ИИ как предсказатель утечек данных

Валерий Естехин, *эксперт по вопросам информационной безопасности, автор блога estekhin.blogspot.ru*

Личный опыт использования какой-либо технологии всегда имеет большее значение, чем любой маркетинг. Опыт работы с DLP-решениями (Data Leak Prevention) влияет на знание деталей применения, а осмысление этого опыта подталкивает иногда к довольно острым умозаключениям.

Прогресс цивилизации заключается в увеличении количества важных действий, которые мы выполняем не думая.

Альфред Норт Уайтхед

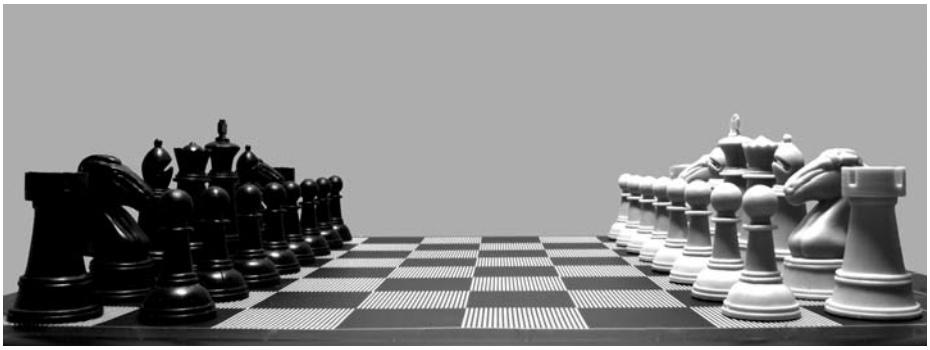
Участники:
Максим Ксенофонтов, *ведущий инженер Департамента информационной безопасности АМТ-ГРУП*
Дмитрий Кандыбович, *генеральный директор StaffCop (ООО "Атом Безопасность")*
Анна Попова, *руководитель блока DLP, Infosecurity a Softline company*
Галина Рябова, *руководитель направления Solar Dozor компании "Ростелеком-Солар"*
Алексей Дрозд, *начальник отдела информационной безопасности "СёрчИнформ"*
Александр Клевцов, *руководитель направления InfoWatch Traffic Monitor*
Андрей Арефьев, *директор по инновационным проектам ГК InfoWatch*
Мария Воронова, *директор по консалтингу ГК InfoWatch*
Дарья Орешкина, *директор по развитию бизнеса, Web Control*
Владимир Ульянов, *руководитель аналитического центра Zecurion*

Когда покупаешь DLP-решение, чувствуешь свою важность

Обычно DLP-система позиционируется как решение для защиты от утечек данных и противодействия инсайдерам. DLP – недешевое удовольствие. Такое решение при расчете на количество охваченных системой пользователей в диапазоне 1500–2000 человек в докризисные времена могло стоить 10–12 млн руб. Поэтому, когда руководство согласовывает бюджет на DLP, безопасник чувствует себя весьма значимым лицом в компании, участвующим в принятии важных решений.

На профильных конференциях нередки высказывания о том, что половина затрат на обеспечение информационной безопасности неэффективна. DLP-решения, как мне кажется, являются подходящей иллюстрацией. Проблемы эксплуатации DLP-систем кроются не столько в технических аспектах работы, сколько в непонимании на начальном этапе эксплуатации сложности внедрения применяемых технологий и, как следствие, в завышенных ожиданиях пользователей таких систем. У меня отношение к DLP такое же, как к офисным пакетам: большинство потребителей использует только, условно говоря, 10% возможностей подобного ПО.

Что характерно, базовые вещи в DLP-системе, такие как контроль почты, контроль съемных носителей, поиск по ключевым словам, регулярные выражения, а также нелюбимые всеми DLP-агенты работают нормально. Но детали применения DLP обычно меняют картину до неузнаваемости.



Тонкости, о которых знают только профессионалы

Даже если вы приобрели решение, вобравшее, как вам кажется, в себя все лучшее, что на данный момент представлено на рынке, не факт, что оно идеально впишется в вашу ИТ-инфраструктуру:

- если система собирает всю возможную информацию, то она будет требовательной к вычислительным ресурсам;
- если система с высокой точностью определяет факт утечки, то она требует детального описания ваших активов и правил контроля за ними;
- если система может прерывать высокорисковые процессы, то она и сама создает дополнительные риски для бизнеса.

После развертывания системы в полном объеме вдруг всплывают вопросы недостатка вычислительных ресурсов, места для хранения архивов, недостаточной скорости передачи данных по сети. Как следствие, чем больше аналитиков подключаются напрямую к серверу обработки данных, тем медленнее работает система, перегружаясь событиями.

Комментарии экспертов

Дарья Орешкина: Подвох кроется в краткости определения DLP: можно подумать, что это рубильник для выключения утечек, но это не так. Система дает возможности отслеживания взаимодействия людей как внутри компании, так и с внешними контрагентами, и именно с помощью этой ценности можно попытаться обнаруживать или даже предотвращать утечки. DLP может автоматизировать задачи сбора и базового анализа информации, но покупатель должен хорошо представлять, что именно нужно автоматизировать и как использовать результаты.

