Критерии выбора: что включает в себя эффективная DLP-система

Когда перед человеком стоит выбор той или иной технологии, каким бы подкованным он в данном вопросе ни был, он обращается к отзывам и рекомендациям коллег, работающих с похожими задачами. Чтобы облегчить вопрос выбора, редакция опросила производителей, интеграторов и заказчиков DLP-систем: на что они рекомендуют обратить внимание, какие нюансы остаются вне поля их зрения и, конечно, о планах по развитию продуктов и ожиданиях конечных потребителей.

Роман Ванерке, *технический директор, АО "ДиалогНаука"*
Сергей Вахонин, *директор по решениям DeviceLock, Inc. ("Смарт Лайн Инк")*
Дмитрий Кандыбович, *генеральный директор, StaffCop (ООО "Атом Безопасность")*
Петр Ляпин, *эксперт по информационной безопасности*
Алексей Парфентьев, *ведущий аналитик, "СёрчИнформ"*
Алексей Плешков, *эксперт по информационной безопасности*
Алексей Раевский, *генеральный директор Zecurion*
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), Банк "Санкт-Петербург"*

– Выбор DLP-системы, ее возможности и эффективность предотвращения утечек – на что вы как разработчик (интегратор) рекомендуете обратить внимание? Что считаете самым важным?

Роман Ванерке

– Мы как интеграторы рекомендуем сперва обратить внимание на границы проекта – другими словами, выполнить классификацию информации ограниченного доступа, проранжировать ее по степени важности, определить, в каких бизнес-процессах и как эта информация обрабатывается и хранится, и т.д. Без предварительной работы бессмысленно подходить к выбору системы защиты.

Если же исходить из того, что подобная работа уже проведена и вы понимаете, что и как нужно защищать, то и выбирать становится гораздо проще. Так, например, в этом случае вы знаете, по каким каналам, кому и в каком виде передается информация ограниченного доступа. Отсюда уже вытекают и требования к DLP-системе: какие каналы должны контролироваться (Web, почта, съемные устройства, IM, печать, сетевые диски и т.д.), какие способы идентификации конфиденциальных документов (ключевые слова, словари, цифровые отпечатки, машинное обучение и т.п.) необходимы.

Говоря о предотвращении, хочется отметить, что редко кто решается перейти с режима мониторинга на режим блокировки, т.к. всегда есть риск ошибок второго рода (когда мы легитимную операцию приняли за инцидент). Но если подойти к внедрению DLP-системы комплексно, выполнить обследование и понимать, что система требует ежедневной работы с ней, то можно переходить в проактивный режим. С другой стороны, в последнее время наблюдается обратная тенденция – отказ от режима блокировки. Это обусловлено тем, что затраты на поддержание системы в проактивном режиме существенно выше возможных потерь и куда эффективнее будет повысить качество мониторинга.

Сергей Вахонин

– Первый вопрос, на который заказчику стоит ответить перед выбором DLP-системы: для какой цели приобретается DLP-решение, какую ключевую задачу оно должно выполнять? Говоря проще, надо решить, требуется ли предотвращать утечки данных (да, это ключевая задача для DLP-систем, но далеко не все представленные на российском рынке продукты действительно решают эту задачу техническими способами) или достаточно пассивного наблюдения за перемещением информации наружу и расследования инцидентов по фактам состоявшихся утечек. Если требуется предотвращать утечки, то выбор DLP-систем будет весьма ограничен, а внимание стоит обратить на полноту и качество контроля над всеми каналами, интерфейсами и периферийными устройствами компьютера, а также возможности контентной фильтрации в режиме реального времени. Особенно это касается контроля сетевых коммуникаций, качество и полнота которого во многом определяются способностью DLP-решения перехватывать, прозрачно дешифровывать и фильтровать контент сетевых коммуникаций, защищенных стандартным SSL или проприетарным шифрованием. Функциональный арсенал DLP-системы, решающей задачу предотвращения утечки информации, должен включать в себя способность с равным успехом функционировать внутри корпоративной сети и вне ее, возможность не допустить утечку данных ограниченного доступа при том, что предоставляется доступ для передачи для неконфиденциальных данных (это реализуется за счет контентной фильтрации в режиме реального времени), и т.д.

Для пассивного наблюдения, в свою очередь, рынок предлагает довольно большой спектр продуктов в разных вариантах реализации и архитектуры. При этом стоит учесть, что DLP-системы, способные технически предотвращать утечку данных, также предоставляют инструменты событийного протоколирования, ведения архивов и расследования инцидентов.

Особо подчеркну, что технические инструменты предотвращения утечки основываются на механизмах селективной блокировки доступа к устройствам, портам и каналам сетевых коммуникаций, в противовес специфической для российского рынка ИБ концепции неотвратимости наказания за выявленную утечку данных (которая, безусловно, должна иметь место, но не подменять собой принципы технического предотвращения утечек данных). Наконец, важно, чтобы все сформулированные клиентом основные функциональные требования к DLP-решению были полностью поддержаны в выбранном продукте, доступном на рынке в уже реализованном виде, а не в перспективе или с оговорками.

Дмитрий Кандыбович

– Сейчас бизнес хочет получать не решение какой-то одной задачи, а комплексную ИТ-систему, которая включает в себя DLP-систему и решает ряд задач для разных направлений. Заказчик смотрит на три основные вещи: универсальность, цену и возможность кастомизации. Если построить систему мониторинга на коммерческой файловой системе, то добавляются расходы на приобретение лицензии и обновления, не считая требований к оборудованию. А если основывать систему на Open Source, то она будет иметь нулевую стоимость владения. Что касается DLP, то она должна быть доступной по цене и легкой по инфраструктуре внедрения, должна иметь потенциал для интеграции с такими системами, как SIEM, "ГосСОПКА" и пр.

