Какой должна быть эффективная DLP-система?

DLP-системы существуют уже несколько лет. За это время они заняли определенное место на рынке средств защиты информации и оформились в отдельные продуктовые предложения. Однако сейчас вокруг DLP вновь разгорелся спор: способны ли эти системы обеспечить эффективный контроль за всем многообразием коммуникаций, да еще и в условиях постоянно изменяющихся технологий? От кого и от чего все же должны защищать DLP-системы? На эти и другие вопросы редакции журнала ответили эксперты:

Роман Ванерке, *технический директор АО "ДиалогНаука"*
Сергей Вахонин, *директор по решениям DeviceLock, Inc. ("Смарт Лайн Инк")*
Дмитрий Кандыбович, *генеральный директор компании StaffCop (ООО "Атом Безопасность")*
Александр Ковалёв, *заместитель генерального директора Zecurion*
Алексей Кубарев, *менеджер по развитию направления DLP Solar Dozor компании "Ростелеком-Солар"*
Елена Нагорная, *руководитель направления департамента по защите активов и информации АО "Техснабэкспорт"*
Алексей Плешков, *эксперт по информационной безопасности*
Константин Саматов, *руководитель направления в Аналитическом центре Уральского центра систем безопасности, член Ассоциации руководителей служб информационной безопасности, преподаватель дисциплин информационной безопасности в УрГЭУ и УРТК им. А.С. Попова*
Анатолий Скородумов, *заместитель директора, начальник отдела информационной безопасности (CISO), ПАО "Банк "Санкт-Петербург"*

– Выбор DLP-решения: какие возможности системы рассматриваются как наиболее значимые заказчиком? На что стоит обратить внимание заказчику?

Роман Ванерке

– Всесторонний анализ, широкое покрытие возможных каналов утечки, агрегация и визуализация данных. Немаловажным является также удобство работы с системой. Если ее трудно настраивать, непонятно, как использовать и как в ней работать, то такая система рано или поздно перестанет применяться.

Сергей Вахонин

– Прежде всего мы рекомендуем заказчику сфокусироваться на определении сути задачи, на формулировании основных функциональных требований к системе, думать не о модулях, а о функциях. Все сформулированные по принципу "ничего не забыть" функциональные требования к DLP-решению должны быть полностью реализованы в выбранном продукте, а не в перспективе или с оговорками. Стоит обратить внимание на фактическую применимость заявленных возможностей, особенно таких, как семантический анализ, продвинутые технологии детектирования конфиденциальных данных, ведь описанные в маркетинговых брошюрах и на сайтах функции анализа частенько работают только для решения одной из глобальных задач DLP-систем – для анализа архива событий и теневых копий и расследования инцидентов. Необходимо понять, способна ли рассматриваемая система эффективно решать задачу предотвращения утечек данных (да, это ключевая задача для DLP-систем, но далеко не все представленные на российском рынке продукты действительно решают эту задачу техническими способами), или ее функциональный арсенал обеспечивает только наблюдение за перемещением информации наружу и расследование инцидентов по фактам состоявшихся утечек, т.е. защита от утечек "опирается" на организационные меры и страх увольнения при выявлении инцидента. Изучая этот вопрос, особое внимание следует обратить на спектр, полноту и качество контроля потенциальных каналов утечки информации, способность в реальном времени обнаруживать в потоке передаваемых данных информацию ограниченного доступа; здесь стоит учесть, что часто заявленные возможности предотвращения утечек и тем более функции анализа содержимого в момент передачи данных лимитированы весьма узким спектром каналов передачи данных. Достаточно ли аналитических возможностей и отчетов для регулярного анализа и выявления потенциальных злоумышленников? Наконец, хватит ли собственных ресурсов для запуска и эксплуатации системы, качественно ли выполнена документация или без помощи интегратора не обойтись? Все эти вопросы стоит изучить в ходе независимого от вендоров и интеграторов пилотного исследования решений.

Дмитрий Кандыбович

– Сейчас нужно как можно больше логов, больше архива, функционал логирования переписки, звука с микрофона, мессенджеров, взаимосвязей и прочего –

эти инструменты стали обязательными в DLP-системах. Ими пользуются в основном офицеры службы безопасности, которые конкретно работают по группе риска. Проблемы здесь две: дороговизна инфраструктуры, что отталкивает людей от внедрения DLP, и сложность ее настройки. Пять лет назад мы поняли, что будущее за продуктами Open Source. При таком подходе есть возможность обойти сложности со стоимостью инфраструктуры, выбирая продукты, у которых серверная часть, например, полностью опенсорсная. Сложность настройки связана с ложными срабатываниями. Подход блокировки по контенту понемногу себя изживает в соответствии с рядом ограничений. Мы используем блокировки по меткам файлов, это дает хороший результат.