Максим Ксенофонтов: Зачастую DLP-система действительно покупается по принципу "чтобы не хуже, чем у других", особенно когда на это есть бюджет и возможность убедить руководство в необходимости таких затрат. Но есть и другой подход: когда специалисты по информационной безопасности проводят технический и процессный аудит ИБ в компании, разрабатывают модель угроз и модель нарушителя, формируют адаптированный перечень мероприятий для защиты от выявленных угроз. И уже только тогда понимают, есть ли среди этих мероприятий установка DLP и какие модули необходимы. И цена в расчете на пользователя в таком случае получается намного меньше, чем если покупать весь набор лицензий без предварительного анализа.

Александр Клевцов: Такие вопросы снимаются за счет подготовки к внедрению. Вендор на этапе пилота проводит расчет вычислительных мощностей, объемов хранения, сроков, объемов трафика, количества контролируемых сотрудников, заранее снимает риск неправильного выбора железа. DLP не внедряется за один день, хотя некоторые пытаются.

Галина Рябова: В 2019 г. мы проводили исследование основных причин разочарований заказчиков в DLP-системах. По итогам опроса одна половина заказчиков ответила, что современные системы защиты от утечек перегружены различной функциональностью, а другая – что они, наоборот, имеют недостаточный функционал. Такая ситуация возникает потому, что на рынке нет единой концепции применения DLP-систем, какие задачи и как они должны решать. Сфера деятельности закрытая: применяя DLP для решения задач безопасности, заказчик, как правило, не делится своим опытом с вендором и отраслью, поэтому не вырабатываются best practices. В итоге заказчики не осознают в полной мере все возможности этих решений и используют лишь малую часть доступного функционала.

Владимир Ульянов: Действительно, выбор DLP-системы, особенно для компаний, где свыше тысячи рабочих мест, – процесс нетривиальный. Если смотреть только маркетинговые материалы разработчиков, скорее всего вам захочется купить все – так они хороши. В этом случае поможет независимая внешняя оценка.

Анна Попова: Зачастую, принимая решение о покупке DLP-системы, мы не задумываемся о том, к чему нас это обязывает, какие мы должны выполнить требования при этом и как будет организована трудовая деятельность аналитиков и инженеров при работе с системой. Поэтому так важно при подборе DLP-системы, ее тестировании составлять чек-лист, по которому возможно будет сформировать грамотное и реально работающее ТЗ на систему.

Алексей Дрозд: Самый простой способ рассчитать нагрузку на ИТ-инфраструктуру – ставить на тест DLP в "максимальной комплектации" на как можно большем количестве машин. Поэтому на время пилота мы не ограничиваем число бесплатных лицензий. Если нужно контролировать больше, чем позволяет инфраструктура клиента, можно ввести распределенную систему обработки перехвата или развернуть КИБ в облаке.

Дмитрий Кандыбович: Наше решение очень легко устанавливается, очень легко масштабируется под размеры рабочего парка, поэтому проблем с перегрузками у нас не возникает. Касательно вопроса работы с активами – на мой взгляд, при правильно организованном, логичном контроле за работой ответственных лиц эта проблема не проявляет себя. А если еще и имеются мощные средства анализа, то эта проблема перестает быть актуальной в принципе. Главное – это правильный подход к проработке DLP-системы, начиная от общего принципа и заканчивая набором инструментов, предлагаемых системой.

Функциональность "из коробки" и кастомизация

В процессе эксплуатации DLP приходит понимание, что результативность работы системы сильно зависит от грамотной настройки автоматизации поисковых алгоритмов. Как следствие, установив систему "из коробки", что-то обнаружить можно только при очень большом трудолюбии или совсем явном нарушении со стороны сотрудников. У безопасников сразу возникает масса дополнительной ручной работы по анализу данных. А значит, неминуемо встает вопрос доукомплектации штата для работы с DLP-системой – нужны грамотные аналитики..

Мало кто в компании обладает видением всего бизнес-ландшафта, каждый занимается лишь своим участком работ, поэтому потребуется сформировать общий перечень категорий информации. И это, как правило, становится самостоятельным проектом по защите данных, который не вызовет энтузиазма ни у кого в компании, кроме, может быть, вас. Это проявится в полной мере, когда потребуется прийти с неудобными вопросами в бизнес-подразделения, отнимая их внимание и время на зарабатывание денег для организации.

Комментарии экспертов

Алексей Дрозд: DLP, которая дает 100%-ный результат "из коробки" – утопия. Даже с огромным набором предустановленных правил контроля (у нас, например, таких больше 300) система требует донастройки под конкретную компанию. Чтобы упростить эту задачу для клиента, у нас работает отдел внедрения.

Анна Попова: Кастомизация работы DLP-системы, тюнинг ее политик и настроек – это, пожалуй, базовая вещь, без выделения ресурса на которую нет смысла в приобретении ПО.

Александр Клевцов: Для крупных организаций DLP-системы по определению не могут быть коробочными, мы давно это говорим. Для упрощения жизни клиента у нас есть консалтинг, делающий внедрение безболезненным. Одновременно делаем упор на развитие технологий анализа: чем умнее технологии, тем меньше ручной работы.

Максим Ксенофонтов: В целом это базовая задача для любого департамента ИБ: знать защищаемые информационные активы, их свойства (категории, содержание и пр.), места хранения, владельцев и модель доступа к ним. И если

ранее такая "инвентаризация" не была сделана, то действительно приходится сначала проводить базовое обследование для определения защищаемых активов.

Дмитрий Кандыбович: Использование системы ложится на офицеров ИБ, без этого никак, любая система может только предупреждать и ограничивать в простейших операциях. Проводить расследование – обязанность человека.