Алексей Парфентьев

– Мы всегда стояли на том, что DLP – это инструмент, а не черный ящик, работающий сам по себе. И рынок, кажется, наконец согласился, что парадигма "Prevention = блокировка" не всегда оправданна. Ведь нарушение предваряет процесс, значит была идея, планирование, подготовка и только потом реализация. Выбирать технологию нужно, исходя из реальной задачи. Например, потоковая блокировка хороша для предотвращения случайных утечек, но бесполезна для выявления групп риска на ранних стадиях. Подход также не дает комплексного понимания причин и следствий. В то же время инструменты прогнозирования хорошо работают только при скрытом режиме, они не пресекают нарушение в момент совершения.

Алексей Раевский

– Все зависит от набора задач, которые планирует решать пользователь DLP. Для кого-то важным будет производительность системы, для кого-то – набор контролируемых каналов или удобная отчетность. Часто играет роль гибкость при внедрении и совместимость с различными компонентами инфраструктуры, например наличие собственного прокси-сервера, потому что не всегда есть возможность перестраивать архитектуру сети ради DLP-системы. В последнее время заказчики стали больше обращать внимание на наличие продвинутых возможностей, таких как поведенческий анализ пользователей (UBA) и аналитика с использованием технологий больших данных.

– Ключевая задача DLP-системы – предотвращение утечки техническими методами. Какие способы обхода DLP-систем могут использовать инсайдеры и как им противостоять?

Роман Ванерке

– В первую очередь стоит отметить, что традиционные DLP-системы – это прежде всего системы защиты от непреднамеренных утечек. По разным оценкам, общая доля непреднамеренных утечек составляет от 40 до 70%. Злоумышленник может использовать шифрование, различные скрытые каналы передачи данных (тот же DNS), свой телефон (фотографирование, видео, диктофон) или свою память. Очевидно, что защититься от последнего вряд ли возможно.

В последнее время производители добавляют функционал, позволяющий выявлять факты утечек по косвенным признакам – с помощью предустановленных индикаторов компрометации (например, передача файлов, зашифрованных неизвестным типом шифрования) или функционала UEBA. Решения класса UEBA могут существенно помочь в выявлении внутренних злоумышленников.

Сергей Вахонин

– Действительно, в мировой практике считается первичным именно решение задачи технической возможности предотвращения утечки, а не психологической, построенной на анализе журналов и расследовании инцидентов с последующим наказанием сотрудников. Соответственно, чем уже широта контроля потенциальных каналов утечки данных, тем шире возможности инсайдеров. Это означает, что 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. Псевдо-DLP-система может собрать множество событий и теневых копий в архиве, но это не предотвратит намеренную утечку, особенно учитывая, что для выявления инцидента постфактум потребуется некоторое время. Грамотный подход к защите данных от утечки заключается в нейтрализации наиболее опасных векторов угроз утечки информации – тех, которые исходят от обычных инсайдеров или связаны с их поведением, в сочетании с мониторингом прочих потенциальных каналов утечки инфор-

мации для снижения негативного влияния угроз. Кроме того, важным элементом противостояния злоумышленникам является надежность DLP-системы, которая в контексте DLP означает защищенность от вмешательства пользователя (и в особенности с правами локального администратора) в работу решения – т.е. защиту от преднамеренных или случайных действий пользователя, направленных на прекращение нормальной работы DLP-системы или изменение заданных службой ИБ политик контроля, а также отсутствие зависимости от типа и наличия сетевого подключения (а это, между прочим, самый простой способ обхода контроля сетецентричных DLP-систем).

Дмитрий Кандыбович

– Если человек один раз увидел, что его действия привели к блокировке контента, то в следующий раз он приложит максимум усилий, чтобы его не вычислили. Самое простое – отфотографировать информацию телефоном. При этом нужно понимать, имеем мы дело с профессионалом, который пришел в компанию с целью получить информацию, или с обыкновенным сотрудником. Если это сотрудник, которого подкупили либо который не имеет умысла, то он будет пользоваться теми каналами связи, которые под контролем, и 90% нарушений можно отследить таким образом. Если речь идет о профессионале, то он имеет возможность обойти технические средства. Есть способы обнаруживать таких людей на ранних стадиях, например с помощью анализа поведенческих паттернов.

Алексей Парфентьев

– По иронии, способ обхода инсайдеру подсказывает базовый инструмент DLP – блокировка. Она раскрывает факт наличия DLP и тем самым вынуждает пользователя искать другие способы слить данные. По принципу "один канал закрыт – пробую другой". То есть, по сути, система сама учит, как ее можно обойти. Что касается решения этой проблемы: показательно, что всего несколько из более чем 2 тыс. наших клиентов используют блокировку. Вместо того чтобы оставлять инсайдерам способ обойти систему, они оставляют каналы открытыми и тщательно отслеживают поведение пользователей. Это позволяет разоблачать мошеннические схемы на этапе планирования, видеть новые лазейки инсайдеров и совершенствовать систему безопасности в реальном времени.