Александр Ковалёв

– Современные DLP-решения Enterprise-сегмента достаточно близки по функционалу, но для себя мы видим следующие тенденции при выборе:

- работоспособность в сложной инфраструктуре. На практике часто после реального пилота серьезно меняется расклад сил в пользу надежно работающего и управляющегося максимально просто продукта;
- наличие полноценного Linux-агента, который раньше часто требовался для галочки, а теперь является реально используемой возможностью контроля;
- качество поведенческого анализа (UBA) и другой дополнительной автоматизированной аналитики в помощь ИБ-аналитикам;
- интеграция или наличие собственных смежных решений, например NGFW/SWG/прокси, SIEM, PAM;
- гибкая система отчетности и удобный Web-интерфейс в единой консоли, которым пока могут похвастаться далеко не все даже ведущие вендоры, – это существенно упрощает реальную эксплуатацию после пилота;
- поддержка современных каналов, таких как Telegram или WhatsApp, как разных типов приложений, так и Web-версий;
- возможность частичной замены популярного Microsoft TMG в части прокси, контроля трафика, связи трафика с пользователями LDAP (так называемый Identity Awareness), ограничение доступа к Web-ресурсам по современным базам URL и т.п.;
- развитые инструменты аналитики (в т.ч. пресловутых больших данных).

Если смотреть шире, то в DLP крайне важна удобная масштабируемость, отказоустойчивость и практичность в управлении и построении отчетов.

Алексей Кубарев

– По нашему опыту общения с заказчиками, наиболее востребованными возможностями DLP-систем являются покрытие реально используемых в компании каналов коммуникаций, скорость работы системы (перехвата и анализа) и способность обработки трафика больших объемов, удобство использования (представления информации, формирования отчетов и т.п.). Кроме того, крайне важно не только правильно выбирать техническое средство защиты от утечек, но и отдавать предпочтение производителю, который обладает всей необходимой экспертизой в конкретной отрасли, чтобы система была настроена в соответствии со спецификой организации. Также важно оперативное исправление замечаний, возникающих в процессе пилотирования и боевой эксплуатации DLP-решения.

Елена Нагорная

– Считаю, что на данный вопрос нет однозначного ответа. В каждом конкретном случае зависит от потребностей заказчика. В зависимости от того, насколько критичная информация обрабатывается в системах компании, решившей внедрить DLP-систему, будет и формироваться потребность в функционале. Для нашей компании основным функционалом, которым должна обладать DLP-система, является возможность системы работать с "цифровыми отпечатками" документов, ввиду большого объема документов с информацией ограниченного распространения. Думаю, что для некоторых компаний важен функционал оценки лояльности сотрудников и учета их рабочего времени.

Алексей Плешков

– Одним из ключевых требований к современной DLP-системе является наличие в интерфейсе гибких возможностей для самостоятельного создания заказчиком отдельных цепочек правил или присутствие набора предустановленных правил выявления и предотвращения утечек чувствительной информации, созданных на основе предыдущего опыта внедрения решения и лучших мировых практик. Не менее важной является "совместимость из коробки" с ведущими комплексами для мониторинга инцидентов информационной безопасности. Преимуществом DLP, на которое также стоит обратить внимание заказчику, является функционал поиска и выявления вероятных утечек в максимально широком поле файловых форматов и расширений, в том числе проприетарных (поддержка в DLP расширений только офисных файлов должна сразу насторожить заказчика).

Константин Саматов

– При выборе DLP-решения важно определить, какие каналы передачи информации используются в организации (почта, съемные носители, мессенджеры) для осуществления рабочих коммуникаций. Исходя из выявленных каналов необходимо выбрать решение, способное обеспечивать их перехват. Кроме того, необходимо обращать внимание на архитектуру информационной системы, чтобы при внедрении системы избежать проблем с совместимостью.

Анатолий Скородумов

– Все зависит от того, какие цели ставит заказчик при внедрении DLP-решения. В общем случае при выборе DLP-системы стоит обратить внимание на наличие следующих функций:

- возможности использования системы в режиме предотвращения утечек;
- объем покрытия актуальных для вас каналов утечки информации;
- возможность создания архива всей исходящей информации с обеспечением гибкого поиска по этому архиву;
- наличие предустановленных политик по выявлению отправки стандартных типов защищаемой информации: персональных данных, финансовой информации, клиентских списков;
- возможность выявления заполненных форм стандартных для организации документов;
- умение работать с цифровыми отпечатками документов с возможностью указания степени совпадения;
- наличие модулей для мобильных устройств;
- наличие развитого функционала в агентах, устанавливаемых на конечные рабочие станции.

Стоит также обратить внимание на политику лицензирования продукта, возможности его масштабирования и нали-

чие механизмов отказоустойчивости. И безусловно, для установки в своей организации следует серьезно рассматривать системы, имеющие большое количество реальных внедрений в России.

– Существует мнение, что никакие DLP-системы не способны обеспечить эффективный контроль за всем многообразием всевозможных коммуникаций практически в условиях постоянно изменяющихся технологий. Так ли это?