Галина Рябова: Одной из задач, которые мы ставили при разработке DLP, была автоматизация рутинных сценариев работы офицера безопасности. В этой части DLP-системы не должны требовать заметной кастомизации. Гораздо важнее наличие методик решения стандартных задач. Что действительно требует настроек – это политика фильтрации, потому что в каждой компании свои информационные активы, которые нужно защищать, и форматы их представления, а ложноположительные срабатывания, подобно спаму, съедают время безопасников.

Дарья Орешкина: Ключевой вопрос при внедрении DLP – заинтересован ли бизнес в контроле коммуникаций. Если да, то необходимый импульс можно будет сформировать и передать по иерархической цепочке управлений и департаментов. Любого сотрудника, даже самого ответственного и дружелюбного, нужно мотивировать на выполнение той или иной задачи.

Владимир Ульянов: По нашему многолетнему опыту, даже сами сотрудники бизнес-подразделений не всегда знают точно, где какая информация хранится. Поэтому большую помощь окажут инструменты класса Discovery, которые входят в состав Enterprise DLP. Эти программы в автоматизированном режиме сканируют корпоративные ресурсы, классифицируют данные и находят все места хранения конфиденциальной информации.

Выбрали DLP с охватом всех возможных каналов утечки?

В поисках ответа потребуется определить реальные каналы утечки информации, обычно это является частью аудита информационной безопасности в компании. Если обнаруженные потенциально опасные каналы не решаются DLP-комплексом, приходится подключать дополнительные технические меры защиты. Возможно, DLP поможет предотвратить утечку, но система не может заменить все современные инструменты защиты данных.

Производители часто заявляют, что настроили простой и понятный процесс наладки DLP, который не потребует регулярных консультаций у технических специалистов. Но в реальности помощь вендора понадобится как в начале работы, так и в процессе последующей эксплуатации системы; по моему опыту, частота таких подключений – примерно раз в квартал. За каждый дополнительный запрос с вашей стороны производитель, скорее всего, выставит солидный счет на доработку.

Комментарии экспертов

Максим Ксенофонтов: DLP может не покрывать все возможные каналы утечки информации, например ПЭМИН, лазерную разведку или DNS Exfiltration. Соответственно, для тех угроз, которые не закрываются DLP, необходимо реализовывать другие мероприятия для защиты информации.

Владимир Ульянов: Именно здесь и выявляются расхождения между заявлениями разработчика и реальной эксплуатацией. Хороший вариант – попробовать DLP на пилотном проекте. Это позволит оценить реальные возможности системы и удобство ее использования, а не только красочность маркетинговых брошюр или талант менеджера по продажам.

Дарья Орешкина: Доработка и донастройка требуют определенных ресурсов. Но раз люди начинают использовать новые технологии и решения, значит они удобнее прежних и дают дополнительные преимущества. Безопасность ни в коем случае не должна препятствовать развитию.

Галина Рябова: Да, DLP-система требует квалифицированного внедрения и технического сопровождения. Но как у хорошего сисадмина мало работы, так у хорошо внедренной DLP-системы мало проблем. Поэтому, конечно, имеет смысл обращаться к вендору, ведь у него самая глубокая экспертиза по своему продукту.

Анна Попова: На практике это часто работает так: ты завел тикет в службу техподдержки вендора и ждешь. Иногда долго. Затем начинается процесс "борьбы" с вендором за выяснение обстоятельств сбоя или ошибки системы, который может ничем не закончиться.

Алексей Дрозд: Часто дело не в недостатке функционала DLP, а в том, что у клиента до нужных функций "не доходят руки". Чтобы таких ситуаций не возникало, мы бесплатно обучаем работе с системой. Мы остаемся на связи с заказчиками, потому что живой фидбэк – основа для развития продукта и релиза новых.

Андрей Арефьев: Со временем задачи эволюционируют. На начальном этапе ИБ хочет знать, что происходит, и закрыть очевидные проблемы. По мере роста зрелости процессов защиты информации возникают новые задачи, это нормально. Платить за доработки придется, если система незрелая.

Дмитрий Кандыбович: Поэтому наше решение не является только DLP-системой, а включает в себя множественный функционал, стоящий на трех основных китах – мониторинге, аналитике и блокировке. Мы делаем хорошо свою работу, поэтому неважно, как свою работу делает клиент, наше решение сработает в любом случае.

Правовые основания для поиска злодеев

Любая организация, установив DLP-систему, начинает всматриваться в свои ряды в поисках злодеев. Негодяи, как правило, находятся. Чтобы с ними "расправиться", требуется тщательная подготовка правовой стороны применения DLP-систем в организации. Необходимо публично определить границы личного и производственного, зафиксировать это в документах и ознакомить сотрудников.

А для этого задача предотвращения утечек информации должна быть зафиксирована вашей организацией по результатам оценки рисков. Должно быть также принято решение о проведении деятельности по предотвращению утечек информации конфиденциального характера (о требованиях и рекомендациях по предотвращению утечек информации в кредитных организациях можно узнать из нормативных документов: ГОСТ Р 57580.1–2017; РС БР ИББС-2.9–2016).

Комментарии экспертов

Дмитрий Кандыбович: В любой компании, которая озабочена своей ИБ не для галочки, а для реальной защиты бизнес-процессов, а по факту – денег, все это должно быть проработано. Где деньги, там обязательно поблизости крутятся злоумышленники, а для борьбы с ними юридическая основа обязательно должна быть готова. Нельзя стрелять из пушки, не купив порох.

Максим Ксенофонтов: Кроме того, некоторые DLP позволяют не читать всю переписку пользователя, а обращать внимание только на предположительные нарушения, расследование которых является вполне законным мероприятием. А сам же анализ переписки происходит машинным способом, что не нарушает тайну переписки.