Алексей Раевский

– Мы в свое время проводили исследование методов, с помощью которых можно обмануть DLP-систему. В их числе как довольно простые, доступные практически любому, например "склеивание" файлов, так и такие экзотические, как стеганография. Многие из этих способов DLP-система может выявить, и надо это уточнять и проверять в ходе переговоров с вендором и пилотного проекта. Но надо понимать, что стопроцентно предотвратить все утечки невозможно и, например, всегда остается дыра, которую очень любят приводить в пример DLP-скептики – фотографирование экрана компьютера на мобильный телефон. Однако делать вывод о бесполезности DLP-системы из этого неправильно, поскольку ее задача не ликвидировать риски утечки полностью, а уменьшить их до приемлемого уровня и сделать так, чтобы затраты на приобретение и эксплуатацию системы были бы значительно меньше, чем потенциальный ущерб от утечки.

– Многие российские DLP-вендоры делают акцент на инструментарии анализа событий и инцидентов при слабых возможностях недопущения утечки данных. В чем эффективность таких DLP-систем и какую реальную пользу они могут принести заказчикам?

Роман Ванерке

– Российские вендоры идут в правильном направлении. Изначально, позиционировав себя как средство архивации, они проигрывали, т.к. не обладали всеми возможностями зарубежных DLP-систем. Но в последнее время за счет использования решений Open Source, их возможностей по визуализации и обработке больших объемов данных, такие системы позволяют своим клиентам получить не только архив и инциденты, но и средство визуализации, анализа взаимосвязей и оценку величины риска по своим сотрудникам.

В итоге "наши" вендоры по сути комбинируют технологии DLP- и UEBA-систем.

Сергей Вахонин

– Любой инструмент в DLP-решениях, даже вспомогательный, с канонической точки зрения на DLP-системы приносит пользу, если в конечном итоге он направлен на противодействие утечкам данных. Значимость и эффективность инструментария анализа событий определяется широтой охвата инспектируемых системой каналов передачи данных (здесь следует иметь в виду полный спектр потенциальных каналов утечки информации – сохранение информации на съемные накопители, печать документов, использование интернет-сервисов и сетевых протоколов). Если в решении сделан акцент на Post-DLP-арсенал возможностей, вендор предлагает прежде всего огромный набор красивых и быстрых отчетов, графов, карточек и т.п., но при этом состав отчетов формируется только на основании данных пассивного перехвата некоторых почтовых сетевых протоколов да пары мессенджеров, – значимость такого инструментария в плане борьбы с утечками данных сводится к нулю, а вендор ищет возможности интеграции с другими DLP-решениями.

Дмитрий Кандыбович

– Только 10% заказчиков применяют в DLP блокировки. Для их использования нужен опыт и хороший регламент. Часто системы, настроенные на блокировки, дают ложные срабатывания. Блокировка не является фактом наказания. Для СБ этот факт скорее вреден, потому что это сигнал для нарушителя. Польза DLP-системы в том, что она оповестит СБ об инциденте, соберет исчерпывающий лот по всем действиям и можно будет проследить, кто еще втянут в инцидент, получить информацию более обширную, чем единичный сигнал. DLP-система контролирует только файлы, а система мониторинга – еще и метаданные, аудио, нажатие клавиш, посещения, взаимосвязи. При этом DLP может стоять на шлюзе и контролировать почту. Информацию надо пропускать, но широкий инструментарий работает лучше.

Алексей Парфентьев

– Большинство вендоров реализовали основные возможности блокировки, но проблемы остались. DLP блокируют подозрительные письма, но не могут распознать человека из группы риска, не могут вовремя разоблачить сговор, не дают комплексного понимания причин и следствий. К нам приходят компании и рассказывают: "Вот есть у меня нарушение из DLP по почте. Я вызываю человека и всегда слышу, мол, этого не делал, письмо вижу впервые. И мне нужно воссоздать нарушение по шагам, собрать доказательства".

Поэтому возможности расследования предельно важны, без них СБ не сможет закрыть целый ряд задач. DLP не инструмент борьбы с техническими угрозами, как антивирус или файрвол, а средство защиты от человеческого фактора, где первостепенно важен контекст.

Алексей Раевский

– Действительно, в последнее время получили распространение DLP-системы, которые имеют ограниченные возможности по предотвращению утечек. По отношению к ним даже использование термина DLP не очень корректно. Источник этой тенденции, на мой взгляд, лежит на стороне заказчика, который часто опасается, что в случае некорректной работы DLP-системы будет нарушено функционирование ИТ-служб. Например, заблокируется Интернет или не отправится важное письмо по электронной почте. Причиной таких сбоев может быть как не очень высокое качество некоторых DLP-систем, так и просчеты администратора DLP-системы при настройке правил и политик.

Мы тоже часто сталкивались с тем, что заказчик не торопится переключать DLP-систему в режим блокировки, ограничиваясь пассивным перехватом трафика и реагированием на утечки постфактум, после того как они уже произошли. Возможно, на начальном этапе внедрения системы, в первые несколько месяцев, когда правила и политики только настраиваются, это оправданно. Однако, приобретая DLP-систему, в которой возможности по блокировке слабы или отсутствуют полностью, заказчик поступает крайне недальновидно.

Так что сейчас нельзя делать акцент на чем-то одном, современное DLP-решение должно обеспечивать и блокировку подозрительных операций, и развитые возможности по анализу инцидентов.

– Какие функциональные возможности DLP-системы являются для вас определяющими при выборе? На что рекомендуете обратить внимание тем, кто еще выбирает?