Роман Ванерке

– Конечно, пока не придумали устройства, стирающего память, как в "Людях в черном", ведь конфиденциальную информацию всегда можно запомнить. Кроме того, ее можно переписать ручкой, сфотографировать/записать видео, записать на диктофон и т.д. Поэтому ни одно решение не заявляет и не может заявить, что защищает на 100%. Эффективное качественное решение позволяет анализировать основные, наиболее вероятные, каналы передачи данных – Web, почта, съемные устройства, печать, мессенджеры, в большинстве случаев этого более чем достаточно. Все остальные каналы рекомендуется блокировать как на уровне МЭ, так и на уровне АРМ.

Сергей Вахонин

– Такое мнение чаще всего опирается либо на печальный опыт, когда приобретенная DLP-система приводит к утечке информации, либо на недостаточные знания о возможностях полнофункциональных DLP-систем. Утечки информации при наличии установленной DLP-системы происходят чаще всего или потому, что выбранное DLP-решение устанавливалось "для вида" и имитации бурной деятельности службы ИБ, или оно неспособно предотвращать утечки в силу своей ограниченности по широте каналов либо из-за акцента на анализ архива событий и теневых копий (post-DLP).

Безусловно, нет смысла спорить с тем, что в эпоху бурного развития коммуникационных технологий постоянно видоизменяются и растут возможности пользователей, но, с другой стороны, отрицать как необходимость защиты от утечки данных, так и принципы построения комплексных систем, когда для решения задачи используются одновременно набор технических средств в сочетании организационными мерами, тоже некорректно. Существует простое правило: чем меньше в DLP-системе контролируемых каналов утечки данных, тем шире возможности злоумышленников. Попытки злоумышленников найти неконтролируемый канал для намеренного слива информации будут существенно ограничены при использовании полнофункционального DLP-решения, решающего все три основных задачи контроля: Data-in-Use, Data-in-Motion и Data-at-Rest. Разработчики же в свою очередь должны учитывать развитие коммуникационных систем и постоянно расширять спектр контролируемых каналов передачи данных.

Грамотный подход к защите данных от утечки заключается в сочетании трех ключевых мер. Первая – нейтрализация наиболее опасных векторов угроз утечки информации, достижимая через реализацию сценария минимальных привилегий, когда пользователям доступны только те каналы передачи данных и устройства хранения, которые действительно необходимы для работы, при этом данные, передаваемые и сохраняемые через доступные каналы и устройства, инспектируются на предмет наличия информации ограниченного доступа, передача которых недопустима и должна быть заблокирована. Вторая ключевая мера – мониторинг прочих потенциальных каналов утечки информации для снижения негативного влияния угроз. Наконец, третья – регулярный анализ данных, хранимых на рабочих станциях сотрудников. А если еще и посмотреть в сторону создания стерильных рабочих сред в средах виртуализации с использованием удаленного доступа, который ставится под защиту DLP-системы, то вероятность утечки конфиденциальной информации становится намного ниже.

Дмитрий Кандыбович

– End-Point-решения позволяют собирать очень много данных не только по движению информации, но и по запуску программ, меняют сертификат на агенте, т.е. покрывают полный функционал. Вы можете видеть, что человек делает, с какими документами работает, их передвижение, копирование, удаление, на особо важные документы вы можете делать теневую копию на любое действие. Против мобильных устройств пока нет решения. Есть разнообразные технические средства, которые обещают защиту или как минимум понимание, кто фотографировал и у какого пользователя был документ. Но они работают на особых условиях и на российском рынке массово не продаются. Зарубежные аналоги стоят достаточно дорого. Какую бы DLP-систему вы ни внедрили, с этим бороться достаточно сложно.

Александр Ковалёв

– Конечно, ни одно решение по ИБ не защитит на 100%, однако надежность работы правильно настроенной DLP-системы крайне высока. К тому же есть много смежных кейсов, например мониторинг активности подозрительной группы сотрудников, профилактика утечек, архивирование информации о действиях сотрудников, контроль за привилегированными пользователями, выявление невидимых глазу аномалий и т.п., которые трудно реализовать без DLP.

Алексей Кубарев

– Перед DLP-системами никогда не стояла задача контроля всех коммуникаций, речь всегда шла о коммуникациях в корпоративной среде. С этой точки зрения проблемой становится перенос рабочих коммуникаций во внерабочую среду, где у работодателя нет не только технической, но и юридической возможности контролировать своих сотрудников.

Что касается корпоративных коммуникаций, то я не вижу негативной тенденции: даже оказавшиеся в какой-то момент вне контроля мессенджеры сегодня вполне успешно контролируются DLP-функциональностью. Что, на мой взгляд, сегодня действительно важно – это возможность увидеть общую картину коммуникаций по различным каналам. Поэтому аналитические возможности DLP и возможности визуализации приобретают все большее значение.

Елена Нагорная

– Все зависит от уровня зрелости компании в вопросах информационной безопасности. В ряде организаций, с которыми мне приходится взаимодействовать, закрыты USB-порты, отсутствует прямой доступ в сеть Интернет, запрещено использование программного обеспечения, не входящего в перечень разрешенного к использова-

нию, закрыты права локального администратора на АРМ. В случае, если уровень обеспечения информационной безопасности в компании находится на высоком уровне, это будет только в помощь внедренному решению. Любая DLP-система справится с оставшимися "не под запретом" задачами.