Анна Попова: Юридические аспекты нужно обсуждать и решать еще до внедрения или при внедрении системы, а не на этапе ввода ее в боевой режим. В противном случае ваша работа, и особенно результаты ваших внутренних расследований с использованием данных, полученных благодаря DLP-системе, могут пойти прахом.

Галина Рябова: Для своих заказчиков мы разработали набор рекомендаций, как легализовать DLP в компании. Однако на практике в России больше половины компаний устанавливают системы защиты от утечек, не уведомляя об этом сотрудников. Соответственно, и большинство инцидентов, связанных с утечкой конфиденциальной информации, решаются вне правового поля.

Алексей Дрозд: DLP можно и нужно пользоваться легально, для этого никаких препятствий нет. "Легализация" DLP необходима как минимум для выполнения требований закона (от ФЗ-152 до норм Конституции).

Мария Воронова: Систему нужно настроить и обеспечить ее правомерность, чтобы все фиксируемое DLP априори являлось доказательной базой. Для этого нужно закрепить принципы легитимной обработки конфиденциальной информации, установить правовые основы для мониторинга и контроля инфопотоков, обеспечить возможности для расследования инцидентов, сбора доказательств и принятия решений о взыскании, увольнении, обращения в правоохранительные органы и т.д.

Дарья Орешкина: Зачастую нарушения происходят неумышленно. Тогда DLP помогает предотвратить случайные инциденты. Также замечено, что сотрудники обычно не хотят ввязываться в активности, о которых система проинформирует как о нежелательных. В этом случае DLP с функциями real-time-оповещения пользователей выступает в роли обучающей системы по корпоративным нормам информационной безопасности.

Владимир Ульянов: Очевидно, что права сотрудника не должны нарушаться, но никаких нарушений в контроле организацией своей коммерческой тайны нет. Сложнее бывает соблюсти баланс интересов работника и работодателя, сделать так, чтобы сотруднику было комфортно в офисе, не чувствовать себя зверьком, действия которого рассматриваются под лупой.

Еще несколько нюансов

Приведу еще несколько наблюдений о DLP из личного опыта двухлетней давности. Возможно, что-то из приведенного ниже списка уже неактуально.

1. Пользователю системы приходится администрировать большую часть компонентов системы из разных консолей – это неудобно.

2. Ненормально, что не предусмотрена защита от удаления DLP-агента, который обнаруживается на компьютере продвинутым пользователем с обычными правами.

3. Как показывает практика, цифровые отпечатки полноценно работают только применительно к текстовым документам.

4. Пользователю системы, как правило, недостаточно предустановленных правил контроля и словарей с экземплярами защищаемых данных.

5. В большинстве DLP отсутствует машинное обучение.

6. Существует мало реальных интеграций DLP с существующими на рынке SIEM-системами.

Комментарии экспертов

Максим Ксенофонтов: Если обобщить, то подобные проблемы сводятся к двум типам: функциональности нет, так как она слабо востребована или новая (например, машинное обучение), или что-то не настроено в конкретной инсталляции (например, интеграция с SIEM). Первый тип проблем решается с помощью запросов на улучшение (RFE) разработчику, а второй – хорошим интегратором и грамотным заданием на работы.

Дмитрий Кандыбович: Staffcop Enterprise не только отслеживает что именно сотрудник делает на компьютере, но и ограничивает в запуске приложений, потенциально опасного софта, веб-сайтов, внешних носителей и т.д. Это искореняет проблему атак на локальный агент. Важно не только оснастить систему функционалом и упростить внедрение, но и сделать так, чтобы пользователь просто пользовался (как в Apple). Одной из наших целей было сокращение времени настройки, чего мы успешно добились.

Анна Попова: К сожалению, заявленный функционал системы не всегда соответствует реальному. В основном обычно разочаровывают заявления вендоров о том, что система перехватывает данные такого-то мессенджера, например. На деле мы видим, что не во случаях перехватывает или ограниченно (только текст или без голосовых звонков). Также продвинутые технологии распознавания часто могут подвести только из-за того, что распознаваемый документ будет просто нечитабелен из-за плохой скан-копии, и ни одна система с этим ничего сделать не сможет.

Галина Рябова: Машинное обучение как подход в DLP развития не получил, потому что для любой обучающейся модели нужен большой объем данных и много часов обучения. Но заложенные в Solar Dozor UBA алгоритмы класса "обучение без учителя" не требуют на этапе обучения экспертной маркировки категорий данных. Соответственно, не нужны и предварительные работы по настройке и адаптации технологии под новые условия эксплуатации. Для анализа устойчивости показателей поведения пользователя и детектирования аномалий (отклонений в поведении) достаточно истории поведения за два месяца.

Алексей Дрозд: Например, в КИБ агент надежно скрыт даже от привилегированных пользователей. КИБ интегрируется с SIEM любых производителей (в том числе нашей собственной) и почти с любыми другими ИТ-системами, от СКУД и расчетчиков зарплаты до DCAP и DAM.

Александр Клевцов: По нашему опыту, в больших компаниях администрирование и эксплуатация DLP – это разные роли. Иногда консоли разделяются отдельно для настройки,

администрирования и отдельно для мониторинга и расследований. Агент Traffic Monitor с обычными правами не получится отключить, привилегированные права и даже продвинутые "хакерские приемы" не помогут: системный драйвер, отвечающий за целостность агента, вернет его обратно. У TM интеграции есть с многими производителями SIEM.