Петр Ляпин

– Основной задачей DLP-систем является реализация автоматизированного контроля конечного множества информационных каналов (каналов утечки). Поэтому при выборе видится правильным рассматривать в первую очередь возможности системы по контролю тех каналов связи, которые используются в организации. Причем так, чтобы охват был если не полным, то максимальным, с компенсационными мерами в непокрытой части. Нюанс в том, что система (или система вкупе с компенсирующими мерами) должна покрывать все применимые каналы утечки, "лоскутный" метод здесь неприменим. Последующие факторы, которые следует учесть, – это доступные способы интеграции DLP с целевыми системами (снизить нагрузку на них до минимума), наличие подходящих заказчику сценариев использования, удобство интерфейсов и т.д.

Алексей Плешков

– Не самыми основными, но востребованными функциями для DLP в настоящее время являются: интегрируемость/совместимость с продуктами и решениями по сбору и автоматическому анализу собранных/поступающих в DLP данных, а также возможность по желанию заказчика гибко/настраиваемо переключаться из режима избирательного сбора данных в режим сбора данных в полном объеме и вытекающая из этого возможность выполнения анализа и тестирования работоспособности новых правил для DLP на ранее собранных архивах данных (ретроанализ). Все остальные функции стали уже типовыми для большинства решений, представленных на отечественном рынке DLP.

Константин Саматов

– Если речь идет именно о системе класса DLP, то одной из важных характеристик должна выступать возможность блокировки исходящего за периметр организации трафика. Тем, кто выбирает, рекомендую четко определить класс системы, который им нужен. Я имею в виду то, что системы класса DLP часто путают с системами класса UAM (User Activity Monitoring), обеспечивающими мониторинг активности пользователей, но не защиту от утечки информации вовне. Большинство существующих решений представляют собой комплексные системы, сочетающие в себе возможности обеих систем, однако если речь идет о необходимости предотвращения утечек, то обязательной функциональной возможностью должна быть блокировка трафика.

Анатолий Скородумов

– Наиболее важными для нас в DLP-системе являются охват системой максимально возможного спектра каналов утечки информации, возможность ее гибкой настройки в режиме предотвращения утечки данных, развитые возможности поиска по сохраненному архиву информации и наличие набора настроенных правил "из коробки". При выборе DLP-системы важно четко понимать ее место в комплексной защите данных в вашей организации от утечки, четко определить цели ее внедрения. В обязательном порядке стоит пропилотировать в организации то решение, которое вы выбрали.

– В последнее время повышается значимость принципов невмешательства в личную переписку и личную жизнь, появляются новые законы (такие как GDPR). Учитывают ли разработчики DLP-систем, что в потоке данных могут попадаться личные данные, а их сбор и хранение в архивах может быть незаконным и привести к юридическим последствиям?

Роман Ванерке

– Определенно система DLP обладает всеми возможностями по перехвату данных, в которых могут быть и личные данные сотрудников. С одной стороны, зачем использовать корпоративные ресурсы для своих целей (и многие работодатели пользуются этим, утверждая, что все, что обрабатывается в их сети, не может быть личным и, соответственно, не подпадает под действие закона). С другой стороны, даже если система обрабатывает личные данные, то это автоматизированная обработка, которая не запрещена. DLP-система обладает необходимым инструментарием по управлению доступом к накопленным данным, оповещению как офицеров ИБ, так и владельцев информации, а также и самих пользователей. Кроме этого, система должна выполнять обфускацию критичных данных.

Сергей Вахонин

– 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 должна быть предусмотрена техническая возможность обрабатывать только те персональные коммуникации, в которых выявлены конфиденциальные корпоративные данные, а также возможность собирать, обрабатывать и хранить только эту часть коммуникаций работника, исключив таким образом проблему сбора и хранения личных коммуникаций организацией. Это реализуется, если в полной мере использовать возможности контентной фильтрации, задать политики для детектирования только тех данных, которые непосредственно являются конфиденциальной корпоративной информацией, например содержат определенные службой ИБ признаки, теги, ключевые слова и выражения. При корректном задании правил контентной фильтрации в реальном времени (разумеется, при наличии такой функции в DLP-решении) служба ИБ может контролировать содержимое исходящих сообщений в чатах, почте и передаваемых файлах, особенно когда контент фильтруется в момент передачи непосредственно на хосте.

Дмитрий Кандыбович

– Практики применения европейского закона GDPR маловато. Согласно 152-ФЗ, вся информация, которая относится к персональным данным, и регламент ее использования описаны ФСТЭК. Компания имеет право контролировать информацию, касающуюся бизнеса. Но работников следует оповестить о том, что информация контролируется, и они должны подписать соответствующие документы. На крупном предприятии желательно ввести режим коммерческой тайны. Можно негласно собирать информацию, но с ней нельзя обратиться в суд. Оператор связи несет ответственность за сохранность передаваемых данных согласно ст. 138 УК. Мы даем инструмент с очень широким функционалом, а как его использовать – ответственность за это несет заказчик.

Алексей Парфентьев

– Мы учитываем Европейский регламент защиты данных и серьезно доработали свое решение под него. Во-первых, изолировали и дополнительно защитили хранение чувствительных пользовательских данных, сделали их аудит опциональным. К примеру, пароли для входа в личные кабинеты, клиент-банкинги и т.д. могут исключаться из теневого копирования либо храниться в особо защищенном виде и с отдельными настройками доступа даже для сотрудников ИБ.

Во-вторых, расширили возможности инструментов аудита персональных данных внутри корпоративной инфраструктуры, чем закрыли одну из ключевых задач GDPR. Заказчикам доступно углубленное детектирование персональных данных, даже если компания использует облачные сервисы СУБД, виртуализации или хранения.