Алексей Плешков

– Эффективность функционирования решения класса DLP, как и многих других комплексных решений, сильно зависит от стабильности и неизменности инфраструктуры той среды, в которой оно внедрено. Для псевдостатического случая, когда обновления и реконфигурация DLP происходят чаще, чем внешние изменения в окружающей DLP инфраструктуре, она продолжает выполнять контрольные функции в соответствии с изначально заявленными требованиями. В динамически изменяющейся среде, когда патчи и обновления с новыми функциями для DLP регулярно запаздывают, мастер релизы флагманской версии агентов не успевает за обновлениями операционной системы, а несовместимость агентов с актуальными базами обновлений антивирусных средств вызывает на рабочих станциях фатальные последствия, говорить о каком-либо эффективном контроле на местах не приходится.

Константин Саматов

– Внедряемое DLP-решение действительно контролирует лишь определенный набор заложенных разработчиком ПО каналов передачи информации. Однако нередко с обновлением ПО расширяются контролируемые каналы передачи информации.

Анатолий Скородумов

– На мой взгляд, это действительно так. Развитие DLP-систем отстает от развития современных средств и способов коммуникации между людьми и методов обмена информацией. Поэтому, внедряя DLP у себя в компании, надо четко понимать, какие каналы утечки информации вы планируете с помощью нее закрыть и насколько это будет эффективно при наличии других, незакрытых каналов.

– От кого и от чего все же должны защищать DLP-системы?

Роман Ванерке

– Основное назначение – защита от непреднамеренных (случайных) утечек конфиденциальной информации.

За счет правильной настройки политик и размещения компонентов системы – защита от внутреннего злоумышленника.

Также повышение эффективности систем защиты от APT, т.к. система выполняет анализ данных и может зафиксировать передачу чувствительных данных (файл с паролями, например) или неизвестные типы шифрования, что повышает эффективность защиты от внешних злоумышленников.

Сергей Вахонин

– Казалось бы, вопрос риторический и напрашивается ответ "от инсайдеров, конечно". Однако инсайдер – это всего лишь человек, имеющий доступ к внутренней информации, причем чаще всего необходимой ему для выполнения своих задач. Поэтому правильный ответ: DLP-системы должны защищать организации от умышленных и случайных попыток передачи, печати и сохранения информации, а также выявлять и устранять факты несанкционированного хранения данных ограниченного доступа, и все это во имя одной цели – не допустить утечку. Все остальные возможности DLP-систем, такие как аналитические модули, системы поиска по архиву, отчеты и графы, досье и карточки, функции анализа контроля поведения пользователей, – это важный, но по большому счету все же дополнительный "обвес" к ключевому функциональному блоку, решающему задачу контроля перемещения данных и предотвращения утечек информации ограниченного доступа. Если DLP-система позволяет так или иначе перекрывать передачу данных только по электронной почте да на флешке, а с остальных каналов умеет только снимать теневые копии, то с досье и графа связей толку не будет, это уже не система предотвращения утечки данных, а дубина, которой размахивают после утечки.

Дмитрий Кандыбович

– Производители DLP фокусируются на внутренних проблемах. Какие риски исходят от инсайдеров? В первую очередь сотрудники обрабатывают документы, которые принадлежат компании, и не всегда пользователи с этим согласны. Внутреннее мошенничество многогранно, безгранично и уникально для каждой компании. Внутри компании, независимо от сферы и специфики деятельности, есть возможность внутреннего входа и есть группа риска, которую нужно по полной обкладывать логами и тотально разбирать все их события. Второе направление – люди просто могут не работать в течение своего рабочего времени, если их не контролируют.

Александр Ковалёв

– Правильнее было бы сказать, ЧТО должны защищать DLP-системы, а это данные. И потенциальную угрозу для них несут в первую очередь инсайдеры, обладающие доступом к ним и намеренно или случайно имеющие возможность вынести их за пределы корпоративной сети для передачи конкурентам или продажи на черном рынке. Для своевременного обнаружения таких утечек и блокирования их на этапе передачи данных DLP-решения подходят идеально. И конечно, крупные организации сами активно борются с инсайдерами и публично ставят их в топ угроз данным и бизнес-процессам.

Алексей Кубарев

– Традиционно DLP-системы призваны защищать конфиденциальную информацию компаний от случайных и намеренных утечек, а также служить инструментом для проведения расследований инцидентов, связанных с утечками данных. Однако за последние пять лет на рынке DLP произошли изменения: DLP-система из инструмента информационной безопасности превратилась в инструмент безопасности в широком понимании. Сегодня DLP решает задачи экономической безопасности, противодействия коррупции, управления конфликтом интересов, внутреннего контроля. А это значит, что фокус внимания смещается от данных к человеку. Какую бы угрозу безопасности мы ни рассматривали, за ней всегда стоит человек, по неосторожности ли он наносит ущерб или по злому умыслу.