Владимир Ульянов: Для DLP-систем нормальна модульная архитектура, повышающая гибкость использования. Заказчик может под себя сконфигурировать систему, сократив и бюджет проекта, когда отдельные модули не нужны. Несколько консолей не только существенно затрудняют работу офицера безопасности, но и сказываются на эффективности защиты.

Дарья Орешкина: В глобальном смысле множество консолей, похоже, не исчезнет никогда, потому что как только появляется "единая консоль", технический прогресс добавляет нам новую систему с собственной консолью.

На стыке DLP, пандемии и ИИ

Представим организацию в виде человеческого организма, в котором завелся вирус (в терминах DLP – инсайдер). Наша задача – найти в организме информацию о вирусе, который движется по кровеносным сосудам организма.

Прежде всего нас, конечно, интересует работа сердца (бизнес-процессы организации), чистота легких (в нашем примере пусть это будет электронная почта) и деятельность разных клеток крови:

- эритроцитов (например, сотрудников), которые переносят кислород и углекислый газ;
- лейкоцитов (сотрудников с повышенными привилегиями в информационных системах), обеспечивающих работу иммунной системы;
- тромбоцитов (руководство), обеспечивающих свертываемость крови.

Кстати, как тромбоциты не признаются учеными-медиками полноценными клетками, так и в контексте борьбы с утечками и инсайдерами топ-менеджмент иногда выводится за скобки мониторинга DLP-систем.

Принято определять здоровье организма, измеряя температуру тела (информацию, которая движется в электронном виде внутри организации), а также проверяя пульс (в контексте DLP аналогом станет модуль контроля рабочего времени).

Совокупность всех измеряемых параметров организма-организации помогает поставить диагноз (собрать доказательную базу), присутствует или нет вирус-инсайдер. Иногда вирус может до определенного времени вообще никак себя не проявлять, и тогда болезнь протекает бессимптомно.

Если у вас нет вакцины, то вам трудно защитить организм от неизвестного вируса. Элементами такой вакцины в контексте DLP могут стать технологии искусственного интеллекта (ИИ), машинное обучение и нейронные сети. С их помощью можно автоматизировать процесс обнаружения защищаемых данных в компании, что позволит целенаправленно лечить органы, которые в этом нуждаются.

Комментарии экспертов

Галина Рябова: В нашей UBA-системе есть профиль нормального поведения пользователя – аналог нормального состояния здоровья человеческого организма. Как врач измеряет у пациента температуру тела, давление, пульс, так и UBA измеряет внешнюю и внутреннюю активность сотрудников, объем отправленных/полученных информационных объектов, интенсивность взаимодействия с коллегами и т.п. Если показатели здоровья/поведения человека вдруг отклоняются от нормы, это повод для врача/службы безопасности разобраться в причинах. Может быть, человек заболел, а может быть он в данный момент занимается спортом, может готовится реализовать в компании мошенническую схему, а может поссорился с домочадцами и сильно переживает.

Алексей Дрозд: ИИ уже есть в DLP, другое дело, что применяем мы его для решения только тех задач, где он действительно эффективен, где можно достичь баланса между ложными сработками и пропущенными инцидентами. Точность "попаданий" в 95% – не тот результат, с которым готовы мириться клиенты. Одна из задач, которую успешно решает ИИ, это, например, распознавание печатей и штампов. В систему загружаются документы с разными печатями, в будущем она узнает любые подобные изображения.

Александр Клевцов: Мы не ограничиваем руководство в его действиях, но можем понимать, в каком объеме потребляются корпоративные данные и как ими распоряжаются. С помощью политик и технологий анализа можно описать "здоровый организм" и обращать внимание только на отклонения. "Вакцина" в виде режима блокировки утечки не позволит отклониться от здорового состояния. К привилегированным может применяться специальная диагностика, а в отношении руководства важно просто постоянно наблюдать за симптоматикой.

Максим Ксенофонтов: Несомненно, часть задач офицеров безопасности также можно переложить на плечи ИИ, и прежде всего это задачи поведенческого анализа. И скорее всего, крупные разработчики DLP уже делают первые шаги в сторону машинного обучения, остается только дождаться их релиза.

Дмитрий Кандыбович: Конечно же, мы внедряем нейросети, для автоматизации работы, для упрощения той же аналитики. Система сама вычисляет отклонения в поведении сотрудника и сигнализирует об этом. А также мы используем их для упрощения рутинных задач, например распознавания документов и лиц сотрудников: нет нужды подключаться к каждому компьютеру и лично проверять, кто за ним, это сделает программа.

Дарья Орешкина: Технологии машинного обучения сейчас используются в Symantec DLP. ML облегчает настройку политик и точность их срабатывания. В ближайшем будущем замещение офицера безопасности не предвидится, но со временем, очевидно, ИИ все больше задач будет решать не хуже человека, в том числе и в области предотвращения утечек.

Владимир Ульянов: Использование технологий ИИ и машинного обучения – одна из перспектив отрасли. В 2019 г. Zecurion разработал уникальный продукт Camera Detector, который выявляет факты съемки экрана компьютера внешними камерами. Это позволяет бороться с утечками, когда инсайдеры фотографируют конфиденциальную информацию с экрана монитора личными смартфонами.

В основе работы Camera Detector лежит технология машинного обучения на базе нейронной сети, что позволяет детектировать смартфоны любых производителей и моделей, в чехлах и без, на разном фоне, в том числе частично скрытые другими объектами.