Алексей Раевский

– Ввод в действие GDPR, наоборот, должен позитивно повлиять на рынок DLP в Европе. Раньше внедрение DLP-систем в европейских странах осложнялось как раз тем, что там общество традиционно очень ревностно относится к приватности и анализ переписки сотрудника, даже на работе, воспринимался в штыки профсоюзами и общественными организациями. С принятием GDPR использование DLP-систем легитимизируется, поскольку без них выполнение ряда требований этого закона невозможно. Как при этом будет решаться проблема приватности самих сотрудников, пока непонятно. Скорее всего, им придется не использовать для решения личных вопросов рабочий компьютер, как это принято в других странах.

– Как вы решаете проблему невмешательства в личную переписку своих сотрудников, используя DLP-системы со сплошным журналированием сетевого трафика?

Петр Ляпин

– Не касаясь вопросов противодействия терроризму, ответ на этот вопрос следует искать на границе конституционного и трудового права. С одной стороны находятся гарантированные Конституцией РФ права граждан на неприкосновенность частной жизни, тайну переписки, телефонных переговоров и иных сообщений, а с другой – дисциплина труда и трудовой распорядок, в частности те его положения, которые касаются предоставления работодателем работнику инструментов и ресурсов для исполнения последним трудовой функции. Иными словами, работник в соответствии с установленной трудовой дисциплиной вправе использовать переданные ему и принадлежащие работодателю средства (информационные системы) исключительно для выполнения трудовых функций, а работодатель вправе устанавливать режим использования таких средств и осуществлять необходимый контроль.

Алексей Плешков

– Вмешательство в личную жизнь происходит только в тех случаях, когда личная переписка и личные материалы обрабатываются на тех же устройствах / в тех же каналах, работа которых контролируется DLP-решениями. Если организационно разделить все "личное" и "рабочее", установить правила работы сотрудников с конфиденциальной информацией, для всех работников организации определить уровни допуска к конфиденту, каскадировать ответственность и предоставить гибкие возможности для выполнения бизнес-функций без проникновения в личное пространство сотрудника, то проблема решится сама собой. Проверенным и действенным посылом для реализации предложенной выше модели является формирование у работника четкого понимания существования рядом с ним в организации "большого брата": наличия технического и организационного контроля (в т.ч. с применением DLP) со стороны работодателя за использованием предоставленных работнику инструментов без проникновения в его личную жизнь.

Константин Саматов

– Данная проблема решается подготовкой и ознакомлением работников с организационно-распорядительной документацией, в которой отражается в том числе, что пользователям запрещается хранение личной информации на рабочих ресурсах, пользование личной почтой и иными сервисами, не относящимися к выполнению функциональных обязанностей; компания не является оператором связи и не гарантирует тайну связи; в целях обеспечения безопасности осуществляется контроль технических средств и информационных ресурсов компании, в том числе сетевого трафика.

Анатолий Скородумов

– Все сотрудники организации официально предупреждены о недопустимости использования банковских компьютеров, банковской электронной почты и банковского канала Интернет в личных целях. Но даже если в переписке сотрудника проскочит какая-то информация личного характера, ничего страшного. Система срабатывает по определенным правилам, которые позволяют выявлять во всем потоке именно ту информацию, разглашение которой может нанести ущерб организации. Аналогично поиски по архиву сохраненных данных осуществляются в части установления лиц, отправлявших конкретные банковские данные. Никто не сидит и "глазами" не читает обычную переписку сотрудников, на это не хватит никаких ресурсов. На личные мобильные устройства агенты DLP-системы не устанавливаются. Средствами MDM-системы на мобильном устройстве пользователя формируется среда, максимально препятствующая утечке банковской информации, к которой работник имеет доступ со своего мобильного устройства.

– Почему большинство российских DLP-систем практически не используются на Западе? Существует ли принципиальная разница между DLP-системами российских и зарубежных вендоров? Что влияет на продажи больше всего – функциональные возможности, геополитические аспекты, легальность использования?

Роман Ванерке

– Основная разница заключается в том, что российские вендоры изначально отставали от своих западных коллег по технологиям выявления утечек конфиденциальной информации (цифровые отпечатки, машинное обучение, интеграция со сторонними решениями) и компенсировали ее за счет применения DLP-системы как системы тотальной архивации. Архивация также упрощала внедрение системы, т.к. не требовала со стороны подразделения ИБ затрат на обследования, классификацию и т.п. Очевидно, что архивация несет в себе как преимущества, так и недостатки. К недостаткам можно отнести высокие требования к системе хранения данных, ограничения, накладываемые СУБД на объемы данных, и возможные юридические последствия из-за хранения всех данных.

Сергей Вахонин

– Прежде всего отмечу, что наш продукт был изначально ориентирован на весь мировой рынок в целом, свою популярность приобрел вначале именно на Западе и более трети клиентов компании – как раз организации Америки и Европы, при том что доля рынка СНГ для нашей компании также составляет менее половины общего объема продаж.

Что касается большинства остальных российских вендоров, полагаю, что причины их незначительного присутствия на Западе – это изначальная ориентация на освоение домашнего рынка, специфически "домашняя" техника продажи с использованием административного ресурса и, что самое важное, недостаточный уровень решения ключевой для DLP-систем задачи предотвращения утечек данных с преобладанием функционала пассивного наблюдения, анализа поведения пользователей, расследования инцидентов. Зарубежные DLP-продукты, как правило, фокусированы на предотвращение утечки данных. Наши разработчики сталкиваются на Западе с тем фактом, что рынок уже активно освоен ведущими вендорами, а идеология Post-DLP мало востребована. Зарубежные заказчики зачастую предпочитают простые, надежные и гарантирующие защиту от утечки решения, а не аналитические инструменты для копания в архивах, да еще и требующие при этом значительных затрат на внедрение и поддержку. Активное развитие вспомогательных для DLP функций при отсутствии возможности избирательного контроля и анализа содержимого передаваемых данных существенно снижает и возможность легального применения такого ограниченного DLP-решения в глазах западного потребителя, поскольку нарушаются принципы невмешательства в личную переписку и личную жизнь.

