3. Введение

Компания «Ростелеком-Солар», национальный провайдер технологий и сервисов кибербезопасности, представляет исследование «Топ 5 разочарований пользователей DLP-систем». Это первое на российском рынке исследование по тематике защиты от утечек информации (DLP), в котором рассмотрены реальные недостатки систем, выявленные самими заказчиками в процессе боевой эксплуатации.

Глобальный рынок систем защиты данных от утечек, с момента своего зарождения и до настоящего времени демонстрирует стабильный и уверенный рост, несмотря на периодические экономические кризисы и связанные с этим бюджетные ограничения компаний-заказчиков. Так, по данным международного исследовательского агентства The Radicati Group, глобальная выручка от продажи корпоративных DLP-систем в 2018 году составила 1,1 млрд USD. А к 2022 году аналитики прогнозируют ее удвоение (более 2,2 млрд USD).

Актуальная статистика по объему российского рынка систем защиты от утечек, к сожалению, на данный момент в публичном поле отсутствует. Однако, согласно исследованию «Анализ рынка информационной безопасности в России. Часть 2», опубликованному в начале 2019 года Аналитическим центром Anti-Malware.ru, DLP-системы использует порядка 29% российских компаний. При этом авторы отмечают, что, несмотря на анонимный характер проведенного для подготовки исследования опроса, респонденты крайне неохотно делились информацией об используемых в их компаниях средствах защиты. Во многих случаях отмечалось, что такая информация носит закрытый характер, или указывались «произвольные значения» (прочерки, общие слова, произвольный текст и т. п.). Таким образом, вполне вероятно, что в действительности процент российских компаний, использующих системы защиты от утечек, может быть несколько больше.

В связи с очевидными перспективами роста данного сегмента ИБ-рынка аналитики «Ростелеком-Солар» решили выяснить у российских компаний, уже внедривших и эксплуатирующих DLP-системы, с какими трудностями они столкнулись на начальной стадии использования систем, чего заказчикам не хватило в применяемых решениях как с точки зрения функциональности, так и в плане их интеграции в ИТ-инфраструктуру предприятия.

Результаты данного исследования будут полезны для изучения как компаниям, которые только задумываются о внедрении средств защиты от утечек, так и их разработчикам и интеграторам для дальнейшего совершенствования и корректировки как функциональности самих систем, так и методологии и инструментария их внедрения.

Для целей данного исследования были отобраны компании разного размера, исходя из численности их компьютерного парка, и различной отраслевой направленности (7 отраслевых направлений).

4. Результаты исследования

По результатам опроса пятерка наиболее критичных для заказчиков недостатков, выявленных после запуска DLP-системы в боевую эксплуатацию, выглядит следующим образом:

№ п/п	Критичный недостаток	% компаний
1.	Не работает/отсутствует заявленный функционал DLP-системы	65%
2.	Не хватает функционала для решения моих задач	53%
3.	Серьезные сложности внедрения в инфраструктуру компании	35%
4.	Неразрешимое противоречие между ложноположительными и ложноотрицательными срабатываниями	34%
5.	Нет общей концепции работы с DLP	29%

Рассмотрим подробнее каждый из выявленных недостатков.

4.1 Не работает/отсутствует **заявленный** функционал DLP-системы

Этот недостаток возглавляет рейтинг, поскольку две трети опрошенных ИБ-специалистов посчитали его наиболее критичной слабостью современных систем защиты от утечек. Проанализировав тенденции рынка, аналитики «Ростелеком-Солар» пришли к выводу, что существует несколько причин, порождающих данный недостаток.

Во-первых, очень часто вендоры DLP-систем спешат добавить в свои решения новые фичи под давлением маркетинговых сравнений функциональности решений «по галочкам». При этом сами вендоры могут считать, что эти фичи на самом деле не так уж и нужны, поэтому прорабатывают их слабо, лишь формально. Также далеко не все производители привлекают к разработке своих систем специалистов по проектированию пользовательских интерфейсов. В результате иногда заложенная в системе полезная функциональность неудобна, и ею попросту не пользуются.

Во-вторых, на практике частой причиной жалоб заказчиков на некорректную работу тех или иных функций системы является неправильная ее настройка на этапе внедрения. В большинстве случаев проблема решается быстро и просто при подключении вендора: его технические специалисты выезжают к заказчику, устраняют проблемы настроек, и заявленная функциональность начинает работать.