Анна Попова: К сожалению, выявить реальных злоумышленников внутри крайне сложно, если они просто пользуются недоступными для перехвата DLP-системой коммуникациями. Спасает, как правило, только накопительный эффект. В поле нашего зрения могут попасть разные сотрудники по разным причинам, даже малозначительным. Важно "присматривать" за ними на периодической основе, и обязательно будет ожидаемый результат.

Лицензии впрок

Борясь с пандемией, неразумно покупать аппараты ИВЛ впрок, не зная предположительно, сколько у вас будет легочных больных, и тем более ставить их всем подряд без разбора, чтобы просто оправдать их приобретение. Но именно так приходится поступать при покупке DLP-лицензий, приобретая их впрок, без какой-либо статистики аналогичных случаев (инцидентов).

Даже если:

а) проведена оценка рисков в компании (поставлен диагноз, возможно и неправильный);

б) руководство сформулировало вам задачу "закрутить гайки" и держать курс на "терзать и трясти собственных сотрудников"; это вовсе не означает, что вам выдан карт-бланш на мониторинг всего и вся, а также неограниченный бюджет на эти цели.

Покупая DLP-систему, вы должны достаточно точно представлять:

- сколько системных агентов вам понадобится для мониторинга каналов;
- логику комбинирования возможностей различных DLP-агентов с другими инструментами системы: механизмами управления инцидентами, парсерами, анализаторами протоколов, перехватчиками и т.д.

Комментарии экспертов

Алексей Дрозд: Мы как раз за то, чтобы "закупать ИВЛ впрок": если не контролировать максимум каналов для всех сотрудников, в защите будут дыры. Тем не менее КИБ позволяет распределить лицензии гибко. Каждый канал контролируется независимо, настройку лицензий по одному модулю необязательно "синхронизировать" с другим.

Максим Ксенофонтов: Как показала текущая история с пандемией, страны, которые имели запас аппаратов ИВЛ, оказались в лучшем положении, чем страны без запаса. Нельзя просто взять и поставить еще 200 аппаратов ИВЛ, когда все текущие будут заняты. Хорошая практика – оценить будущие потребности в лицензиях и заранее их заложить при закупке. Ведь будет неприятно остаться без лицензий, например, при организации и найме нового отдела. Если же подобной возможности нет, то по сложившейся практике закладывается 10% дополнительных лицензий на случай роста.

Галина Рябова: Обычно лицензии на защиту каналов коммуникаций закупаются на всех сотрудников компании. Исключение составляют endpoint-агенты. В ряде случаев компании закупают агенты только для контроля групп риска. Сейчас на рынке DLP приняты цивилизованные лицензионные ограничения: при превышении лимита заказчику напоминают о необходимости докупить лицензии, а не отказывают в обслуживании.

Анна Попова: Вопросы бюджетирования и вынужденных ограничений всегда важны. Но практический опыт говорит, что ценность DLP-системы в том, что в ней накапливается бесценная информация, польза от которой не только оперативном выявлении инцидентов здесь и сейчас, но и в возможности проведения ретроспективного анализа при внутреннем расследовании.

Андрей Арефьев: Важно понимать, что DLP-система – один из кирпичиков в стратегии ИБ. То, насколько корректно составлена стратегия, помогает определить нужный в будущем объем ресурсов: серверов, СХД, количество лицензий. Важна и консультационная поддержка вендора, все это взятое вместе позволяет правильно прогнозировать ресурсы.

Владимир Ульянов: Действительно, DLP редко бывает единственным продуктом для корпоративной безопасности. Наоборот, когда дело доходит до внедрения DLP, уже имеются другие решения. Инсайдерские угрозы, безусловно, важнейшие с точки зрения защиты информации от утечки, но нельзя забывать о проблеме привилегированных пользователей (решения класса PAM) и внешних угрозах (SWG-решения). DLP – неотъемлемый элемент системы корпоративной безопасности, и здорово, когда он тесно интегрируется с другими важными классами, что позволяет сделать надежную бесшовную защиту от разных типов угроз.

Дарья Орешкина: DLP значительно гибче многих других классов систем позволяют организовать покрытие контроля. Часто компании начинают контролировать сначала почту и вебтрафик, затем расширяют контроль endpoint и хранилищ.

Дмитрий Кандыбович: Наша задача – понять, какие задачи пытается решить клиент, здесь важен плотный контакт с теми, кто внедряет продукт, так как именно они в первую очередь владеют знанием о том, что у них есть сейчас. И конечно же, наш продукт можно настраивать очень гибко, поэтому, по сути, нам не столь важно – карт-бланш, не карт-бланш, мы поможем с настройкой так, как нужно клиенту.

Мониторинг соцсетей и удаленный доступ

Зачастую корпоративная жизнь – это сонное царство, бесцветное и зарегулированное. Если бы это было не так, то загруженные на вход искусственного интеллекта корпоративные данные на выходе выдавали бы попутную рекомендацию: уволить каждого второго.

Сейчас фокус определенно смещается в сторону мониторинга соцсетей: без преувеличения можно утверждать, что все проводят там время. Уже проводились эксперименты, когда ИИ после обучения на высказываниях в Твиттере признавался в ненависти к человечеству.

Для мониторинга социальных сетей корпоративная DLP-система бесполезна, ведь доступ к соцсетям внутри компаний, как правило, запрещен. Для этих целей существет достаточно много онлайн-сервисов, в том числе и бесплатных.