Дмитрий Кандыбович

– Есть ряд российских компаний, продукция которых продается на Западе и соответствует их стандартам. Западные законы жестче и ответственность выше, поэтому используется стандарт DLP, он более формализован. Контролируется только информация, ни в коем случае не метаданные или что-то еще. В западных компаниях более развита корпоративная культура, сотрудники более дисциплинированны. В России другой функционал, управление более слабое, масса нестандартных вариантов по поводу хищений, которые даже не связаны с информацией. У нас шире перечень задач и инструментарий и действительность суровее, и законы более расплывчаты. На продажи в России влияет административный ресурс, в мире – функциональные возможности.

Алексей Парфентьев

– Да, разница между продуктами есть, но очевидно в пользу отечественных: функционал наших DLP развит куда больше. Например, возможности КИБ для рынков Латинской Америки, ЮАР и Ближнего Востока стали новым подходом к ИБ: защищать не только информацию, но и бизнес от всех видов мошенничества. Это нужно организациям на всех континентах, так что концепция получила название Money Loss Prevention и вызвала большой интерес. Но в некоторых странах проблемой стало российское происхождение. Так что единственная сложность присутствия отечественных продуктов за рубежом – в политике. И мы убедились в этом: когда один из партнеров прикрыл нас "белым лейблом", продукт стал продаваться.

Алексей Раевский

– Российские ИБ- и ИТ-вендоры традиционно слабо продвигают себя на глобальном рынке. Обратных примеров буквально единицы, это исключения, которые лишь подтверждают правило. Тому есть несколько причин. Во-первых, если говорить о DLP-системах, то западные и российские DLP принципиально отличаются. Западные направлены в первую очередь на решение проблемы Compliance, т.е. соответствия требованиям законов и стандартов в области ИБ, поэтому их функционал довольно скромен, администрирование упрощено и эксплуатация системы возможна в полуавтоматическом режиме. Российские системы в большей степени ориентированы на задачи внутреннего контроля и защиты конфиденциальной информации, поэтому настройки в них более гибкие и сложные и они подразумевают постоянную работу с системой администратора безопасности или контролера. Но не на всех рынках такой расширенный функционал востребован, многих пользователей пугает сложность системы и необходимость содержать дополнительного сотрудника. Во-вторых, западные DLP предлагаются вендорами как компоненты более широкого, интегрированного решения, в которое входит антивирус, защита облачной инфраструктуры и многое другое. В-третьих, к российскому ПО всегда настороженно относились на Западе, а в последнее время, принимая во внимание известные политические события, ситуация еще сильнее ухудшилась.

Тем не менее я считаю, что работа российских вендоров на зарубежных рынках обязательна для того, чтобы оставаться в тонусе, не замыкаться в одном сегменте рынка и развивать продукты и технологии. Поэтому и наша компания, и многие другие российские производители сейчас активно начинают продвигаться за рубежом, и это надо всячески приветствовать.

– Импортозамещение в сегменте DLP-решений – оправданно ли, с точки зрения потребителя?

Петр Ляпин

– Импортозамещение оправданно всегда (или почти всегда), когда речь идет о неприемлемости рисков, связанных с факторами, выходящими за пределы юрисдикции РФ, такими как внешнеполитические события и зависимость от иностранных поставщиков. В качестве примера можно привести объекты критической инфраструктуры. Что касается субъектов малого и среднего бизнеса, то в подавляющем большинстве случаев объективная оценка рисков уже будет содержать в себе нужный ответ.

Алексей Плешков

– Сам по себе термин "импортозамещение" является сложно применимым к ИТ-решениям, поскольку при детальном рассмотрении степень замещения (полная или частичная) является поводом для дальнейшего экспертного обсуждения и споров. Тем не менее в контексте DLP замещение импорта, скорее, решение конкретного заказчика, чем вынужденная мера. Отечественные DLP-решения по праву являются одними из самых конкурентоспособных на российском и мировом рынке, не только благодаря привлекательной ценовой политике, но и в силу объективно высокого качества реализации отдельных функций и опережающих западные аналоги темпов внедрения в промышленную эксплуатацию новых фишек, возможностей и инструментов, в т.ч. составленных на базе анализа потребностей заказчиков.

Константин Саматов

– С точки зрения потребителей, первичным должен быть не производитель, а функционал DLP-системы и возможность ее интеграции в существующую инфраструктуру. По крайней мере, я бы рекомендовал именно на это обращать внимание. Кроме того, большинство исследований, проводимых разными компаниями и опубликованных в общедоступных источниках, свидетельствует о том, что российские аналоги не уступают зарубежным, а по опыту автора – пожалуй, даже превосходят их.

Анатолий Скородумов

– Российские DLP-решения всегда были конкурентоспособны. В части формирования общего архива исходящей информации и поиска по этому архиву российские решения всегда были и остаются более функциональными, чем зарубежные. Другое дело, что полноценное внедрение DLP-системы – процесс довольно длительный и трудоемкий. Лицензии на DLP-систему в крупной организации – это серьезные инвестиции. Поэтому для принятия решения о замене уже работающей зарубежной DLP-системы на российскую нужны весомые основания.