Елена Нагорная

– DLP-решения должны не защищать, а нивелировать риски утечки за пределы контролируемой зоны значимой для компании информации. Такая утечка может быть намеренной и ненамеренной. Практика показывает, что большая часть ставших известными утечек происходит не по злому умыслу, а из-за ошибок, невнимательности, небрежности работников.

Алексей Плешков

– К сожалению, DLP как отдельное средство защиты уже на протяжении многих лет не используется. Связано это прежде всего с невозможностью управлять ошибками первого и второго рода в работе DLP. Сейчас DLP функционирует скорее как средство контроля постфактум онлайн-инцидентов информационной безопасности. Активная блокирующая функция DLP уступает место инструментам сигнальной функции о возможной утечке и/или функциям активного уведомления о наступлении событий с признаками инцидентов ИБ.

Константин Саматов

– Если говорить именно о DLP-системах, то они должны защищать от утечек конфиденциальной информации за периметр организации, как случайных, так и умышленных.

Анатолий Скородумов

– Безусловно, хочется иметь DLP-систему, которая защищала бы от всего спектра возможных угроз утечек данных по всем доступным в настоящее время каналам. Но такой панацеи на рынке средств информационной безопасности нет.

На данный момент DLP-системы неплохо справляются с защитой от утечки значимой информации из-за неумышленных действий пользователей (отправил файл себе на личную почту, чтобы с ним поработать дома; отправил, не подумав, информацию контрагенту через Интернет в незащищенном виде; ответил по почте на запрос клиента, приложив клиентские данные, и т.п.).

В ряде случаев DLP-система может помочь выявить умышленный "слив" данных, но зачастую утечка происходит по причине низкой квалификации работника, осуществляющего эти действия. Поймать квалифицированного специалиста, копирующего себе информацию, вряд ли удастся исключительно средствами DLP-системы. Для этого необходим целый спектр механизмов защиты и организационно-технических мероприятий.

– Анализ событий и инцидентов в архиве vs противодействие утечкам: что важнее, полезнее, эффективнее?

Роман Ванерке

– Эти два подхода скорее дополняют друг друга, т.к. позволяют решить разные задачи. В первом случае за счет наличия истории: возможность постфактум выявить источник утечки, какие еще данные могли быть переданы, с какими лицами было взаимодействие, как оно было осуществлено и т.д. Во втором случае – обеспечение защиты, предотвращая или заметно усложняя передачу конфиденциальных данных в момент передачи. По сути, это как противокражное оборудование и система видеонаблюдения в магазине. Противокражное оборудование иногда ошибается, "пищит", когда не нужно, или, наоборот, если снять метку, будет молчать, но в целом никто не сомневается в эффективности обеих мер.

Сергей Вахонин

– Любой инструментарий в DLP-системах, даже вспомогательный, приносит пользу, если в итоге он направлен на противодействие утечкам данных. Противодействие утечкам, да еще и с возможностью инспекции содержимого передаваемых данных в момент их передачи (контентная фильтрация в реальном времени) – безусловно, наиболее эффективная функция для решения задачи "не допустить утечку данных". Для анализа рисков и выявления потенциальных злоумышленников важно иметь развитый аналитический инструментарий анализа архива событий и теневых копий, причем с широкого спектра каналов передачи данных. Все функции важны, все функции значимы.

Дмитрий Кандыбович

– Блокировки по контенту не работают из-за ложных срабатываний. Требуется большой штат сотрудников, которые будут в режиме реального времени их обрабатывать. Бизнес такую систему выпилит за два инцидента, после того как прибежит коммерческий директор и скажет, что письмо не ушло из-за ложного срабатывания и компания потеряла деньги. Для СБ факт отправки сотрудником письма с секретным документом не показателен. Доказать умысел невозможно. Нужно, чтобы инцидент произошел, чтобы офицер службы безопасности был оповещен и собрал доказательную базу, которую признают в суде, и чтобы можно было остановить человека с флешкой на проходной. Если есть полноценный лог, по которому можно найти первоисточник, кусок документа, событие, кто был в него вовлечен, как оно развивалось, – это гораздо ценнее.

Александр Ковалёв

– Эффективнее соединить оба подхода и блокировать наиболее опасные активности. При этом многие нарушения персонала, связанные с данными или информационными активами организации, могут и не превратиться в утечку, например внутренняя переписка, обсуждение каких-то противозаконных планов в Web-версии Telegram или обмен персональными данными конкретного сотрудника. Однако DLP может обнаружить все цепочки связей и стать Push-системой для поиска более значимых нарушений или вредящих организации активностей, например внутреннего саботажа, кражи денег или махинаций с картами клиентов.

Алексей Кубарев

– Если говорить о российских DLP-решениях, то вопрос противопоставления здесь не стоит. Как правило, системы защиты от утечек, имеющие развитые средства блокировки на основе контентного анализа, имеют и зрелый архив, развитые средства поиска и аналитику. Для некоторых компаний ввиду специфики их деятельности вполне имеет смысл использовать поиск в архиве

вместо блокировок. Но компании, которым нужна блокировка, не обойдутся без инструментов расследования и аналитики.