И, наконец, в-третьих, нередки случаи, когда ИБ-специалисты заказчика недостаточно хорошо знают функциональность эксплуатируемой DLP-системы, не изучают руководство пользователя. Не в последнюю очередь это происходит из-за слабого уровня сопроводительной документации к системе. Поэтому заказчикам при выборе средств защиты от утечек имеет смысл обращать внимание в том числе и на качество предоставляемой вендором документации.

4.2 Не хватает функционала для решения моих задач

Результаты исследования выявили, что немногим более половины опрошенных компаний испытывали потребности в различной дополнительной функциональности DLP-систем для решения специализированных задач информационной безопасности. Однако, по итогам полученных ответов на вопрос, каких именно функций защиты от утечек не хватает компаниям, выяснилось, что респонденты не могут выделить наиболее важную функциональность, востребованную большинством. Ответы участников опроса распределились равномерно между множеством разных функций.

В то же самое время чуть менее половины респондентов отметили перегруженность современных DLP-систем с функциональной точки зрения. По мнению авторов исследования, некоторое противоречие, заложенное в двух вышеприведенных тезисах, можно объяснить тем, что на самом деле каждая компания хотела бы, чтобы DLP-системы решали ее индивидуальные, весьма узкие задачи, не востребованные другими участниками рынка. То есть по сути речь идет о запросах в области индивидуальной, а не продуктовой разработки.

4.3 Серьезные сложности внедрения в инфраструктуру компании

Чуть более трети респондентов столкнулись с серьезными сложностями внедрения DLP-системы в существующую инфраструктуру предприятия. Это может происходить по нескольким причинам.

Во-первых, по причине недооценки заказчиком ресурсов, необходимых для реализации внедрения, – как инфраструктурных, так и кадровых. DLP-система не антивирус; ее интеграция требует, с одной стороны, определенной зрелости инфраструктуры компании, а с другой, – наличия готовых работать над проектом ИТ-специалистов на стороне заказчика.

Зачастую техническим специалистам заказчиков, взаимодействующим с представителями вендора на этапе внедрения, не хватает знаний о технических возможностях системы защиты от утечек, о преимуществах, которые получит компания при эксплуатации системы. Недостаточная квалификация по этому направлению порождает низкую мотивацию ко внедрению DLP.

В этой связи для успешной реализации любого проекта внедрения необходимо на самом раннем этапе налаживать связь специалистов вендора и заказчика: обеим сторонам начинать погружение во все детали предстоящих работ, изучать всю имеющуюся документацию. Это позволит при самом внедрении заниматься сугубо практической работой, а не теоретической подготовкой.

Также на ранней стадии, возможно, уже в процессе реализации пилотного проекта, техническим специалистам заказчика необходимо максимально погрузиться в процесс, сделать наброски архитектуры для будущего реального внедрения и т.п. Все это в дальнейшем поможет быстро внедрить систему с полным понимаем и без лишних трудозатрат.

Во-вторых, процесс внедрения системы защиты от утечек в значительной степени зависит от компетенций исполнителя. При вдумчивом проектировании можно избежать практически любых проблем на этапе внедрения, что доказано на кейсах из реальной практики. В частности, один из недавних примеров – реализация внедрения многомодульной DLP-системы «под ключ» в 17-ти региональных филиалах территориально распределенной компании за 3 недели.

В-третьих, конечно, вендор должен заниматься управлением ожиданиями заказчика. Необходимо объяснить компаниям, приступающим к внедрению DLP-системы, что инфраструктурные особенности, а, порой, и узкие места, не являются приговором для реализации проекта. Напротив, это позволяет демонстрировать гибкость DLP-решения при внедрении и возможность дополнительного конфигурирования при его эксплуатации, включая возможность взаимодействия с информационными системами, которые будут интегрированы в инфраструктуру в будущем. Безусловно, такая «кастомизация» потребует планомерной пошаговой работы и чуть больше времени.