– Какие новые функциональные возможности вы добавили в свое DLP-решение в прошлом году?

Роман Ванерке

– Не могу говорить обо всех решениях, но западные решения идут в облака (поддержка Office 365), ведется внедрение контролей облачных сервисов и интеграция с решениями класса CASB.

Сергей Вахонин

– За год, прошедший с момента последнего обзора, мы выпустили несколько обновлений предыдущей версии и в июне 2018 г. в свет вышла новая версия DeviceLock DLP Suite 8.3. Подчеркну, что обновления текущих версий в продукте DeviceLock DLP – это не только

оптимизация и устранение выявленных проблем, но и добавление новых функций. Так, в течение года с момента выпуска версии 8.2 и до июня 2018 г. в нашем комплексе появился интерактивный граф связей, реализован контроль мессенджеров Viber, Telegram и WhatsApp, добавлена поддержка ряда сервисов Web-почты, социальных сетей и файлообменных сервисов, в комплект поставки включались новые словари и шаблоны регулярных выражений и многое другое. Новейшая версия DeviceLock DLP Suite 8.3 получила новый механизм контроля протокола SMB с возможностью контентной фильтрации исходящих файлов, поддержку меток классификатора Boldon James и давно ожидаемую нашими клиентами технологию детектирования данных по цифровым отпечаткам (фингерпринтам). Предмет особой гордости наших разработчиков – тот факт, что анализ по цифровым отпечаткам, как и другие технологии контентной фильтрации, реализованные в DeviceLock DLP, применяются для предотвращения утечек данных, обеспечивая инспекцию содержимого передаваемых, печатаемых и сохраняемых на внешние носители данных в режиме реального времени.

Дмитрий Кандыбович

– Удаленный рабочий стол, видеозапись рабочего стола. Контроль и полная блокировка USB-устройств по классам устройств, возможность ограничения записи на USB- и CD-носители. Анализ содержимого и обнаружение зашифрованных архивов. Добавлена функция OCR – оптического распознавания символов на изображениях. Фиксирование фактов и продолжительности звонков с помощью IP-телефонии. Инвентаризация установленного оборудования и программного обеспечения на компьютерах сотрудников.

Разработан функционал мониторинга действий сотрудников на GNU-/Linux-системах (в т.ч. российских системах специального назначения Astra Linux, Rosa и т.п.): отслеживание активности сотрудников, файловый мониторинг, мониторинг посещения сайтов, перехват печати, контроль командной строки в терминальном режиме, контроль логов, запись с микрофонов.

Автоматический детектор аномалий – функция распознает неестественное поведение пользователей и возможные утечки данных. Имеет настройки чувствительности.

Значительно доработаны статистические отчеты – они стали интерактивными, практически все отчеты используют технику Drill Down для быстрого перехода от общего к частному и расследований по цепочке. Появились новые отчеты – карточки измерений, они представляют собой агрегированную информацию по измерениям: пользователь, компьютер, файл, Web-сайт и т.п.

Интеграция с СУБД ClickHouse, которая позволяет в десятки раз увеличить скорость обработки данных при больших объемах данных.

Алексей Парфентьев

– За последний год выпустили консоль аналитика (она объединила SearchInform Client и ReportCenter), активно занимаемся разработкой Web-интерфейса, интегрировали КИБ со СКУД, ускорили работу системы, добавили поддержку Telegram, WhatsApp, контроль Web-камеры, усовершенствовали блокировки и технологии анализа аудиоканалов. И, конечно, нашим прорывом стал ProfileCenter – собственная разработка, позволяющая ИБ-специалистам профилировать пользователей и держать под контролем человеческий фактор.

Алексей Раевский

– За последний год Zecurion DLP кардинально обновился. Можно сказать, что вышла не просто новая версия системы, а новое ее поколение. Во-первых, все модули теперь полностью интегрированы, их объединяют общие политики, общая консоль управления, единые отчеты и аналитика и т.д. В настоящее время многие DLP-решения не могут этим похвастаться. Во-вторых, серьезно переработан интерфейс системы, теперь она управляется через Web-консоль, добавлены элементы документооборота (Workflow) событий и инцидентов. В-третьих, появился собственный модуль поведенческого анализа пользователей (UBA), который выводит систему Zecurion DLP на новый уровень и ставит ее в один ряд с продуктами мировых лидеров. Наконец, для снижения зависимости от проприетарного ПО и платформ мы реализовали поддержку СУБД PostgreSQL из реестра российского программного обеспечения и сейчас готовим версию DLP-агента для нескольких дистрибутивов Linux.

– Чего вы ожидаете в будущем от DLP-решений? Чего не хватает DLP-системам российских разработчиков?

Петр Ляпин

– Не является секретом то, что среди сильнейших игроков на мировом рынке DLP-решений уже давно присутствуют российские разработчики. Технические возможности систем на текущем этапе идут в ногу со временем и соответствуют развитию контролируемой ими инфраструктуры. Практика использования ряда решений говорит о том, что сбор и фиксация первичных данных реализованы в достаточной мере практически во всех решениях, а вот функции управления нуждаются в определенном развитии. Среди текущих направлений – такие, как направленность на реализацию и автоматизацию реальных сценариев работы с событиями, их данными и интерфейсами, что моментально сделает работу с системой более удобной и, соответственно, эффективной. В перспективе видится целесообразным изучить возможности выявления связей между событиями, применения искусственного интеллекта и других доступных технологий.