А кто знал, что в 2020 г. будет проведено глобальное тестирование компаний на соблюдение "требований по организации безопасного удаленного доступа" из планов непрерывности деятельности! Корпоративная активность с началом пандемии переместилась на домашние компьютеры. Практика и суровая реальность взяли верх над, казалось бы, незыблемыми устоями информационной безопасности компании. Реагируя на это, корпоративные DLP-системы должны перестроиться под новую задачу – удаленная работа как допустимый формат на постоянной основе.

Комментарии экспертов

Максим Ксенофонтов: Социальные сети сейчас – это большое поле возможностей для многих систем ИБ, и DLP-системы здесь не отстают. Обычные утечки в виде post-запросов на страницы (комментарии, сообщения и пр.) DLP-системы уже давно умеют мониторить. Но с развитием соцсетей появился и новый набор функций: многие DLP-системы имеют в агентах специализированные модули, рассчитанные на мониторинг популярных социальных сетей, включая работу со специфическими протоколами.

Дмитрий Кандыбович: Staffcop Enterprise позволяет логгировать и перехватывать переписку в соцсетях, осуществлять теневое копирование отправляемых файлов, отслеживать контрольные слова и даже записывать голосовое общение через мессенджеры. Как говорится, кто, что, где, с кем и зачем. И все это делает очень просто, удобно просматривается и хранится в безопасном месте – на сервере. Контроль сотрудников – это важная часть ИБ, одна из важнейших, поэтому наше решение позволяет осуществлять тотальный контроль.

Анна Попова: Мы предлагаем разделять цели и использовать для мониторинга активности в социальных сетях специально созданные для этого модульные решения. Что касается режима удаленки из-за пандемий и прочего, то здесь можно только посочувствовать производителям DLP-систем, которые не были готовы к тому, что понадобится полностью контролировать MS Teams или Zoom.

Галина Рябова: Я бы разделяла частную жизнь сотрудников в соцсетях и перенос корпоративной активности на домашние компьютеры. Нам надо все время помнить: безопасность – это всегда комплекс мер. Существует много способов обеспечить безопасную работу удаленных сотрудников, начиная от самых простых – использования только корпоративных доменных ноутбуков с установленными средствами защиты и заканчивая организацией доступа в сеть с домашних компьютеров через защищенный слой VDI-брокера.

Алексей Дрозд: Механизмов контроля много, вся соль – в установке стабильного контакта агента с сервером, когда контролируемый ПК находится вне корпоративной сети. Например, в КИБ можно задать правила, чтобы агент самостоятельно парсил перехват и не нагружал канал связи. Плюс задать альтернативные адреса подключения к серверу. Если же связи нет, то информация "складируется" в скрытом хранилище. В итоге DLP работает в полном функционале, перехват не теряется, а бизнес-процессы не тормозятся.

Александр Клевцов: В конце 2019 г. InfoWatch представил клиентам возможность контролировать соцсети прямо из DLP-системы на предмет утечки конфиденциальной информации в публичных постах и комментариях, даже если они сделаны с личных устройств, вне периметра компании и в нерабочее время. Мы интегрировались с платформой "Крибрум", адаптировали технологии контентного анализа под язык и формат, специфичные для соцсетей, и предусмотрели, чтобы разбирать такие инциденты было удобно, в привычном интерфейсе Traffic Monitor. Даже если сотрудник работает с облачными сервисами и с личного мобильного устройства, Traffic Monitor все равно продолжает контролировать его действия.

Дарья Орешкина: Концепция контроля корпоративной информации в условиях применения собственных пользовательских устройств из любой локации передовыми компаниями продумывалась уже давно, в разной степени практики безопасного доступа были реализованы и в коммерческих, и в государственных компаниях. Похоже, пришло время активнее использовать автоматизированные системы как для обработки, так и для контроля информации в условиях удаленной работы.

Владимир Ульянов: Переход на удаленный режим работы добавил забот специалистам по ИБ, риски утечки возросли кратно, слить информацию стало легче. Прибавьте к этому сомнения в завтрашнем дне, снижение лояльности, и станет понятно, почему сотрудники копируют корпоративные данные даже без злого умысла, но просто на всякий случай. И программы мониторинга рабочего времени, которые иногда выдают за разновидность DLP, конечно, не снизят риски утечки. Наоборот, тотальный контроль и требование высидеть положенные часы за компьютером лишь повысят беспокойство работника.

У нас так много средств защиты, что не для всех из них придуманы угрозы

Порой создается впечатление, что компании – производители систем защиты информации при поддержке регуляторов отыскивают у потребителей пока не существующие угрозы, лоббируя "монстров" лингвистического и статистического анализа – DLP-решения с их будущими проблемами обнаружения данных определенного формата (анализ формальных структур), проклятием нехватки вычислительных ресурсов и сложностью интеграции выбранного решения с имеющимися SIEM-системами и системами защиты.

Темпы развития современных коммуникаций переросли уровень тех технологий, которые еще вчера использовались для защиты информации в компаниях. Например, маркировка документов в соответствии с их информационной категорией в современной коммерческой компании давно потеряла смысл. Поиск по регулярным выражениям себя не оправдывает. Правила контроля надо постоянно подкручивать: например, фраза "подхватил вирус" до пандемии имела один смысл, а сейчас у нее может быть совершенно иное значение.

Современные DLP, являясь крайне высокотехнологичным программным обеспечением, тем не менее пока не дотягивают до уровня, при котором безопасники могли бы совершать важные действия с минимальными усилиями.

Комментарии экспертов

Галина Рябова: Вы так говорите, как будто это что-то плохое. Я считаю, что это один из путей развития, когда под продвинутые технологии находятся задачи в материальном мире. Эволюция DLP – один из таких положительных примеров. Начав свое становление с узкой задачи защиты от утечек, современные DLP-системы, обладая продвинутыми аналитическими возможностями, способны решать широкий спектр задач службы безопасности в целом, и даже напрямую задачи бизнеса, например мониторинг эффективности работы удаленных сотрудников. Это выгодно для бизнеса – использовать одну систему для решения многих задач.

Алексей Дрозд: Автоматизация, в том числе элементы ИИ, уже используются в DLP для решения узких задач. Но каким бы продвинутым ни был такой функционал, DLP еще долго не станет "виртуальным безопасником". Это не антивирус, который работает автономно.

Максим Ксенофонтов: Несомненно, пока не будет создан сильный ИИ, человек всегда будет нужен там, где требуется принимать нестандартные решения. Существующие ИИ и машинное обучение смогут разгрузить офицеров безопасности, сняв с них, например, задачу анализа паттернов поведения. Но всегда остается вероятность ЛПС, для исправления которых необходим профессиональный взгляд и анализ ситуации специалистом.

Андрей Арефьев: Организация –- это живой организм, меняющийся под влиянием рынка. Нельзя настроить DLP один раз и забыть про нее. Во-первых, нужно дать ИБ инструменты, чтобы удобно и быстро анализировать происходящее и подстраивать политики. Во-вторых, важно поддерживать актуальными базы защищаемых документов, что нетрудно, это давно делается автоматически. И конечно, ИИ, используемый для категоризации документов, берет на себя все больше задач.

Дарья Орешкина: При эксплуатации любой системы со временем выявляются недочеты, которые набивают оскомину при работе с ней. DLP ввиду своей сложности имеет массу нюансов как при сборе информации, так и при ее анализе. Но все встает на свои места, если задаться вопросом: а как бы хотелось отслеживать пользовательские взаимодействия? За плечом каждого вешать видеокамеру? Ну допустим, а как нарушителя искать из тысяч сотрудников в многочасовых видеозаписях? В конце концов мы приходим к выводу, что в текущей реализации DLP не хватает упрощения настройки политик и функций помощи в точном обнаружении инцидентов. Похоже, ИИ должен справиться с этими задачами в скором будущем.

Владимир Ульянов: Развитие DLP сегодня направлено в сторону предугадывания нарушений, так, чтобы их можно было предотвратить заранее, а сотрудника, вызывающего сомнения, поставить на особый контроль. Именно поэтому многие DLP уже получили встроенные модули поведенческого анализа UBA. Zecurion пошел дальше и позволяет отслеживать эмоции контролируемых пользователей, которые также могут свидетельствовать о потенциальной угрозе. Как показывает практика, человек может скрыть подготовку к краже данных, но маскировать свои истинные эмоции на протяжении долгого времени не способен.

Авторское заключение

Организации научились собирать данные с помощью DLP-систем. Теперь им надо понять, что делать с этими данными. На передний план выходят не столько сами данные, сколько технологии их обработки.

Очевидно, что будущее за интеграцией технологий: DLP, машинного обучения, искусственного интеллекта, автоматизации с применением нейронных сетей. Уже сейчас с помощью искусственного интеллекта в компаниях пробуют предсказывать, например, увольнения сотрудников.

Возможно, от предсказания увольнений с помощью ИИ до предсказания утечек данных остался всего один шаг?

Технологии стали главным источником информации. Но пока "выявлять чувствительные персональные данные и разбираться с ними столь же сложно, как и определять, какая корпоративная информация сохранила или потеряла свою деловую ценность с течением времени", как мудро заметил Марк Кассетта, старший вице-президент по стратегическим вопросам компании Titus. ●

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

Колонка редактора

Сергей Рысин,
эксперт по ИБ

К наблюдениям за развитием DLP

У каждой DLP-системы свои особенности, каждый производитель активно рассказывает о важности именно своего подхода. Стоит, не претендуя, впрочем, на категоричность, вспомнить, с чего системы начинали: к примеру, Zecurion и InfoWatch начинали с хорошей работы на сетевом уровне, а SearchInform и DeviceLock изначально были сильны в работе на конечных устройствах.

Дальнейшее развитие систем протекало в жесткой конкуренции, но именно скорость обработки данных внутри системы и быстрота принятия решения позволяли на том этапе занять больший рынок.

Сейчас же все производители систем постепенно, но планомерно приходят к реализации концепции DLP Next Generation, содержащей, кроме функционального потенциала, еще и маркетинговый.

Однако у нас, конечных потребителей, есть свой набор требований к DLP-системе:

- скорость доработки выявленных при эксплуатации проблем;
- качество технической поддержки: ведь любой заказчик рано или поздно обращается к вендору за помощью и важно, чтобы этот процесс был комфортным;
- простота и послойность перехода к новой версии;
- простота подключения и внедрения новых паттернов, интересных для защиты интересов бизнеса;
- скорость внедрения новых подходов в системе;
- визуализация данных: это новый тренд в ИБ, позволяющий конечным операторам быстрее вырабатывать и принимать качественные решения.

Отмечу, что на сегодняшний день эти задачи в той или иной степени реализованы у всех DLP-вендоров. Поэтому мой личный опыт свидетельствует, что выбирать стоит не столько систему, сколько производителя. Того, кто готов помогать быстро и качественно решать ваши проблемы для достижения вами успеха в решении задач бизнеса, который вы защищаете. ●