Необходимо понимать, что конкретные особенности инфраструктуры заказчика могут потребовать предоставления более детализированной информации об этих особенностях. СПО, клиент-серверные информационные системы, технические ограничения площадки, нестандартные источники данных, особенности рабочих станций – информирование о любых подобных деталях инфраструктуры позволит спланировать работу участников проекта, определить реальные сроки реализации и соответствовать ожиданиям заказчика.

4.4 Неразрешимое противоречие между ложноположительными и ложноотрицательными срабатываниями

Также немногим более трети компаний (34%) отметили, что их не устраивает неразрешимое противоречие между ложноположительными и ложноотрицательными срабатываниями, присущее любой DLP-системе.

К сожалению, данная проблема не имеет точного математического решения, поскольку математические критерии полноты анализа (считать нарушением то, что таковым не является) и точности анализа (не детектировать событие, в действительности являющееся утечкой) в определенной степени противоречат друг другу. Когда задача решается, согласно одному из критериев, другой автоматически размывается.

По мнению авторов исследования, наиболее очевидным решением проблемы является поиск баланса со смещением в сторону одного из двух критериев в зависимости от задач, решаемых компанией-пользователем DLP-системы. Для одних пользователей приоритетным является точное детектирование инцидента с возможностью не отвлекаться на ложные срабатывания. Для других важна максимальная полнота мониторинга событий информационной безопасности.

Как показывает практика, часто заказчики, добиваясь снижения ложных срабатываний, проверяют на достоверность только ложноположительные срабатывания. Авторы исследования рекомендуют при высоком проценте точности внимательно анализировать и ложноотрицательные. В противном случае можно, сэкономив на нервах и трудозатратах, пропустить реальную утечку.

В целом, существуют различные подходы к политикам фильтрации информационного трафика на предмет рисков информационной безопасности. Например, вот такой: https://habr.com/ru/company/solarsecurity/blog/347992/ и https://habr.com/ru/company/solarsecurity/blog/348010/

4.5 Нет общей концепции работы с DLP

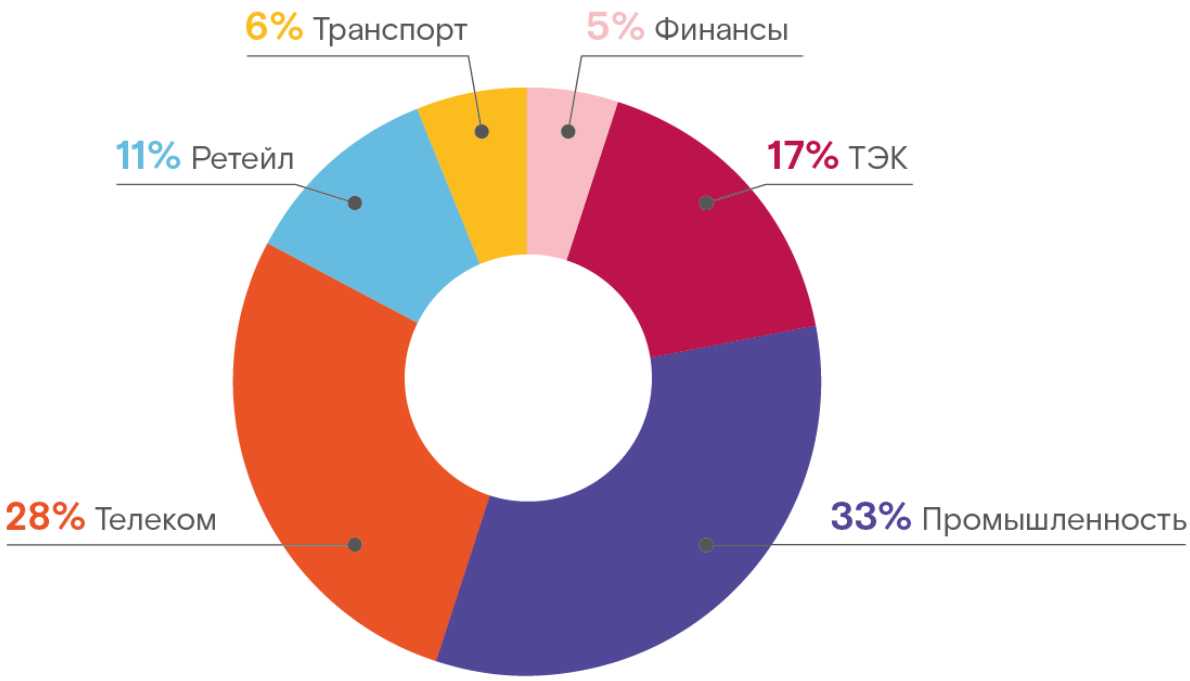
Несмотря на то, что данный недостаток замыкает пятерку рейтинга наиболее критичных разочарований от использования DLP (его отметило более четверти опрошенных компаний), он является очень важным звонком для разработчиков систем защиты от утечек. Этот фактор означает, что существенный процент компаний испытывает большие сложности с эффективным использованием DLP-систем после их внедрения. Неумолимая статистика подтверждает данный вывод: большинство компаний использует не более 10% функционала запущенных в эксплуатацию DLP-систем. Таким образом, бОльшая часть функциональности систем защиты от утечек после внедрения в компании простаивает, поскольку