Елена Нагорная

– Все же я являюсь сторонником противодействия утечкам. Система должна быть настроена так, чтобы проактивные действия были эффективными. Все-таки DLP-решения изначально предназначались именно для этих целей и только потом появились дополнительные возможности, и то преимущественно в решениях российских производителей. Да и ценность информации при ее утечке теряется, а для некоторых компаний информация – самый ценный ресурс.

Алексей Плешков

– Мой опыт работы с DLP указывает на то, что в DLP функции онлайн-блокировки и аналитики в режиме реального времени существенно уступают возможностям ретроспективного анализа как в ручном, так и в автоматическом режиме. Присутствие в инфраструктуре заказчика дополнительных компонентов, с которыми должна быть интегрирована DLP (например, системы корреляции событий информационной безопасности, комплексные дашборды, внешние учетные или аналитические ИБ-системы, визуализаторы и пр.), практически сводит к нулю применение собственной (встроенной) онлайн-аналитики в DLP. С другой стороны, если у заказчика нет сложной инфраструктуры и решение DLP внедряется и применяется по схеме Stand-Alone, тогда весь арсенал встроенных возможностей DLP, может, и будет применяться и играть важную роль в системе информационной безопасности данной организации.

Константин Саматов

– Если говорить о DLP-решении, то необходимы обе функции. Прежде всего необходимо предотвращение утечки конфиденциальной информации по ошибке (случайная отправка электронного сообщения, содержащего конфиденциальную информацию). В свою очередь, аналитические инструменты для работы с архивом попадающей в DLP-систему информации важны при выявлении утечек информации, связанных с умышленными действиями пользователей.

Анатолий Скородумов

– DLP-системы прежде всего должны предотвращать утечку данных, а уже во вторую очередь помогать разбираться с тем, как та или иная утечка могла произойти. Большое количество данных "утекает" в Интернет из-за неумышленных ошибочных действий сотрудников. Гораздо более оптимально предотвращать утечку и учить таких пользователей правильному обращению с конфиденциальной информацией, чем просто фиксировать утечки и наказывать виновных. Ведь попавшие в Интернет данные со 100% гарантией уже не удалить. Некоторые специалисты по безопасности считают, что лучше скрывать от сотрудников наличие в компании DLP-системы и тайно следить за действиями сотрудников. Но это очень быстро становится секретом Полишинеля. Скажу больше, даже если у вас в организации нет DLP-системы, работники все равно будут считать, что служба безопасности просматривает всю исходящую почту и любую другую информацию.

– Активное продвижение UAM-решений под флагом DLP-систем имеет ли право на жизнь? Насколько эффективны функции мониторинга пользовательской активности?

Роман Ванерке

– UAM-решения могут эффективно использоваться в качестве одного из элементов в системе защиты от утечек.

Сергей Вахонин

– Функции анализа пользовательской активности, от отчетов до снятия и сохранения клавиатурного ввода и записи экрана, могут стать весьма ценным "довеском" к DLP-системе, если они не являются первичными в реализации системы и предназначены прежде всего для сбора доказательной базы при расследовании инцидентов и собственно анализа поведения, выявления аномалий и групп риска.

При этом попытки декларировать UAM-системы как решающие задачу предотвращения утечек данных – не более чем желание отщипнуть кусочек пирога с рынка DLP-систем, а их эффективность в решении этой задачи строится на психологическом факторе и весьма условна.

Дмитрий Кандыбович

– Мы позиционируемся как система мониторинга. Если у вас есть ценная информация, вы можете загнать ее в определенный периметр и там уже настраивать блокировки. Можно технически заблокировать ряд каналов и оставить "дырку в заборе", которую контролировать и которой будут пользоваться сотрудники, склонные к нарушениям. Должна быть возможность настройки автоматических алертов. Их можно настраивать как в DLP на контент (слова, словосочетания, маски), так и на любое событие. Например, отправка через почту определенного документа в шифрованном архиве. Алерт на аномалии поведения пользователей – тоже очень полезная функция. Алерты должны быть привязаны не только к контенту, но и к тем событиям, которые по вашей карте безопасности считаются неправомерными.

Александр Ковалёв

– Для UAM-решений, конечно, это имеет право на жизнь, если приносит прибыль. При этом стоит разделять сегменты и масштабы внедрений, ведь редко какой продукт мониторинга активности сотрудников справится с производительностью даже агентской части, не говоря уже про сетевой разбор десятков гигабайт трафика, оперативный поведенческий анализ (UBA), контроль второстепенных каналов и объединение всей этой информации в диаграммы связей для мгновенного реагирования на инциденты.