Алексей Плешков

– Одним из наиболее востребованных сейчас инструментов на рынке DLP являются мобильные DLP-агенты, совместимые с флагманскими версиями программного обеспечения ведущих производителей мобильных телефонов/планшетов/ноутбуков. Недостаточно разработать клиентское приложение, совместимое с текущей версией операционной системы на целевом телефоне, необходимо продумать жизненный цикл этого DLP-агента так, чтобы он позволял адекватно реагировать на инциденты, связанные с актуальными угрозами конфиденциальности информации, хранимой и обрабатываемой вне традиционного периметра безопасности. Теряет свою актуальность "заплаточный подход". Сегодня применять только MDM-решения и контейнеризацию в статическом исполнении уже неэффективно. Бизнес-пользователи требуют от информационной безопасности новые, более гибкие, но не менее защищенные продукты и решения, одним из которых является DLP.

Константин Саматов

– В настоящий момент большинство DLP-систем поддерживает работу агентской части, осуществляющей сбор информации и контроль каналов коммуникации на уровне хоста, только с операционными системами MS Windows. При этом все большее количество организаций переходит на операционные системы семейства Linux. Кроме того, в современных условиях мобильности рабочих процессов большое значение приобретает использование DLP-систем для контроля утечек информации с корпоративных мобильных устройств, работающих на мобильных операционных системах (iOS, Android и SailFish). Прогнозирую, что большинство производителей DLP в ближайшем будущем будет уделять внимание возможности использования своих решений на Unix-платформах.

Анатолий Скородумов

– На наш взгляд, современным DLP-системам не хватает следующих вещей:

- глубокого понимания структуры организации с возможностью построения правил обработки информации на основе этих данных;
- возможностей по выявлению аномалий поведения пользователей;
- отсутствие ИТ-зрелости, прежде всего в части надежности работы, отказоустойчивости, масштабируемости, управляемости.

Еще одна проблема DLP-систем – это хроническое отставание от современных ИТ-технологий. Есть существенное запоздание между появлением новых ИТ-технологий и их охватом системами DLP.

– Чего ждать от разработчиков DLP-систем в обозримом будущем, куда движется отрасль?

Роман Ванерке

– Я выделяю два основных направления развития DLP-систем: все большая интеграция с различными облачными решениями и появление технологий выявления аномалий (UEBA). Очевидно, что не всегда есть возможность описать конфиденциальные данные заранее, и в этих случаях на помощь придут технологии UEBA. Например, использование агента на рабочей станции как сенсора, который обеспечит сбор необходимых данных для построения профиля поведения и выявление аномалий, когда сотрудник неожиданно стал копировать много различных документов, пытаться получить доступ к сетевым папкам, куда ранее доступ не запрашивал, и т.д.

Сергей Вахонин

– Отрасль движется разнонаправленно, кто-то развивает свои продукты, стараясь обеспечить широту и качество контроля каналов передачи данных, кто-то акцентируется на поведенческом анализе и расследовании инцидентов… Однако, будучи убежденным сторонником концепции предотвращения утечек данных, не могу не отметить отрадную тенденцию появления в последние пару лет в ряде самых раскрученных на российском рынке DLP-систем функции блокировки доступа к USB-устройствам, принтерам и базовым почтовым протоколам.

В стратегическом плане перспективы развития DLP-систем следует ожидать повышения уровня соответствия актуальным угрозам и рискам, дальнейшего усложнения аналитических инструментов вплоть до сращивания DLP с другими средствами инфобезопасности или их прозрачной интеграции.

Дмитрий Кандыбович

– На первый план выходит честный функционал, который у всех систем сейчас примерно однотипный. Лидеры рынка обновляют свои решения, добавляют Web-интерфейсы. И, конечно, важна цена. Кроме того, обращают внимание на нижнюю часть айсберга: какое оборудование устанавливать, какова стоимость владения, какой будет результат и насколько система универсальна. Она сразу же должна иметь возможность интеграции в информационную инфраструктуру заказчика, а также интегрироваться с другими системами. Преимущество отдается простым, коротким проектам с быстрой отдачей. Нужно взять коробочное решение, и чтобы оно сразу же заработало. Проект должен в разумные сроки решить поставленные задачи.

Алексей Парфентьев

– Если говорить в общем – очевидна тенденция к расширению применения DLP под смежные задачи. Например, контроль эффективности пользователей, проведение расследований, PAM-/PUM-контроль, шифрование носителей, анализ аудиоканалов, eDiscovery. Все ключевые игроки так или иначе уже встали на эти рельсы: кто-то дорабатывает свои решения сам, кто-то заключает партнерские соглашения с узкоспециализированными вендорами.

Если говорить о развитии именно инструментария DLP – решения становятся умнее, появляется сложный статистический анализ, элементы машинного обучения, распознавание речи в текст. В фокусе вендоров также UEBA-технологии. Но мы пошли иным путем и стали автоматизировать профайлинг, поскольку считаем, что релевантную картину вероятных угроз скорее покажет работа с психологией инсайдера, нежели техническая статистика.

Алексей Раевский

– Я бы выделил здесь две тенденции. Первая – это дальнейшее встраивание технологий анализа больших данных и искусственного интеллекта в DLP. DLP-архив содержит огромный объем информации, и получение новых знаний из этого архива – вопрос времени и развития технологий. Вторая тенденция – это более полный контроль операций с облачными хранилищами. Сейчас происходит процесс размывания традиционного периметра сети организаций, многие операции переносятся в облако. И это будет фактором риска до тех пор, пока DLP-системы не научатся контролировать эти операции и эффективно предотвращать утечки независимо от того, где хранится и обрабатывается информация.