пользователи не понимают, как с ней работать и какие задачи с ее помощью можно решать.

По мнению аналитиков «Ростелеком-Солар», отсутствие на рынке единой концепции использования DLP является следствием в том числе и отсутствия доступных в информационном пространстве лучших практик применения систем защиты от утечек. Компании, успешно интегрировавшие и использующие данные системы, не делятся своими наработками с рынком. В результате каждый заказчик вынужден решать свои задачи «с нуля».

4.6 Отраслевая специфика компаний

Распределение опрошенных компаний по отраслям



Отраслевые особенности применения DLP

В процессе исследования выяснилось: на общеотраслевом фоне организаций, использующих системы защиты от утечек, характерными особенностями отличаются два основных направления – бизнес-структуры и предприятия сферы ОПК.

Для коммерческих компаний, деятельность которых сконцентрирована на интенсивном развитии бизнеса и извлечении прибыли, характерна максимальная открытость каналов коммуникаций для сотрудников. В этой связи преобладающим сценарием использования DLP-решений в таких компаниях является мониторинг и глубокий анализ каналов коммуникаций и действий персонала. Согласно прогнозам аналитиков «Ростелеком-Солар», в

обозримом будущем рынок систем защиты от утечек будет развиваться в направлении расширения аналитических возможностей DLP-решений и совершенствования инструментов прогнозирования.

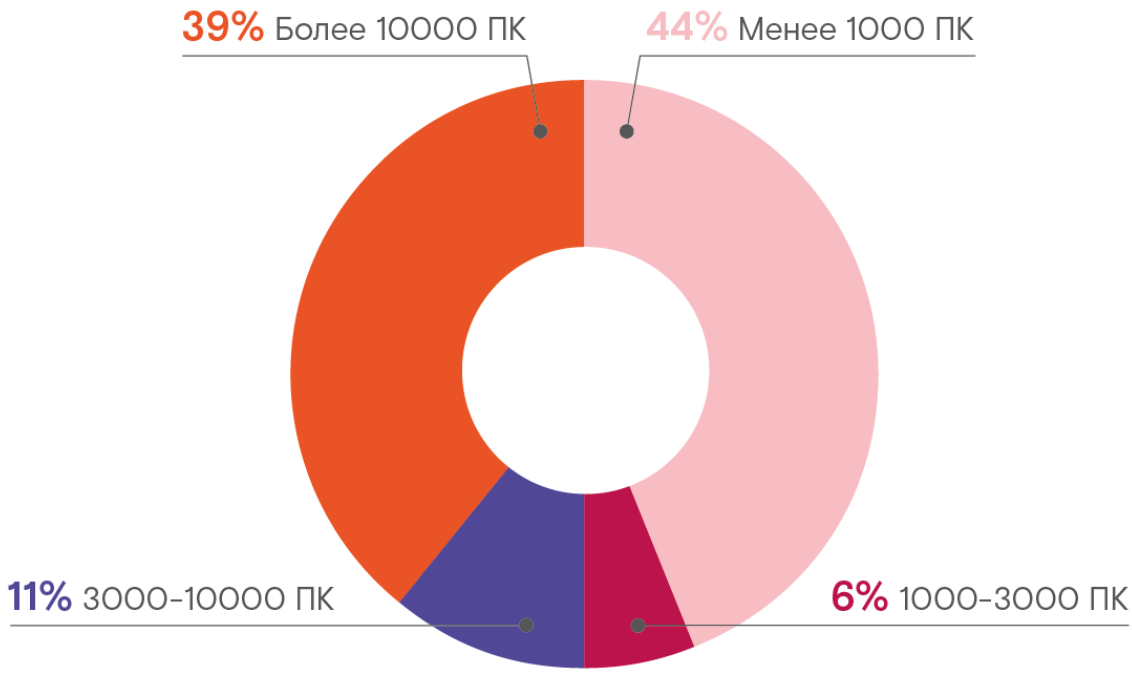
Некоторыми особенностями в бизнес-среде отличается банковский сектор. В связи с наиболее высокими рисками прямого финансового ущерба от ИБ-инцидентов организации данной сферы имеют более-менее формализованные сценарии использования систем защиты от утечек, сформулированные задачи в области DLP, перечень информации и документов, подлежащих защите. В банковском сегменте преобладает использование DLP в режиме блокировки по сравнению с предприятиями других направлений коммерческого блока.

Кроме того, компании финансовой отрасли по причине жесткого отраслевого комплаенса, как правило, имеют четко выстроенные процессы управления инцидентами информационной безопасности. В этой связи ими востребован соответствующий функционал системного управления событиями и инцидентами информационной безопасности. А наиболее развитые DLP-системы являются одним из поставщиков информации о событиях безопасности для систем управления ИБ-инцидентами.

Что касается оборонно-промышленной сферы, предприятия данного профиля ориентированы на максимальные ограничения коммуникаций персонала. Они активно используют блокировку трафика с подозрением на утечку, функциональность управления устройствами, режим выдачи сотрудникам временного доступа к служебным ресурсам и информации и т.п. В целях экономии бюджетных средств компании этого сегмента часто запрашивают у разработчиков DLP-систем различный дополнительный функционал, не характерный для систем данного класса, реализуемый отдельными СЗИ. Например, функционал управления устройствами, шифрования и т.п.

Кроме того, своя специфика прослеживается и у компаний сегмента large enterprise. DLP в подобной инфраструктуре работают на предельном уровне нагрузки и анализируют колоссальные объемы данных. В таких экстремальных условиях крупные заказчики часто предъявляют особые требования к возможностям системы, нетипичные для остальных пользователей. Например, объем архива такой организации может быть настолько велик, что выгрузка информации по требованиям регулятора может занимать до одного месяца. И в течение месяца этому процессу должна быть обеспечена непрерывность и целостность.

4.7 Распределение опрошенных компаний по размеру бизнеса


39% Более 10000 ПК
44% Менее 1000 ПК
11% 3000-10000 ПК
6% 1000-3000 ПК

5. Выводы

Основная проблема отрасли – отсутствие общей концепции работы с DLP

Подводя итоги исследования, аналитики сделали вывод: ключевой причиной разочарований компаний-пользователей в DLP-системах является отсутствие на рынке внятной общей концепции использования DLP, обнародованных лучших практик применения систем данного класса.

Если взглянуть более широко на отрасль информационных технологий в целом, то можно заметить, что практически в любом ее сегменте имеются так называемые best practice использования систем, от которых компании-заказчики могут отталкиваться для решения своих конкретных задач. Так, по любому решению, автоматизирующему деятельность, будь то CRM, различные кадровые системы и проч., имеется множество регламентов, описывающих стандартные задачи, процессы, настройки, регламенты, состав задействованных подразделений, роли сотрудников и т.п. К сожалению, подобные проработанные методики и практики применения систем защиты от утечек на рынке DLP на данный момент отсутствуют.

В то же время авторы исследования уверены: если бы рынок имел общую, согласованную всеми участниками – заказчиками, вендорами и интеграторами – концепцию использования DLP, процент жалоб на отсутствие в этих системах функциональности для решения задач отдельно взятой организации (п. 4.2 данного исследования) был бы значительно ниже. Заказчики смогли бы решить бОльшую часть задач, опираясь на отраслевой опыт.

На нехватке функциональности для решения задач отдельно взятой организации следует остановиться чуть подробнее. Одна из основных причин этого недостатка DLP-систем, отмечаемых заказчиками, кроется в закрытости тематики информационной безопасности в целом и отсутствии доступа вендоров к деталям пользовательского опыта. Когда заказчик ставит разработчику системы защиты от утечек какую-либо задачу, то, к сожалению, он далеко не всегда готов раскрыть причины и предпосылки ее появления, сопутствующие обстоятельства, то есть поделиться всеми деталями кейса. Поэтому вендор часто реализует функциональность по принципу «где-то рядом», а заказчик в итоге получает не совсем то, что нужно.

Если вновь провести аналогию с другими ИТ-системами, то, например, производители средств автоматизации имеют возможность досконально разобрать реальные кейсы заказчиков. Например, если нужно автоматизировать процесс заведения заявки в CRM, вендоры получают доступ ко всем деталям процесса. Однако в случае с утечками информации офицеры безопасности компаний-заказчиков весьма ограниченно делятся с вендорами и интеграторами деталями своих расследований. В результате в DLP-системах появляется «лишняя» функциональность и может отсутствовать желаемая.

Еще один важный вывод, сделанный исследователями по итогам общения с респондентами: у разных отраслей и даже зачастую у разных компаний требования к функциональности DLP-систем не пересекаются. В результате каждому вендору системы защиты от утечек для развития функциональности своего решения приходится выбирать между предпочтениями той или иной отрасли, той или иной группы заказчиков. Таким образом встает вопрос: решаема ли задача разработки силами сообщества общего вектора развития DLP-систем? Возможно ли в целом выстраивание сбалансированного роадмапа для данного класса систем? Или это утопия, и каждый вендор будет развивать свою функциональную линию DLP?

Пути решения проблемы

Использование экспертизы вендора

В отсутствие единой концепции и общепринятых практик применения DLP владельцем наиболее глубокой экспертизы в данном вопросе является вендор. Если же в процессе внедрения системы защиты от утечек интегратор не привлекает вендора, то компания-пользователь DLP эту экспертизу не получает. Соответственно, по результатам дальнейшей эксплуатации системы у заказчика возникают вышерассмотренные разочарования. Участие разработчика DLP-решения на этапе внедрения позволяет заранее учесть накопленный вендором опыт всех его заказчиков, избежать бОльшей части проблем, с которыми эти заказчики ранее уже столкнулись.

Регулярное обучение продукту

Из-за высокой конкуренции на российском рынке DLP функциональность этих систем развивается очень интенсивно. В результате мы наблюдаем некоторый парадокс: зачастую компании, только приступившие к использованию DLP-систем, владеют их функциональностью лучше, чем применяющие ее десяток лет. Одна из причин этого явления – отсутствие у многих старожилов практики регулярного обучения новому функционалу.

Им кажется, что они хорошо знают систему, но на самом деле часто используют лишь десятую часть ее функциональности. Другая причина – наработанные годами привычные сценарии использования решения для защиты от утечек. Но технологии защиты, как и угрозы, постоянно развиваются. Соответственно, службам безопасности компаний необходимо идти в ногу со временем, перестраивать свою работу, выходя за рамки устоявшихся процессов.

Аналитический консалтинг и автоматизация аналитики

В процессе эксплуатации DLP-систем многие пользователи сталкиваются с проблемой отсутствия в достаточном количестве квалифицированных аналитических кадров для работы с системой. Решения класса DLP закрывают обширный и сложный пласт работы в области информационной безопасности. А значит, должны эксплуатироваться квалифицированными специалистами, которые разбираются в информационной безопасности, имеют специализированное образование и аналитический склад ума. И, конечно, отрасль испытывает нехватку таких кадров.

Решение этой проблемы лежит сразу в двух плоскостях: с одной стороны, заказчикам необходим аналитический консалтинг и передача вендорского опыта, без которых не обойтись. А с другой стороны, вендоры должны работать над автоматизацией аналитических возможностей своих решений, чтобы заказчики получали больше ценности «из коробки» и могли самостоятельно решать бОльшую часть своих задач.

Контактная информация

Телефоны:

+7 (499) 755-07-70 — продажи и общие вопросы

+7 (499) 755-02-20 — техническая поддержка

E-mail: info@rt-solar.ru support@rt-solar.ru

Адреса:

125009, Москва, Никитский пер., 7, стр. 1.

127015, Москва, ул. Вятская, 35/4, БЦ «Вятка», 1-й подъезд.