Алексей Кубарев

– Функционал у этих двух классов решений принципиально разный. Системы контроля действий сотрудников по сути контролируют действия приложений на рабочих станциях пользователей. Они способны показать, сколько времени использовалось то или иное приложение на рабочей станции, и на этом основании сделать некоторые выводы: выполнял

ли сотрудник свои трудовые обязанности или бил баклуши. Это задача, никак не связанная с утечками информации, поэтому UAM не может заменить DLP-системы. При этом уже сейчас в DLP-системах есть все возможности для сбора информации о пользовательской активности, остается научить систему обрабатывать эту информацию, а ИБ-специалистов – правильно интерпретировать полученные данные.

Елена Нагорная

– Право на жизнь имеет каждое решение. Каждое решение разрабатывается для каких-то определенных целей и имеет своего потребителя. Как говорится, спрос рождает предложение. На сегодняшний день функции пользовательской активности нами не используются, но мы планируем задействовать ограниченный функционал для контроля продуктивного рабочего времени в рамках перевода ряда работников на дистанционную работу.

Алексей Плешков

– Отдельные российские и белорусские вендоры, давно работающие на рынке DLP-решений в России и в СНГ, регулярно поднимают флаги UAM/DLP. Но это больше маркетинговые флаги. На мой взгляд, нужно всегда идти от задачи заказчика. Чтобы понять, какой тип решения по безопасности нужно предложить заказчику, целесообразно для начала сесть и совместно с ним обсудить, какую конкретную проблему (применительно к инфраструктуре, бизнес-процессам и типам пользователей) он решает в организации. Когда получается построить это обсуждение на реальных кейсах из практики заказчика и внешнего опыта, найти подходящее решение класса UAM, DLP или иные, становится гораздо проще и зачастую эффективнее для всех.

Константин Саматов

– Использование UAM-решений расширяет сферу применения системы, помимо защиты от утечек информации появляются новые возможности: выявление работников, нарушающих трудовую дисциплину, и работников, участвующих в противоправной деятельности (употребление, торговля наркотиками, занятие проституцией, мошеннические схемы). Однако продвижение совсем другого класса решения под флагом DLP вносит путаницу и вызывает сложности с выбором у специалистов по корпоративной безопасности.

Анатолий Скородумов

– Основное отличие UAM-решений от DLP-систем в том, что они не предназначены для предотвращения утечки данных. Если вы планируете использовать DLP исключительно в пассивном режиме, только для мониторинга событий, связанных с возможной утечкой информации, то можно рассматривать UAM-решения как альтернативу такому внедрению.

– Если сохранять в централизованном архиве весь поток данных, это приводит к попаданию в него личных данных сотрудников. Законны ли и допустимы ли их сбор и хранение в архивах? Как решать эту проблему?

Сергей Вахонин

– Во многих странах хранение личных данных сотрудников в корпоративных ИС категорически недопустимо, а за доступ служб ИБ к, например, личным фотографиям могут быть наложены весьма неприятные санкции, и такие прецеденты неоднократно имели место. Принцип невмешательства в личную переписку на Западе является одним из основных факторов при выборе и внедрении DLP-систем. Для решения этой проблемы в DLP-решении должны быть предусмотрены, во-первых, техническая возможность обрабатывать только те коммуникации, в которых выявлены конфиденциальные корпоративные данные, во-вторых, возможность собирать, обрабатывать и хранить только эту часть коммуникаций работника, исключив таким образом проблему сбора и хранения личных коммуникаций организацией. Это реализуется, если в DLP-системе реализована контентная фильтрация потоков данных, когда есть возможность задать политики для детектирования только тех данных, которые непосредственно являются корпоративной информацией, например содержат определенные признаки, теги, ключевые слова и выражения, совпадают с шаблонами (цифровыми отпечатками). При корректной работе правил контентной фильтрации в реальном времени непосредственно на рабочих станциях пользователей (разумеется, при наличии такой функции в DLP-решении) служба ИБ получит возможность контролировать содержимое исходящих сообщений и передаваемых (печатаемых, сохраняемых) файлах, а также сохранять в централизованном архиве только значимую для задач безопасности информацию, не затрагивая личные данные сотрудников.

Дмитрий Кандыбович

– Для того чтобы вы могли правомерно контролировать сотрудника, вам нужно его деятельность, информацию, которую он обрабатывает, технические каналы связи, которые он использует, перевести из разряда личных в служебные. Вы даете человеку бумагу, в которой написано, что на предприятии внедрен режим коммерческой тайны, вы обязаны контролировать документы и от вас этого требует закон. Следует перечислить средства, принадлежащие компании, которые человек использует (Интернет, телефон и пр.), и указать, что в случае попадания личной информации в служебный периметр вы никакой ответственности за это не несете. Эти документы покрывают 99% случаев. Если вы предпринимаете ряд административных мер, то пользоваться DLP или системой мониторинга становится абсолютно правомочно и легально.

Александр Ковалёв

– Это сложный вопрос, и ответ на него лучше адресовать корпоративным юристам до или во время внедрения DLP. Чисто технически можно ограничить сбор персональных данных (не сохранять их в архив, маскировать, токенизировать или вырезать в автоматическом режиме), контроль потенциально только личных каналов передачи и т.п., но в таком случае не будет доказательной базы.

Алексей Кубарев

– Решать эту проблему можно лишь путем легитимизации использования DLP-систем в компании. Если ввести режим коммерческой тайны, подписать с сотрудником соответствующее допол-

нительное соглашение к трудовому договору о том, что он осведомлен об использовании в компании системы защиты от утечек и что его личная переписка по рабочим каналам коммуникаций может попасть под мониторинг и в архив, то использование DLP допустимо. В компании можно ввести процедуру отзыва сотрудником его личных данных из системы мониторинга, подразумевающую письменный запрос в службу информационной безопасности компании.

Елена Нагорная

– Все зависит от политики компании. Рабочий компьютер предназначен для обработки служебной информации, а никак не личных персональных данных. Положения о том, что обработка личных персональных данных на рабочих компьютерах запрещена, часто прописываются в инструкции пользователя, с которой каждый работник должен ознакомиться под подпись. Считаю, что данную проблему можно решить исключительно организационными мерами, такими как внедрение инструкций пользователей с определенными запретами и ограничениями.

Алексей Плешков

– DLP-решения действительно способны собирать весь объем проходящего через них трафика. При такой схеме работы объем свободного пространства, необходимого для хранения собранных DLP-данных, для средней организации исчисляется терабайтами в месяц. Ни одна организация, кроме известных медийных гигантов и иностранных спецслужб, не может позволить себе постоянно хранить такой объем данных и использовать его для решения собственных аналитических и поисковых задач. Поэтому в большинстве случае в DLP настраиваются четкие фильтры по событиям и трафику. Подпадающий под созданные критерии трафик сохраняется а архиве, а весь остальной перерабатывается и пропускается (не хранится). Таким образом, каждая конкретная организация, внедрившая DLP, может самостоятельно определять, как и какие пользовательские данные собирать, хранить и/или удалять, чтобы не нарушать действующие на территории РФ законы и подзаконные акты.

Константин Саматов

– Подобный сбор и хранение информации в архивах законны и допустимы. По сути, работодатель не определяет (не может определить), относится ли обрабатываемая в его информационных системах информация к личным данным сотрудников. Единственное условия законности данной обработки – это информирование работников о том, что обрабатываемая на автоматизированных рабочих местах информация подвергается контролю в целях безопасности, и получение от работников обязательства не использовать ресурсы работодателя в личных целях.

Анатолий Скородумов

– Закон не запрещает копировать информацию, закон запрещает нарушать неприкосновенность частной жизни работников. Если в сохраненных данных автоматизированными средствами осуществляется поиск информации, относящейся к деятельности компании, то ознакомления с личной перепиской сотрудника не происходит, соответственно никакие требования законодательства не нарушаются.

Не лишним будет ввести в организации запрет на использование автоматизированных средств и систем компании в личных целях, в том числе для переписки личного характера.

– Куда движется DLP отрасль? О чем вы хотели бы попросить разработчиков?

Елена Нагорная

– Ни для кого не секрет, что любую DLP-систему можно обойти, добавив документ с чувствительной информацией в архив, запаролив его. Ни одно DLP-решение не вскрывает запароленные архивы. Так вот, хотелось бы, чтобы система, имея перечень допустимых паролей, самостоятельно могла подобрать такой пароль и проверить на наличие информации ограниченного доступа. А в случае если ни один из паролей не подходит, блокировала бы пересылку таких сообщений.

Алексей Плешков

– Имея достаточно длительный опыт работы с DLP, хотел бы попросить DLP-вендоров более внимательно относиться к просьбам, замечаниям и предложениям по модернизации и развитию DLP, поступающим от служб эксплуатации заказчиков. Очень важно также минимизировать сроки выпуска критичных обновлений, как с точки зрения устранения вероятных уязвимостей, так и с позиции выпуска нового дополнительного функционала. Дискретность в полгода/год иногда бывает неприемлемой.

Константин Саматов

– Следуя общим тенденциям развития информационных систем, DLP-отрасль на сегодняшний момент движется в сторону развития аналитических инструментов, направленных на совершенствование политик безопасности для предотвращения утечек данных и эффективность поиска информации при расследовании инцидентов информационной безопасности.

Анатолий Скородумов

– Разработчиков DLP-систем я бы как раз и хотел спросить: куда движется DLP-отрасль? Я не вижу каких-то устойчивых трендов в отрасли в последние годы. Многие DLP "обросли" значительным функционалом, который впрямую не относится к защите от утечек данных. Есть попытки реализовать на базе DLP некие аналитические системы по выявлению внутренних мошенничеств. В то же время есть явное отставание DLP-систем от современных технологий. Мы у себя в организации только начинаем внедрять DLP в технологии VDI, хотя используем их (технологии VDI) уже более трех лет. Для нашей платформы виртуализации этот функционал только-только был реализован. Возникает резонный вопрос: стоит ли накручивать в DLP-системах несвойственный им функционал, если не в полном объеме реализована защита от утечек при использовании современных технологий обработки информации и обмена данными? ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru