ИЗДАЕТСЯ КОМПАНИЕЙ «ИНФОСИСТЕМЫ ДЖЕТ»

Jet Info

WWW.JETINFO.RU

ТЕМА НОМЕРА

DLP СО ЗНАКОМ +

№ 9 (266)/2015

Jet Info

Издается с 1995 года

Редакция:
Дмитриев В.Ю.
Дискина А.Л.
Некрасова Н.А.
Шедова Е.Л.

Дизайн и верстка:
Саблина М.А.

Корректура:
Макеева Е.И.

Над номером работали:
Акимов Е.О.
Аношин М.С.

Издатель:
Компания «Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01
info@jet.msk.su

www.jetinfo.ru

МИХАИЛ АНОШИН,
руководитель направления DLP
Центра информационной безопасности
компании «Инфосистемы Джет»

DLP-решения плотно вошли в обиход ИБ-жизни современных компаний. Информация – один из наиболее ценных активов сегодняшнего бизнеса. Так, многие наши заказчики совместно с нами реализовали мощные проекты по защите от утечек информации, но на этом не остановились.

Постоянно меняющаяся «среда обитания» бизнеса порождает новые задачи для ИБ. Меняются портреты типичных нарушителей, профили инцидентов, общая картина информационного обмена. Все это добавляет к проектам по защите от утечек прикладные задачи и расширяет границы применения внедренного решения. DLP отныне ловит не только утечки информации, а результатами работы системы пользуется не только информационная безопасность. Мы наблюдаем качественное изменение – переход от узкой защиты от утечек к широкому контролю коммуникаций.

В этом номере мы хотим поделиться с читателями своим опытом, мнением наших заказчиков и экспертов о том, как сегодняшние DLP обеспечивают завтрашнюю безопасность.

Содержание

Содержание

ПОСТРОЕНИЕ ДАТА-ЦЕНТРА ДЛЯ ВТБ24

СЕРГЕЙ АНДРОНОВ, директор Центра сетевых решений компании «Инфосистемы Джет»

ВТБ24 и компания «Инфосистемы Джет» запустили в эксплуатацию новый дата-центр мощностью 1,6 МВт, рассчитанный более чем на 90 высоконагруженных стоек различных габаритов, включая оборудование класса Hi-End.

«ВТБ24 – один из наиболее динамично развивающихся отечественных банков. С 2012 г. наша сеть выросла с 700 до 1050 офисов. Этот количественный показатель имеет отражение и в существенном увеличении объемов обрабатываемой информации, что, соответственно, требует увеличения вычислительных мощностей. Приступая к стройке четвертого ЦОД, мы приняли решение объединить на его базе всю ИТ-инфраструктуру в единый отказоустойчивый узел с высоким уровнем надежности и значительным заделом на масштабирование», – рассказывает **Алексей Таракин, начальник отдела инженерного обеспечения и эксплуатации сервисного центра ВТБ24.**

Эксперты компании «Инфосистемы Джет» разработали детальный проект по строительно-архитектурной подготовке помещения офисного класса под размещение дата-центра. В соответствии с ним проведен комплекс работ по усилению перекрытий до уровня 1,5 тонны распределенной нагрузки на квадратный метр, а также сконструирован фальшпол, в пространство которого убрана большая часть коммуникаций.

Спроектирован и внедрен комплекс необходимых для жизнеобеспечения ЦОД инженерных подсистем. В проекте использованы передовые технические решения, в том числе:

- построена структурированная кабельная система, рассчитанная на передачу данных со скоростью до 40G. В соответствии с этими требованиями спроектирована единая сеть для всех дата-центров банка, разработан и реализован детальный план миграции без останова работающих ЦОД. Ядро СКС централизовано, за счет чего, в том числе, в 6 раз сокращено место, занимаемое коммутационными шкафами;
- при создании системы кондиционирования и вентиляции впервые в России использовано новое поколение энергоэффективных чиллерных установок STULZ с системой free cooling и др.

Оборудование дата-центра (более 100 единиц сетевого, инженерного, климатического и пр.) подключено к системе диспетчеризации, позволяющей через единый графический интерфейс анализировать показатели производительности оборудования во всех ЦОД банка и оперативно перераспределять нагрузку между ними.

Все системы зарезервированы по схемам от N+1 до N+3. На случай возможных перебоев в подаче электроэнергии установлен комплекс дизель-генераторных установок, использующий улучшенные технологии фильтрации выхлопной системы и позволяющий обеспечивать полноценную работу дата-центра в течение 8 часов.

ЦОД построен с учетом требований международного стандарта TIA-942, уровень надежности комплекса инженерных систем соответствует TIER III, коэффициент отказоустойчивости – 99,982%, а общая площадь превышает 360 м^2.

«При проектировании мы учитывали требования по энергоэффективности и производительности, а также делали ставку на повышенную гибкость инженерной и ИТ-инфраструктуры. В результате конфигурация каждой системы гарантирует ее эффективность и позволяет решить ряд дополнительных задач: увеличить полезные площади ЦОД, сократить будущие расходы на его модернизацию или отодвинуть ее по времени. Например, использование кондиционеров с наиболее оптимальным соотношением удельной производительности к занимаемой площади позволило сэкономить до 20% полезного серверного пространства», – поясняет **Сергей Андронов, директор Центра сетевых решений компании «Инфосистемы Джет».** JI

ВНЕДРЕНИЕ СИСТЕМЫ КОНТРОЛЯ И МОНИТОРИНГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ГРУППЫ QIWI

ЕВГЕНИЙ АКИМОВ, директор по развитию бизнеса Центра информационной безопасности компании «Инфосистемы Джет»

Группа QIWI и компания «Инфосистемы Джет» запустили в эксплуатацию автоматизированную систему контроля и мониторинга инцидентов информационной безопасности в инфраструктуре платежного сервиса QIWI.

Система контроля и мониторинга инцидентов ИБ осуществляет централизованный сбор, корреляцию и анализ событий информационной безопасности со множества источников, а также автоматизирует процессы защиты баз данных. Система реализована на базе решений IBM Security QRadar SIEM и IBM Guardium. Ее внедрение позволило сократить время на поиск и анализ событий ИБ в распределенной инфраструктуре QIWI, осуществлять мониторинг запросов к базам данных и регистрацию событий информационной безопасности в СУБД, а также существенно повысить общий уровень защищенности корпоративной информационной инфраструктуры. Система также помогает обеспечивать соответствие международным стандартам, таким как PCI DSS и SOX.

«Внедрение системы контроля и мониторинга инцидентов ИБ стало серьезным шагом в развитии комплекса безопасности QIWI. Эта система позволяет в кратчайшие сроки реагировать на инциденты и отслеживать всю активность в нашей инфраструктуре. В совокупности с системой мониторинга баз данных комплекс позволяет обнаружить несанкционированную активность на самой ранней стадии», – сообщил **директор по информационной безопасности Группы QIWI Кирилл Ермаков.**

Проект охватил три московские площадки заказчика – два дата-центра и центральный офис. Специалисты компании «Инфосистемы Джет» провели предпроектное обследование инфраструктуры платежного сервиса QIWI, спроектировали и внедрили решения. К системе контроля и мониторинга инцидентов ИБ были подключены более 1800 источников событий свыше 20 различных типов. Согласно статистике, в день обрабатывается примерно 100 ГБ событий и 50 ГБ сетевого трафика.

Агенты IBM Guardium установлены на основные продуктивные и тестовые базы данных, реализован функционал маскирования (частичного сокрытия при отображении) выводимых критичных данных клиентов сервиса QIWI.

«Яркая особенность проекта с QIWI – большое количество подключенных источников. Часть из них являлись нестандартными, и потребовалась разработка специальных парсеров, – отмечает **Евгений Акимов, директор по развитию бизнеса Центра информационной безопасности компании "Инфосистемы Джет".** – Эта работа выполнялась в тесном взаимодействии с ИТ-администраторами и разработчиками, некоторые из систем QIWI были дополнительно оптимизированы под этот проект».

Единая консоль IBM QRadar позволяет в режиме, близком к реальному времени, анализировать информационные потоки, проходящие через систему контроля и мониторинга инцидентов ИБ, формировать отчеты, оповещения об инцидентах безопасности.

С целью оценки эффективности созданной системы Группой QIWI были организованы независимые работы по проведению внешнего и внутреннего анализа защищенности (pentest). По результатам проведенных тестов специалисты Группы QIWI высоко оценили возможности внедренной системы по обнаружению угроз ИБ и подозрительной активности в инфраструктурных системах.

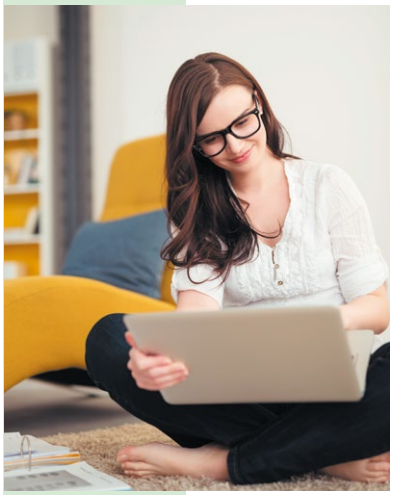
Инфраструктура Группы QIWI очень динамична, постоянно расширяется – по мере появления новых систем они подключаются к системе контроля и мониторинга инцидентов информационной безопасности.

СОЗДАНИЕ СИСТЕМЫ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ ТРАФИКОМ ДЛЯ «ВЫСШЕЙ ШКОЛЫ ЭКОНОМИКИ»

ЕЛЕНА ФОМИНСКАЯ, директор Центра телекоммуникационных продуктов и решений компании «Инфосистемы Джет»

Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ) и компания «Инфосистемы Джет» создали комплексную систему динамического управления доступом в интернет на базе продуктов Jet Subscriber Manager (JSM) и Procera Networks PacketLogic (решение DPI).

«Самая масштабная наша площадка – распределенный московский кампус, кроме учебно-административных зданий включающий крупные общежития, размещенные в Одинцовском районе, и несколько общежитий в Москве. Студенты и преподаватели могут выходить в интернет из любой точки университета, территорий учебно-административных корпусов и общежитий, – рассказывает **Олег Щербаков, директор по ИТ НИУ ВШЭ.** – Для нас важно обеспечивать не просто доступ в интернет всем пользователям, а доступ каждого сотрудника или студента к интернет-сервисам с гарантированными параметрами. Особенно актуально управление трафиком в общежитиях – там, где на пользователя зачастую приходится три и более подключений, а пользователей – более 6,5 тысяч. Несложно понять, что происходит с полосой пропускания в пиковые часы, когда большинство студентов примерно в одно время возвращаются с занятий. Для управления ситуацией нужен инструмент, обеспечивающий персональную авторизацию, качественный анализ трафика с применением к нему соответствующих политик (в том числе ограничения) и справедливое его распределение. Даже понимание того, как работает в сети устройство, существенно расширяет возможности по разрешению инцидентов, например, при беспроводном доступе. Также решение необходимо для повышения безопасности корпоративной сети при атаках изнутри».



На первом этапе внедрение системы осуществлялось на двух основных каналах доступа в интернет из корпоративной сети учебных и административных зданий и одном канале, организованном на три здания комплекса общежитий в Одинцовском районе. Работы заняли около трех месяцев. Эксперты компании «Инфосистемы Джет» сформировали набор правил, по которым должна работать сеть, провели предварительную проверку и настройку DPI-оборудования, осуществили последовательный монтаж каждого из узлов, развернули JSM на виртуальной инфраструктуре университета и настроили политики управления трафиком.

«DPI позволяет администраторам сети видеть структуру трафика, формировать регулярные отчеты о загрузке каналов, прогнозировать их загрузку и необходимость модернизации. Однако стоявшая перед нами задача была шире, нежели простая демонстрация «содержимого» трафика. Для более глубокой аналитики и дальнейшей выработки правил для дифференцированного управления трафиком необходимо было его персонализировать с детализацией до конкретного пользователя», – поясняет **Елена Фоминская, директор Центра телекоммуникационных продуктов и решений компании «Инфосистемы Джет».**

В ходе проекта выполнена интеграция JSM с внутрикорпоративной AD (Active Directory) для доступа работников университета и AD Office 365 для доступа студентов. Это позволило персонифицировать трафик всех категорий конечных пользователей сети НИУ ВШЭ. Также при беспроводном доступе к сети НИУ ВШЭ реализован сервис для гарантированного получения приоритетного права на использование интернет-трафика, позволяющий предоставлять преимущественный доступ к ряду online-сервисов и ресурсов (в том числе при проведении обучающих семинаров, конференций и т.п.) в динамическом режиме по запросу.

Специалисты компании «Инфосистемы Джет» провели расширенный инструктаж для администраторов сети НИУ ВШЭ с демон-

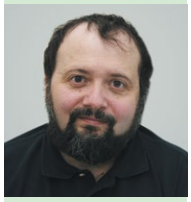
страцией различных сценариев, характерных для университета.

Оборудование в рабочем режиме накапливает статистику уже более полугода (с февраля 2015 года). На сегодняшний день функционал персонификации запущен в административных зданиях, а сеть с общим доступом выводится из эксплуатации. В общежитии режим общего доступа к сети будет деактивирован в ближайшее время.

«Организация управления трафиком в "студенческих" сетях – уже сложившаяся международная практика. В проекте для Высшей школы экономки мы использовали наши best practices и в очередной раз успешно выступили в связке с продуктом класса PCRF компании "Инфосистемы Джет"», – **отмечает Антон Дегтярев, директор пресейл EMEA, Procera Networks.**

В дальнейших планах университета – подключение к системе динамического управления трафиком всех университетских площадок в Москве. Решение также может быть успешно тиражировано на уровне регионов, в том числе с более широкой реализацией функционала DPI и JSM.

ПЕРЕВОД БАЗЫ ДАННЫХ СК «СОГЛАСИЕ» НА ORACLE EXADATA



АЛЕКСЕЙ СТРУЧЕНКО, начальник отдела оптимизации СУБД и приложений компании «Инфосистемы Джет»

Страховая компания «Согласие» перевела базы данных ERP-системы на оптимизированный программно-аппаратный комплекс Oracle Exadata. Партнером по проекту выступила компания «Инфосистемы Джет», Oracle Platinum Partner.

«Переход на новую платформу был связан с планами по централизации учетных систем компании и обеспечению единого информационного пространства для сотрудников филиалов. Текущая платформа не могла обеспечить масштабирование процессорных мощностей для обработки растущих объемов информации, – рассказывает **директор департамента ИТ СК "Согласие" Сергей Клочков.** – Совместно со специалистами "Инфосистемы Джет" мы выбрали платформу оптимальной конфигурации, которая позволила достичь качественно новых показателей производительности, даже несмотря на то, что рост объемов данных превзошел наши первоначальные ожидания».

Комплексное обследование и анализ производительности нескольких платформ произведены под характерной нагрузкой основной продуктивной системы СК «Согласие». В результате был выбран программно-аппаратный комплекс Oracle Exadata.

Платформа интегрирована с имеющимся ИТ-ландшафтом. Процедура миграции со сменой операционной системы была тщательно проработана в тестовом режиме, после чего все базы были переведены в продуктив. При этом для каждого из этапов были заранее продуманы планы возврата к первоначальному состоянию. Наиболее критичная база данных заведена в кластер, а свободные ресурсы программно-аппаратного комплекса выделены под среды разработки и тестирования.

«Трудно переоценить значимость модернизации, ведь изменения коснулись продуктивных систем, обеспечивающих ежедневное функционирование бизнес-процессов страховой компании, – отмечает **Алексей Струченко, начальник отдела оптимизации СУБД и приложений компании "Инфосистемы Джет".** – Отдельно следует отметить интересные вопросы архитектуры: при решении задачи консолидации баз данных рассматривалось несколько вариантов распределения значительных ресурсов Oracle Exadata. Тесное взаимодействие и слаженная командная работа наших экспертов (в числе которых Oracle Certified Master) и специалистов СК "Согласие" позволили выбрать оптимальный вариант и достичь поставленных целей».

«Приятно отметить, что все шире отраслевой охват компаний, которые получают преимущества от Oracle Engineered Systems. Мы рады приветствовать СК "Согласие", которая одной из первых в страховой отрасли России модернизировала ИТ-инфраструктуру на Oracle Exadata и в разы повысила производительность важнейших систем, обеспечив поддержку для многократного роста бизнеса и развития в краткосрочной и долгосрочной перспективе», – отметил **Андрей Пивоваров, руководитель группы перспективных технологий предпроектного консалтинга, Oracle СНГ.**

НЕ СОВСЕМ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ЕВГЕНИЙ АКИМОВ,
директор по развитию бизнеса
Центра информационной безопасности
компании «Инфосистемы Джет»

Информационная безопасность – одна из самых обсуждаемых тем в ИТ. Если посмотреть различные материалы, статьи, доклады на мероприятиях, форумы и блоги по ИБ, выяснится, что в течение последних 10 лет ИБ-сообщество бурлило многочисленными трендами. Все то учились управлять информационной безопасностью (вспомним те надежды, которые были вокруг стандартов 2700х серии), то защищали персональные данные (о существовании № 152-ФЗ, похоже, знает каждая домохозяйка), то строили «настоящие SOC'и», то расследовали киберпреступления.

Но насколько то, чем мы стали заниматься, – действительно информационная безопасность? Т.е. действительно ли наша деятельность направлена на достижение состояния защищенности исключительно информационных ресурсов? Разобраться в этом не столько интересно, сколько полезно – правильное понимание цели даёт возможность достигать её быстрее и проще.

Если не забираться в совсем исторические дебри (10 и более лет назад – уже позавчерашний день), можно уверенно говорить о нескольких сменах ориентиров в области нашей деятельности (аббревиатуру «ИБ» специально не применяем, она же поставлена под сомнение).

Как раз 10 лет назад лучшие практики в области ИБ были собраны в британских стандартах серии BS 7799 (контрольные механизмы – часть 1, система управления – часть 2, управление рисками – часть 3). Достаточно быстро стандарты получили международное признание: они легли в основу ISO 27001, и именно под этим названием практики выбора механизмов защиты на основе управления рисками ИБ получили повсеместное распространение.

Около 3 лет назад мы говорили о переходе от рисковой модели управления ИБ к снижению реальных потерь. Действительно, риски как вероятностная величина не настолько точно и (что немаловажно для отечественных реалий, в которых принцип «пока гром не грянет, мужик не перекрестится» закреплён на уровне поговорки) ярко характеризуют наличие или отсутствие проблем, требующих решения. Почему такая миграция стала возможна? Просто инциденты стали настолько частыми, что за обычный для оценки эффективности период времени (чаще всего год) в компании наверняка что-то происходило, и далеко не раз. Наглядно это демонстрировали, например, DLP-системы: даже в ходе пилота за пару недель обнаруживались 2–3 инцидента, потери от них сравнительно просто пересчитывались в деньги. Экстраполяция на год, и – вуаля! – срок окупаемости посчитан. Причем частенько в этот год и укладывались, а сложная и непоказательная математика с вероятностью, рисками и т.п. для принятия решения не применялась.

Вооружившись до зубов, мир все ещё информационной безопасности начал подобные системы эксплуатировать. И тут выяснилось, что результаты работы DLP-системы (не будем менять пример, он очень удачный) используются отнюдь не внутри подразделения ИБ. Чаще всего служба экономической безопасности инициирует расследование и делает запрос ИБэшникам для анализа коммуникаций попавших под подозрение сотрудников (пассивный вариант). Реже DLP-система сама что-то находит, и для принятия конкретных шагов эта информация передаётся в экономическую безопасность (активный вариант). Мы сталкивались с ситуациями, когда внутри холдинга одним из KPI службы экономической безопасности было количество уголовных дел, заведенных на собственных сотрудников. На добрую половину он выполнялся на DLP-системе.

Насколько эта система стоит на страже информационных ресурсов, если типовой инцидент – это сговор в мессенджере соцсети между сотрудником, отвечающим за закупки, и поставщиком? Очевидно, что в небольшой степени. Но подобные не ИТ-деяния оставляют ИТ-след, который и был обнаружен, а затем использован в целях обеспечения корпоративной/экономической безопасности.

Во всё большем количестве компаний службы «всё еще информационной» безопасности пошли дальше: ведь массовая автоматизация бизнес-процессов позволяет с помощью ИТ-средств обнаруживать не только такие аномалии. В этом смысле уместно привести ещё одно устоявшееся выражение – на этот раз цитату «Как дела в России? – Воруют». Существует множество мошеннических схем, использование которых достаточно просто детектируется с помощью информационных технологий. Например, нечестный кассир, недодавший

в течение смены сдачу, очень часто открывает кассу, чтобы достать «лишние деньги», и проводит операцию по фиктивной продаже нескольких грамм картошки. Такая аномалия служит сигналом службе безопасности. Или (если воруют по-крупному) погрузчик на складе загружает паллету с товаром не в тот грузовик – это отслеживается либо по Wi-Fi-метке на погрузчике, либо за счёт анализа видео.

За последнее время в нашей стране стартовало значительное количество проектов по противодействию мошенничеству и воровству в различных отраслях – в ритейле, на транспорте, в логистических компаниях, нефтянке. Большинство таких внедрений ведутся подразделениями информационной безопасности в сотрудничестве с внутренним контролем и экономической безопасностью, во многом потому что последние с информационными технологиями, скорее, «на Вы, чем на ты». По сути, безопасность информационных ресурсов в этом случае вообще остаётся в стороне, и уровень информационной безопасности никак не меняется.

Однако именно такие проекты часто обозначаются руководством компаний как стратегические, на них делается ставка в развитии бизнеса. Мы сталкивались с ситуациями, когда ROI от таких проектов превышает ROI от традиционных бизнес-проектов – развития филиальной сети, диверсификации бизнеса и пр. Действительно, в текущих экономических условиях во многих отраслях практически нереально хоть сколько-нибудь увеличить объем бизнеса, и ставка на сокращение издержек – основной вектор развития. С учётом того, что от воровства и мошенничества компании теряют 1–4% от своего оборота (и это не сокращение оборота, а недополученная чистая прибыль!), а антифрод-проекты сокращают потери на 30–50% при сроке окупаемости от полугода, давнее стремление ИБэшников приносить деньги в компанию наконец-то начинает реализовываться.

> Результаты работы DLP-системы используются отнюдь не внутри подразделения ИБ. Чаще всего служба экономической безопасности инициирует расследование и делает запрос ИБэшникам для анализа коммуникаций сотрудников

Вхождение традиционной информационной безопасности в подобные «не ИБ»-проекты, с одной стороны, можно воспринимать как данность. С другой – это даёт руководителям более глубокое понимание бизнеса, которое начинает распространяться и на всю остальную деятельность ИБ-подразделения. Меняются и цели проектов. Например, происходит миграция от «надо мониторить инциденты ИБ в соответствии с лучшими практиками» к «управление инцидентами дает возможность оперативно реагировать и сокращать ущерб». При этом естественное желание выбрать лучший в своем классе продукт для решения каждой частной задачи сменяется выбором технологий, имеющих оптимальное сочетание функциональности и совокупной стоимости владения.

Именно такой обновленный взгляд, с одной стороны, более критический, с другой – более широкий, рассматривающий все возможности, предоставляемые ИТ для обеспечения безопасности бизнеса, является характерной чертой сегодняшнего дня. Конечно, это не отменяет, а, скорее, дополняет традиционные практики – управление рисками. Но то, что мы перестали быть только ИБэшниками и существенно лучше разбираемся в том, на чем компания зарабатывает, а на чем теряет, и как мы можем в этом помочь, даёт возможность сделать существенно больше, чем мы могли ещё вчера.

DLP – ЗАЧЕМ НАМ ЭТО НУЖНО, ИЛИ РЕЦЕПТ ОБОСНОВАНИЯ ДЛЯ РУКОВОДСТВА

СЕМЁН ВАСИЛЬЕВИЧ: Ты мне скажи, на какие заработки заместитель директора трикотажной фабрики отгрохал себе двухэтажный особняк?

ДИМА СЕМИЦВЕТОВ: Семен Васильевич, это его дело!

СЕМЁН ВАСИЛЬЕВИЧ: Нет, наше! Мы будем просто-таки нещадно бороться с лицами, живущими на, допустим, нетрудовые доходы!

МИХАИЛ АНОШИН,
руководитель направления DLP
Центра информационной безопасности
компании «Инфосистемы Джет»

Те из нас , кто хоть раз защищали какой-либо проект перед руководством, сталкивались с такими терминами, как «Total cost of ownership», «Return On Investment» и их русскоязычными аналогами «Совокупная стоимость владения», «Окупаемость инвестиций». И у каждого из нас могли возникнуть сложности с этими вычислениями.

Хотя если хорошенько разобраться, ничего сложного с подсчетом коэффициентов, которые эти термины обозначают, нет. Считаются они по вполне определенным формулам, бери значения да подставляй. Когда речь идет о проектах по внедрению средств защиты информации, с первым термином, опять же, сложностей никаких – всегда можно с достаточно высокой точностью подсчитать, в какую копеечку влетит внедрение. В некоторых случаях даже напрягаться не придется – системные интеграторы, набившие руку на таких проектах, предоставят одну из заготовленных моделей TCO. Однако после того как мы готовы во всех красках описать владельцам бизнеса, в какой момент и на сколько опустеют их карманы при ввязывании в «это», наступает самое время прибегнуть ко второму коэффициенту и обозначить оптимистичную финансовую отдачу или хотя бы обозримый срок окупаемости. Вот здесь и начинаются проблемы. Если это не проект по противодействию мошенничеству, с какой-либо вменяемой уверенностью заявить о коэффициенте ROI либо трудно, либо вообще невозможно. Особенно в период финансовой нестабильности и политики тотальной экономии, когда трату каждого рубля нужно уверенно обосновывать. Антифрод-проектам повезло – еще на этапе тестирования можно выяснить, сколько денег поможет сохранить такая система.

Что же до проектов по защите от утечек информации, крайне сложно подсчитать ненаступивший ущерб в результате того, что файлу или письму не дали покинуть периметр компании. Конечно, можно говорить о № 98-ФЗ и коммерческой тайне, о соответствии требованиям регуляторов, которые, кстати говоря, в части защиты от утечек носят лишь рекомендательный характер. Можно пытаться оценить стоимость утечки через рисковую модель и т.д. Любой более-менее разбирающийся в теме держатель бюджета после выслушивания этих доводов в лучшем случае задаст уточняющий вопрос: «Ну и что?».

Опыт многочисленных проектов позволил нам вывести определенную методологию обоснования DLP-проектов для бизнеса. Ниже мы рассмотрим несколько ее составляющих.

«ТЕБЯ ПОСОДЮТ, А ТЫ НЕ ВОРУЙ»

Совершенно очевидно, что основным назначением систем DLP является пресечение воровства – воровства информации (намеренного или случайного) и воровства финансового (откаты, взятки, мошеннические схемы и т.д.).

С первым современные системы научились довольно хорошо справляться: есть достаточное количество автоматизированных средств анализа, которые выявляют среди легитимного потока информации подозрительную передачу конфиденциальных данных. Такой бенефит особенно хорошо превращается в аргумент к приобретению системы для руководства тех компаний, в которых есть место инновационным разработкам, ноу-хау и другим сведениям, представляющим коммерческую тайну, т.е. являющимся основополагающими для бизнеса. Это могут быть планы развития сети банка, разведданные нефтедобывающих компаний, маркетинговые идеи ритейл-корпораций, базы клиентов страховщиков и др. Потеря таких сведений, а тем более их предумышленный вынос ставят под угрозу, как минимум, прибыль и репутацию компании.

Даже если в вашей компании такой информации нет или же она за пределами организации теряет смысл, почти наверняка у вас при-

сутствуют процедуры продажи/закупки. Ими занимаются люди, коммуникации которых стоит контролировать. Нередко результатом контроля беседы между «коллегами по цеху» являются всплывающие случаи мошенничества, сговоры и другие действия, наносящие прямой ущерб компании. Контролируя переписку с внешними людьми, можно обнаружить намеки на взятки/откаты. Все это тоже воровство, которое хоть и проявляется не так часто, как утечка информации, но также заслуживает отдельного внимания и может быть выявлено DLP-системой. Скорее всего, владельцы бизнеса знают о подобных возможных схемах, и в этом месте чрезмерно убеждать их не придется – необходимость контроля очевидна.

БИЗНЕС – ЭТО НЕ ТОЛЬКО ДЕНЬГИ

Если нельзя выразить пользу от системы в прямых доходах (точнее, в сохранении потерь), нужно обратить внимание на другие составляющие бизнеса, не менее важные, чем финансы. Близко к ним лежит тема эффективности – использования человеческих ресурсов, исполнения прописанных бизнес-процессов. И то, и другое можно контролировать системой DLP. Контролируя одну лишь корпоративную электронную почту, DLP покажет, насколько хорошо персонал справляется со своими обязанностями – четко ли исполняются предписанные регламенты, как в целом работает бизнес-процесс, на что сотрудники тратят рабочее время, собираются ли они менять работу и т.д. Из некоторых перечисленных пунктов можно вывести экономическую составляющую. Например, набирающий популярность кейс контроля рабочего времени: все то время, что нанятый сотрудник проводит в соцсетях или тратит на

> Для успешного обоснования проекта по DLP нужно ответить на 2 основных вопроса: «Зачем нам это нужно?» и «Почему это столько стоит?»

просмотр видеороликов, можно умножать на его заработную плату и смело минусовать из бюджета компании. В момент экономического кризиса владельцы бизнеса как никогда заинтересованы в том, чтобы все имеющиеся ресурсы, в том числе людские, работали с максимальной эффективностью, поэтому им будет интересен подобный инструмент.

По причине того же кризиса важно не упасть в грязь лицом перед конкурентами на рынке и сохранить клиентов. Репутация компании и бренда сейчас ценится очень высоко. Клиенты сегодня хотят знать, кому отдают свои деньги. Помимо фиксирования утечек информации, наносящих репутационный ущерб, DLP позволяет выявлять высказывания нелояльных сотрудников в отношении компании или её руководства. Разумеется, если сообщения с этими высказываниями отправляются из компании. Хотя для мониторинга упоминаний компании с неподконтрольных устройств тоже есть специальный продукт.

Ну и наконец, помимо поиска и разбора инцидентов, важен показательно-воспитательный процесс. С одной стороны, DLP позволяет обучать пользователей культуре ИБ. Либо сотрудники просто знают о мониторинге и дважды подумают перед отправкой письма с конфиденциальной информацией, либо DLP выдаст предупреждение о подозрительных действиях пользователя и запросит подтверждение. С другой стороны, при проведении периодической показательной работы с персоналом (дисциплинарные взыскания, увольнения, обнаро-

дование выговоров с занесением) желание совершать проступки у сотрудников резко убавляется. Любое руководство заинтересовано в соблюдении рабочего порядка и всеобщей дисциплине.

ИСКЛЮЧИТЕЛЬНО ВО БЛАГО

Еще одним важным аспектом в подготовке к обоснованию и выполнению проекта по DLP является этап, схожий с этапом продажи товара или услуги, – работа с возражениями. Как и практически любой проект по информационной безопасности, внедрение системы защиты от утечек может вызвать множество вопросов и недоверия: «Не будет ли это мешать?», «Не встанет ли из-за этого наш бизнес?», «Будет ли пользователям так же удобно работать, как и раньше?».

Одна часть ответов на эти вопросы напрямую зависит от схемы и области применения обсуждаемого решения. Важно показать всем заинтересованным лицам, что DLP не оказывает существенного влияния на текущую информационную среду и контролирует только то, что действительно нужно. Для этого лучше всего начинать с DLP, работающей в пассивном режиме. Можно сказать, в режиме «обучения». Система перехватывает весь положенный ей трафик, обрабатывает его и предупреждает о найденных событиях, но никаких активных действий не предпринимает. В таком режиме стоит поработать год, а лучше два. После этого приходит тот самый аппетит во вредя еды, и владельцы бизнеса сами видят необходимость активных действий. Ведь пока система не будет установлена и не начнет работу, трудно будет показать, что именно теряет компания без неё.

Другая часть ответов на обозначенные вопросы относится к технической части и возможностям предполагаемой DLP: чтобы особенности технической реализации системы не мешали работе и не оказывали воздействия на инфраструктуру.

ДОПУСТИМ, НУЖНА… А КАКАЯ?

После того как в пользу DLP-системы набралось достаточно аргументов и были сняты все вопросы, важно обосновать выбор конкретного средства. Чем увереннее в системе будете вы сами, тем быстрее руководство поймет, что вами проведена серьезная предварительная работа по анализу рынка и выбору системы. Важно дать понять держателям бюджета, что это не просто очередная трата их средств, а обоснованный выбор решения, удовлетворяющего оптимальному соотношению цена/качество. Здесь можно порекомендовать активнее прислушиваться к мнениям интеграторов, которым вы доверяете. У некоторых из них за плечами опыт нескольких сотен подобных проектов, и они готовы привести аргументированные «за» и «против» рассматриваемых систем именно в вашем случае. Помимо этого, необходимо тестирование системы. Как правило, когда компания-интегратор достаточно хорошо понимает бизнес и потребности ИБ вашей компании, она проводит успешное тестирование одного или нескольких решений. Результаты обычно значительно упрощают процесс обоснования.

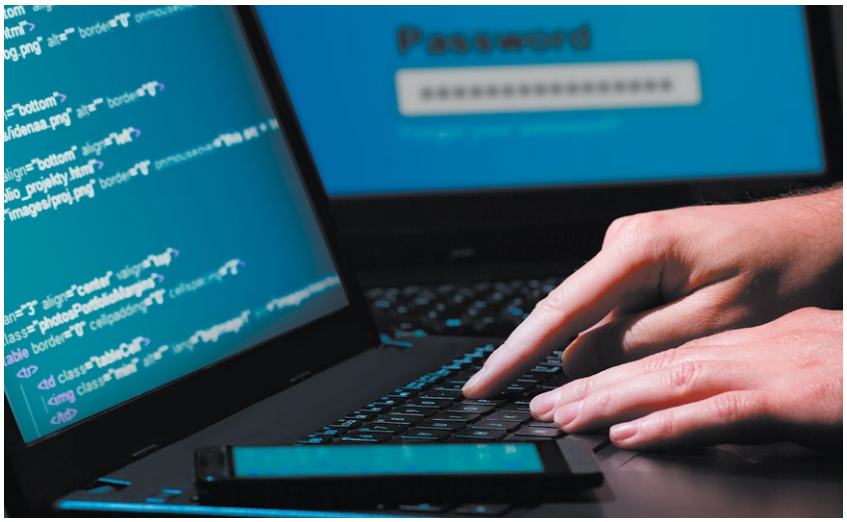
УВЕРЕННОЕ «ИТОГО»

Для успешного обоснования проекта по DLP нужно ответить на 2 основных вопроса: «Зачем нам это нужно?» и «Почему это столько стоит?». Ответ на первый вопрос кроется в понимании узких мест в части информационного обмена: воруют изобретения, уводят клиентов и т.д. Ответ на второй вопрос позволяют получить анализ рынка, выбор решения и интегратора, который будет его внедрять.

По нашему опыту, если есть хотя бы зародыш ответа на первый вопрос (уже случившиеся инциденты, подозрения), можно смело приступать к ответу на второй – подключать опытного интегратора, который поможет с обоснованием проекта перед бизнесом, выбором решения и последующим внедрением, прописыванием регламентов использования и сопровождением системы.

ПРАКТИЧЕСКИЕ СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ВНУТРЕННИМ УГРОЗАМ В БАНКОВСКОМ СЕКТОРЕ

ВСЕВОЛОД ИВАНОВ,
исполнительный директор
компании InfoWatch



С самого момента зарождения решений для защиты от утечек данных (DLP) развитие рыночных требований к продукту пошло у нас и на Западе в двух разных направлениях. В итоге сегодня в европейских компаниях, в том числе финансового сектора, DLP-решения призваны обеспечить соответствие нормам регуляторов (compliance). Такой формальный подход понятен, но не очень интересен, т.к. он не помогает бизнесу, а лишь позволяет соответствовать определенным правилам на бумаге.

Российский же путь развития хотя и учитывал нормы регуляторов, был более ориентирован на потребности бизнеса. В результате сегодня российский рынок DLP включает маленькую часть compliance (например, помогая в выполнении № 152-ФЗ и СТО БР ИББС) и огромную, сложнейшую часть, которая защищает банки уже не только от утечек информации, но и от прочих внутренних угроз, таких как мошенничество, коррупция, сговоры и т.п.

Я бы хотел подробнее остановиться на типичных внутренних угрозах в банках и рассказать о том, какая функциональность DLP-решений позволяет снизить экономические риски, избежать потерь, спасти деньги.

Воровство базы данных клиентов. Разумеется, предотвратить данный инцидент можно даже с помощью базовых технологий DLP, таких как цифровые отпечатки. После внесения базы в список защищаемых документов DLP-решение будет уведомлять офицера безопасности о таких событиях, как пересылка по почте, вывод на печать, копирование на флешку базы данных. Однако сегодня существуют и более сложные технологии анализа, такие как выявление слишком частого обращения к базе данных или выгрузки большого массива БД на жесткий диск. Сами по себе эти события не являются утечкой информации и, следовательно, инцидентом для DLP-системы, однако очевидно, что все это – тревожные звоночки, признаки планируемого нарушения политики безопасности, поэтому современная система должна их учитывать.

Если чаще всего предметом кражи становятся персональные данные (сюда входят и случаи воровства баз данных клиентов), то на втором месте, безусловно, **воровство платежных данных клиентов.** Две эти категории информации обладают наибольшей ликвидностью на черном рынке. Банку потеря этих данных грозит серьезным ущербом: в случае с базой клиентов это их массовый отток к конкурентам, в случае с платежными данными – затраты на эмиссию новых карт, а также огромные репутационные потери.

Сговоры с физическими лицами на получение кредита. Самый частый случай – кредитное мошенничество, при котором инспектор одобряет выдачу кредита человеку, который не должен и не может его получить легальным образом. Например, если кредит пытаются оформить на фальшивый паспорт. Поскольку данный тип мошенничества подразумевает сговор между кредитным инспектором и заемщиком, необходимой мерой противодействия является контроль возможных каналов коммуникации – как служебной, так и личной почты сотрудника банка. Для анализа трафика используются лингвистические возможности решения, так что они должны быть реализованы на высоком уровне. Лингвистические технологии должны не только учитывать и «понимать» словоизменение, опечатки, транслитерацию, но и «знать» специфические термины, часто употребляемые в отрасли. Технология, отвечающая за это, – отраслевая база контентной фильтрации (БКФ), и если банк внедряет решение для защиты от внутренних угроз, он должен убедиться, что эта технология реализована в выбранном продукте на высоком уровне.

Другой вариант описанного типа мошенничества – **сговоры с физическими лицами на получение потребительского кредита.** В этом случае банковский сотрудник выдает кредит подставному лицу, с которым он предварительно вступил в сговор. Покупатель забирает товар, купленный в кредит, перепродает его, делит выручку с кредитным

инспектором и скрывается. По нашему опыту, противодействовать таким ситуациям помогают не только отслеживание и анализ почтового трафика банковских служащих, но и контроль информации на мобильных устройствах. Эти технологии пока только развиваются и есть далеко не во всех решениях, но уже очевидно, что их использование станет настоящим прорывом в области противодействия внутренним угрозам.

Подобным образом решение обнаруживает **сговоры с корпоративными клиентами,** когда менеджер банка за вознаграждение помогает корпоративному клиенту фальсифицировать его отчетность так, чтобы компания могла пройти кредитный комитет и получить финансирование.

Соучастие в преступлениях. Частый сценарий: сотрудник банка, зная, в какой день клиент получит крупную сумму наличных, сообщает об этом грабителям. Преступники, работая по наводке, подстерегают жертву и совершают ограбление. Предотвращение подобных инцидентов также возможно с помощью базы контентной фильтрации, содержащей ключевые слова, употребление которых характерно для лиц, готовящих такое преступление. Сценарий очень типовой, поэтому мы заложили алгоритмы его выявления в универсальную банковскую БКФ, которую предлагаем всем клиентам финансового сектора.

Очень часто наша система используется для обнаружения **внутренних сговоров.** Например, когда началось падение рубля, мы раскрыли ряд мошенничеств в сфере private banking. Утром, якобы по поручению клиента, рубли переводились в доллары, а вечером обратно. При этом на счет клиента возвращалась та же рублевая сумма, а разница шла мошенникам в карман. Наше решение выявило это благодаря лингвистическим технологиям, анализирующим сообщения менеджеров банка в различных мессенджерах и Skype. Поэтому при выборе решения для защиты от внутренних угроз рекомендуется ориентироваться не на общее количество контролируемых каналов передачи данных, а на то, будут ли под контролем все каналы, используемые конкретно вашими сотрудниками.

Аналогичным образом неоднократно выявлялись случаи **коррупции внутри банка, нечестного проведения тендеров, откатных схем. Банковский инсайд** – еще одна серьезная угроза, способная «на пустом месте» нанести серьезный вред. Клиентам сообщается информация, часто ложная, о том, что банк сталкивается с серьезными трудностями. В результате испуганные вкладчики срезают депозиты и уменьшают ликвидность банка. Система для защиты от внутренних угроз перехватывает переписку как с корпоративных, так и с личных ящиков в рабочее время, детектируя фразы, высказывания, свидетельствующие о нарушении.

Сегодня DLP-система предсказывает события. Отметим, что раньше единственным функционалом решений этого класса был контроль или запрет нелегитимной передачи конфиденциальных данных, сейчас же большинство инцидентов связано с раскрытием мошеннических схем, в которых собственно передача конфиденциальных данных не задействована. Именно поэтому мы говорим, что современные системы, и InfoWatch Traffic Monitor в частности, переходят от мониторинга утечек к выявлению и предотвращению всего комплекса внутренних угроз, существующих в каждой компании.

Однако чтобы выявлять **намерения сотрудников** совершить мошеннические действия, решение для защиты от внутренних угроз должно оперировать достаточно сложными технологиями. Для банков мы разработали модель угроз, выстроили алгоритмы возможных видов мошенничества и выделили сопутствующие им признаки, после чего все это было заложено в нашу систему таким образом, чтобы возникновение таких атрибутов интерпретировалось как событие информационной безопасности. Эти технологии уже активно используются заказчиками и успешно выявляют мошенников. Таким образом, в банках решение для защиты от внутренних угроз уже выступает в качестве части антифрод-системы, реагируя на аномалии и заблаговременно предупреждая офицера безопасности о возможных инцидентах.

ОТДЕЛ ИБ КАК СЕРВИСНЫЙ ПРОВАЙДЕР

МИХАИЛ АНОШИН,
руководитель направления DLP
Центра информационной безопасности
компании «Инфосистемы Джет»

Сегодня *aaS – очень модное направление, начиная с аутсорсинга ковриков для прихожей и заканчивая перекладыванием на плечи «провайдера» первой линии разбора инцидентов информационной безопасности. В этой статье речь тоже пойдет об аутсорсинге ИБ, но не о внешнем, а о внутреннем.

Если вы начальник отдела ИБ, то наверняка хоть раз сталкивались с необходимостью доказывать важность и полезность вашего подразделения. Если вы специалист отдела ИБ, то, скорее всего, слышали пожелание руководителя «выловить что-нибудь эдакое», чтобы показать бизнесу, что вы здесь не просто так.

ПОЗИЦИОНИРУЙ ПРАВИЛЬНО

Общаясь с нашими заказчиками, мы видим, что в разных компаниях отношение к информационной безопасности разное. Одна из причин этого – позиционирование. Есть компании, в которых безопасность фактически постоянно борется за существование, т.к. бизнес-подразделением не является, и полезность их работы не так очевидна. Другие же компании не представляют своей жизни без отдела ИБ. Как правило, в них на отдел ИБ завязана работа других подразделений, а иногда и важнейшие бизнес-процессы, напрямую влияющие на основной бизнес. На практике отдел информационной безопасности в таких компаниях является поставщиком внутренних услуг и без него не обойтись. Каких именно услуг? Рассмотрим на примере ИБ-подразделения одной крупной компании.

КАК У ДРУГИХ

В ИБ-отделе этой организации около 7 специалистов. Как правило, за каждым из них закреплено определенное направление (compliance, защита от утечек, защита баз данных, мобильных устройств и др.). У всех этих специалистов есть 2 направления в их ежедневной деятельности – на общее благо ИБ компании (основные задачи) и работа по запросу от других подразделений. Удобнее всего показать внутреннюю сервисную модель работы этого отдела на примере DLP.

> Самые популярные запросы от экономической безопасности: предоставить факт отправки тендерной документации до объявления конкурса, показать наличие активного общения между сотрудниками, отследить «жизненный путь» документа в компании

Так, помимо традиционной работы с системой DLP на предмет контроля коммуникаций и выявления фактов утечек, пользуется спросом предоставление выгрузок об инцидентах для «соседних» подразделений.

DLPAAS ДЛЯ КАДРОВ

Кадровая служба обращается за предоставлением фактов поиска работы и оценкой общей занятости сотрудников. Специалист ИБ готовит выборку (точнее, выполняет заранее заготовленный шаблон запроса) по определенному сотруднику или по всем сотрудникам за определенный период времени. Эта информация помогает HR-специалистам оценить уровень лояльности отдельно взятого сотрудника, понять, насколько эффективно он выполняет свои должностные обязанности, и при необходимости предпринять определенные действия.

Самым популярным запросом HR'ов является поиск бездельников и нелояльных сотрудников. С помощью DLP-системы специалист отдела ИБ в несколько кликов строит отчеты «ТОП пользователей социальных сетей», «ТОП пользователей "аськи"», «Пользователи, занимающиеся поиском работы» и т.п.

DLPAAS ДЛЯ ЮРИСТОВ

Специалисты юридического отдела используют выгрузки из DLP в суде. Причем компания может выступать как ответчиком по иску, так и истцом. Что в первом, что во втором случаях в помощь юристам ИБ-отдел готовит выборку писем, имеющих отношение к рассматриваемому делу.

Один из популярных случаев – подача иска бывшим сотрудником за якобы неправомерное увольнение. Специалист ИБ выбирает из архива переписки те сообщения, которые подтверждают законность увольнения сотрудника. Например, это могут быть факты нарушения установленного режима коммерческой тайны. Специалист ИБ выгружает из DLP 2 сообщения – сам факт отправки конфиденциального файла и подтверждение пользователя, согласно которому он намеренно совершил такую отправку.

DLPAAS ДЛЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Последнее по счету, но чуть ли не первое по важности для компании – это взаимодействие по принципу сервиса между отделом экономической безопасности и отделом ИБ. DLP контролирует коммуникации, что само по себе очень эффективно в плане выявления экономических преступлений – сговора, мошеннической схемы, обхода тендерной процедуры, фактов дачи/получения взяток. В связи с этим отдел ИБ для экономической безопасности является настоящим кладезем информации и фактов инцидентов.

Самые популярные запросы от экономической безопасности: предоставить факт отправки тендерной документации до объявления конкурса, показать наличие активного общения между двумя или группой сотрудников, отследить «жизненный путь» документа внутри компании. Благодаря автоматическому созданию досье как на внутренних, так и на внешних собеседников, система DLP может показать картину сдержанного, официального общения по корпоративной почте и в то же время огромную массу личной переписки по неофициальным каналам обмена информацией.

ВЫГОДЫ: ЭКОНОМИЧЕСКИЕ И НЕ ТОЛЬКО

В рассмотренных примерах без DLP-системы, а значит и без отдела ИБ, интересующие сведения было бы крайне сложно получить: нужны специальные инструменты для их детектирования и, чего боятся больше всего, огромный рутинный труд. Если же подобным вообще не заниматься, велик риск потерь – кадровых, репутационных и финансовых.

При использовании сервисной модели для отдела ИБ все занимаются своим делом, причем эффективно. HR не приходится придумывать, как контролировать отправку резюме, а юрист одним краткосрочным запросом получает доказательную базу по делу. С другой стороны, специалисту информационной безопасности не нужно заниматься выявлением мошенничества и другой непрофильной работой.

В приведенной в качестве примера компании полезность отдела ИБ достойно оценена. Имеется положительный опыт, когда отдел ИБ вместе с другим подразделением получал бюджеты под совместные проекты. В них отдел информационной безопасности выступает «сервисным провайдером», а смежное подразделение – «потребителем сервиса».

Скорее всего, случаи таких взаимодействий встречаются во многих компаниях, остается лишь направить их в правильное русло. Концепция отдела ИБ как «сервисного провайдера» в этом хорошо помогает. JI

DLP В ДЕЛЕ БЕЗОПАСНОСТИ БИЗНЕСА: ИНТЕГРАЦИЯ ТВОРИТ ЧУДЕСА

ЕВГЕНИЙ АКИМОВ,
директор по развитию бизнеса
Центра информационной безопасности
компании «Инфосистемы Джет»

Еще совсем недавно решения класса DLP (Data Leak Prevention) использовались в точном соответствии с их названием – для предотвращения утечки данных. Современная практика использования DLP-систем показывает, что они являются инструментом не столько предотвращения утечек конфиденциальной информации, сколько контроля корпоративных коммуникаций. Выявление лиц, потенциально способных «слить» закрытую информацию внешним контрагентам, обнаружение фактов подозрительных переговоров (ведущихся «не по рангу», чересчур интенсивно и т. п.) – это те функции, которые реально могут выполнять и все чаще выполняют системы DLP. Если эту информацию правильно использовать, получается инструмент скорее экономической, нежели информационной безопасности.

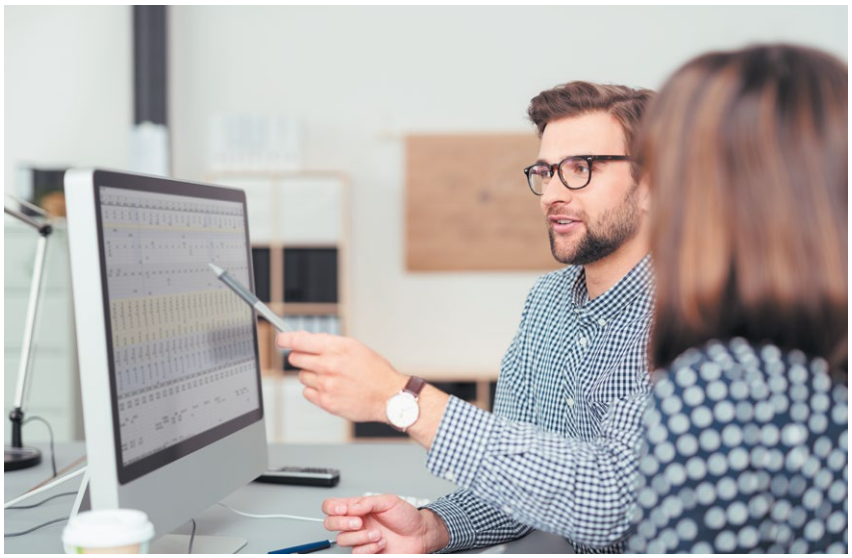
Примеры применения DLP в качестве инструмента экономической безопасности в нашей стране уже есть. Алгоритм обычно таков: служба экономической безопасности подает запрос в службу информационной безопасности, чтобы та подняла архивную переписку определенных сотрудников – по конкретной теме, с конкретными контрагентами и пр. Полученная подборка анализируется вручную. Этот процесс может занимать довольно много времени и не гарантирует своевременности реакции на подозрительную коммуникацию.

Для ускорения процесса его можно автоматизировать. Нужна интеграция систем DLP с другими автоматизированными системами, которые используются службами безопасности, – это дает более ощутимый результат.

SOC и DLP

Интеграция DLP с системами класса SIEM – уже устоявшаяся практика. Она позволяет контролировать события в сети в режиме реального времени, видеть корреляции между разными типами событий и выявлять уязвимые точки. Поскольку SIEM-система содержит архив записей о событиях (логов), совместная работа DLP и SIEM позволит при необходимости восстановить историю событий, что бывает необходимо, например, в случае служебного расследования.

Набирает популярность интеграция DLP с аналитическими (BI) системами, в частности с системами, которые все чаще называют Security Intelligence или Security BI. Эти относительно недавно появившиеся аналитические системы адаптированы конкретно под задачи безопасности. В отличие от SIEM-систем, которые работают только с логами, системы Security Intelligence работают с любыми видами информации, они не ориентированы на выдачу алертов в режиме реального времени, но позволяют выявлять тенденции и строить прогнозы.



DLP для задач HR

Получая информацию от DLP, система Security Intelligence позволяет, например, делать выводы о настроениях в коллективе. Предположим, руководство компании задумало провести организационные изменения. Мониторинг коммуникаций сотрудников в сочетании с аналитическими функциями даст возможность выяснить отношение разных групп сотрудников к грядущим изменениям, увидеть каналы и источники распространения негатива (или, наоборот, позитива) в коллективе. Результаты анализа позволят, например, определить, с кем из сотрудников стоит провести индивидуальную работу, какие можно предложить компенсационные меры и т. д. Лояльность сотрудников – один из важнейших факторов экономической безопасности, поэтому пренебрегать информацией о настроениях в коллективе не стоит.

DLP и контроль контрагентов

Перспективное направление – интеграция DLP с автоматизированными системами проверки и контроля контрагентов. Реализованных проектов в этой области пока нет, но многие компании рассматривают такую возможность. Автоматизированные системы проверки контрагентов исполь-

зуются крупными организациями, работающими с большим количеством поставщиков и подрядчиков. Привлекая и анализируя данные из реестра юридических лиц, учредительных документов, различную коммерчески доступную информацию о компаниях, такая система позволяет сделать выводы о надежности подрядчика, его законопослушности, компетенциях и пр.

Что может привнести в проверку контрагентов система DLP? Рассмотрим пример из жизни.

Строительная компания закупила противоморозную присадку для бетона у поставщика, победившего в тендере. После возведения нескольких этажей здания выяснилось, что качество бетона не соответствует стандартам, хотя все документы на продукцию были в порядке. На каком этапе и каким образом произошел обман? Что было упущено? Строительная компания смогла это выяснить задним числом, проанализировав учредительные документы поставщика – владелец бизнеса оказался родственником топ-менеджера строительной компании, он заранее знал о тендере и успел «подготовиться».

Понятно, что факт родственных связей автоматизированная система далеко не всегда может установить – доступных реестров с такой информацией нет. Однако если бы система проверки контрагентов была интегрирована с системой DLP, компания смогла бы, как минимум, зафиксировать факт коммуникаций топ-менеджера с одним из потенциальных участников тендера и поинтересоваться их содержанием. Напомним, что DLP-система может контролировать не только почтовую переписку, но и мессенджеры, активность в соцсетях и даже некоторые виды голосовых коммуникаций – все каналы

обмена информацией, какими сотрудник пользуется с корпоративного терминала. Интенсивность коммуникаций, период их ведения, статус и полномочия участников коммуникаций – автоматизированное сопоставление этих факторов позволит службе экономической безопасности своевременно обнаруживать ситуации, потенциально способные нанести компании вред.

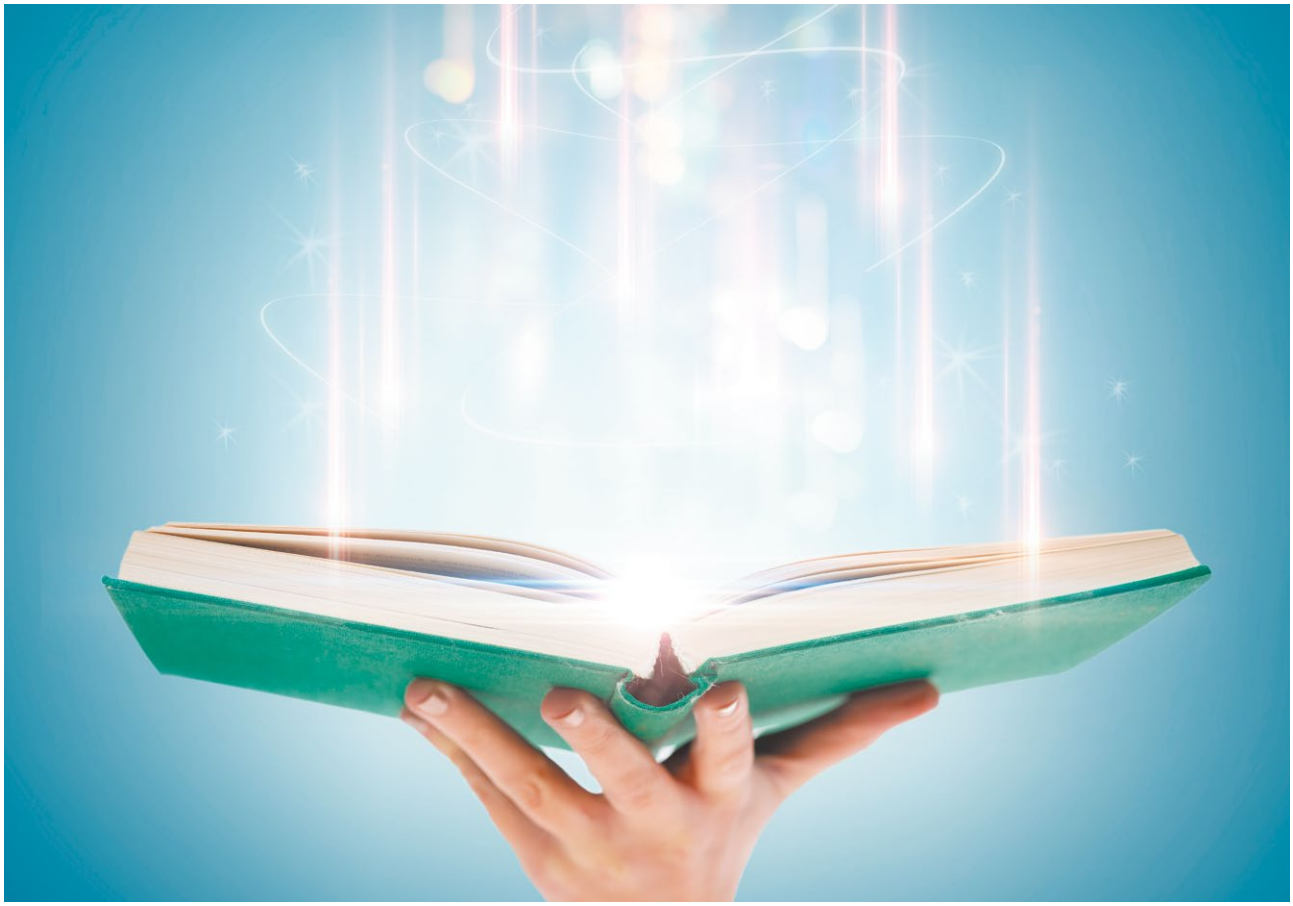
DLP ПРОТИВ «ЛЕВЫХ» ДОХОДОВ

Более сложные сценарии анализа можно задавать при подключении к комплексу HR-системы. В этом случае можно задать круг сотрудников, чьи коммуникации с контрагентами подлежат контролю в том или ином случае – исходя из должности, круга обязанностей, занятости в конкретном проекте и т. д. На конференции, посвященной корпоративной безопасности, руководитель службы экономической безопасности одной из компаний-участниц рассказал, как он проверяет менеджеров на предмет получения «нечестных доходов» – он следит за их тратами. Делается это от случая к случаю, да и пока менеджер среднего звена не приедет на работу на новеньком «порше», факт открытия офшора «сватом или братом» отследить сложновато. Хорошим подспорьем в такой работе может быть анализ коммуникаций людей, находящихся на определенных должностях (эти данные извлекаются из HR-системы) с потенциальными или уже состоявшимися контрагентами.

РЕЗЮМЕ: DLP В НОВОМ КАЧЕСТВЕ

Противодействие утечкам – не единственная функция DLP и даже не всегда основная: сегодня при использовании этих систем функция Data Leak Prevention зачастую отходит на второй план. Система DLP все чаще рассматривается как инструмент работы не столько с информацией, сколько с людьми. Для этого эффективно ее использовать с связке не только с SIEM (это уже классика жанра), но и с Security BI, с системами проверки контрагентов, с HR-системами, а в дальнейшем и с антифрод-системами. Можно ожидать, что это даст DLP-решениям второе дыхание и позволит обеспечивать безопасность бизнеса на уровне, до сей поры недостижимом. JI

ПРОСТАЯ МЕТОДИКА ПРИНЯТИЯ РЕШЕНИЯ ПО ИНЦИДЕНТАМ, ВЫЯВЛЕННЫМ DLP



АНДРЕЙ ТИМОШЕНКОВ,
руководитель направления Solar Dozor
компании Solar Security

DLP-системы или их упрощенные аналоги (системы контроля работы сотрудников) используются во многих организациях, обеспокоенных угрозой утечки информации или инцидентами экономической безопасности. При этом стоит отметить, что эффективность мониторинга и контроля зависит не только от технического решения и его настроек, но и от процедуры управления инцидентами, принятой в компании.

Выявлять и расследовать инциденты не сложно – современные DLP-системы обладают функционалом, позволяющим существенно упростить подобные задачи:

- механизмом контентного и контекстного анализа;
- архивом всей переписки и возможностью построения сложных поисковых запросов;
- интерактивными графами связей (сообщений) между сотрудниками;
- механизмами оценки «Уровня доверия» и «Досье» на сотрудников;
- и др.

Гораздо сложнее принять решение о том, что делать с конкретными нарушителями, какие меры взыскания можно применить и почему. Мы предлагаем использовать простую модель принятия решения, о которой и расскажем в этой статье.

Для того чтобы понять, что делать по каждому конкретному инциденту, по которому мы установили нарушителя правил обработки и хранения информации, мы предлагаем ответить на 5 простых вопросов. А точнее, выбрать один из вариантов ответа и в дальнейшем просуммировать баллы. Вопросы и варианты ответов на них представлены в табл. 1.

Условно мы можем разделить инциденты на 3 группы по степени критичности (см. табл. 2).

Вопрос	Варианты ответа и баллы		
Базовая корреляция	Крупный **6**	Неизвестно или пока ущерба нет, но может быть в ближайшем будущем **3**	Ущерба нет и, скорее всего, не будет **1**
Поведенческий анализ	Да **3**	Неизвестно, умысел не очевиден **1**	Нет, инцидент произошел по ошибке или невнимательности **0**
Корреляция сессии событий	Низкий. Сотрудника знаем плохо, это новый или временный сотрудник, сотрудник на увольнении или «на особом контроле» **3**	Обычный **1**	Высокий **0**
Обогащение данных из других систем	Да **2**	Нет (в системе DLP не зафиксировано) **0**	
Историческая корреляция	Высокая **3**	Средняя (скорее нет, маловероятно) **1**	Низкая **0**
Итого баллов (сумма)			

Табл. 1. Вопросы и варианты ответов на них

Группа	Сумма баллов	Уровень критичности инцидента	Принятие решения
А	1–5	Низкий	Сотрудник ИБ
Б	6–12	Средний	Руководство и отдел персонала
В	13–17	Высокий	Руководство и отдел персонала, юристы и сотрудник ИБ

Табл. 2. Группы инцидентов по степени критичности

Группа А

Если общая сумма баллов от 1 до 5, сотрудник подразделения информационной безопасности может самостоятельно выбрать один из вариантов воздействия:

1. **Перевести сотрудника в группу «особого контроля» и более пристально контролировать его каналы коммуникации.**
2. **Запросить объяснительную у сотрудника и/или его руководителя.**
3. **Провести профилактическую беседу с сотрудником и/или его руководителем.**

Группа Б

Если общая сумма баллов от 6 до 12, по согласованию и при взаимодействии с руководством компании и сотрудниками отдела персонала можно:

4. **Лишить благ и привилегий** (в том числе расширенных прав доступа).
5. **Применить дисциплинарное взыскание в виде замечания или выговора** (ТК РФ ст. 192). При этом следует строго соблюдать порядок применения дисциплинарных взысканий (ТК РФ ст. 193).

Группа В

Если общая сумма баллов от 13 до 17, стоит рассмотреть варианты более строгих наказаний:

6. **Принять решение об увольнении по инициативе работника или по соглашению сторон** (ТК РФ ст. 80 и 78).
7. **Применить дисциплинарное взыскание в виде увольнения по соответствующим основаниям.** Например, за разглашение охраняемой законом тайны (ТК РФ ст. 81 п. 6).
8. **Принять решение о возмещении ущерба за счет сотрудника.** Обратите внимание, если прямой действительный ущерб превышает средний месячный заработок работника, для его возмещения необходимо судебное решение.
9. **Принять решение об уголовном преследовании нарушителя.** Здесь необходимо подготовить заявление в МВД России (в некоторых случаях в ФСБ России) и в дальнейшем активно помогать следственным действиям.

Обычно специалист по информационной безопасности не может принимать соответствующее решение самостоятельно и должен обосновывать и согласовывать его с руководством организации, юристами и специалистами отдела персонала.

Отдельно отметим, что выбор решений с 5-го по 9-е предполагает наличие в организации зрелой системы «бумажной безопасности»: должны быть определены и документированы перечень информации ограниченного доступа, правила обработки и хранения такой информации, базовые правила защиты информации (например, парольной защиты и допустимого использования систем и сервисов). Если в организации обрабатывается информация, составляющая коммерческую тайну, должен быть реализован соответствующий режим (по № 98-ФЗ «О коммерческой тайне»). Это необходимо, для того чтобы минимизировать юридические риски возможных судебных тяжб с работником.

А как же система DLP? Может ли она помочь при определении уровня критичности инцидента? Конечно, и по нашему мнению, современная система DLP обязана это делать. Покажем, как это реализовано на примере решения Solar Dozor, совместив 5 вопросов предлагаемой нами методики с функционалом продукта.

ВОЗМОЖНОСТИ СИСТЕМЫ SOLAR DOZOR

Какова величина ущерба от того или иного инцидента?

При условии, что в организации настроен процесс управления рисками, ответить на этот вопрос аналитику ИБ помогает реализованная в Solar Dozor инцидентная модель расследования нарушений политики безопасности. Администратор может создавать политику с возможностью генерирования так называемых

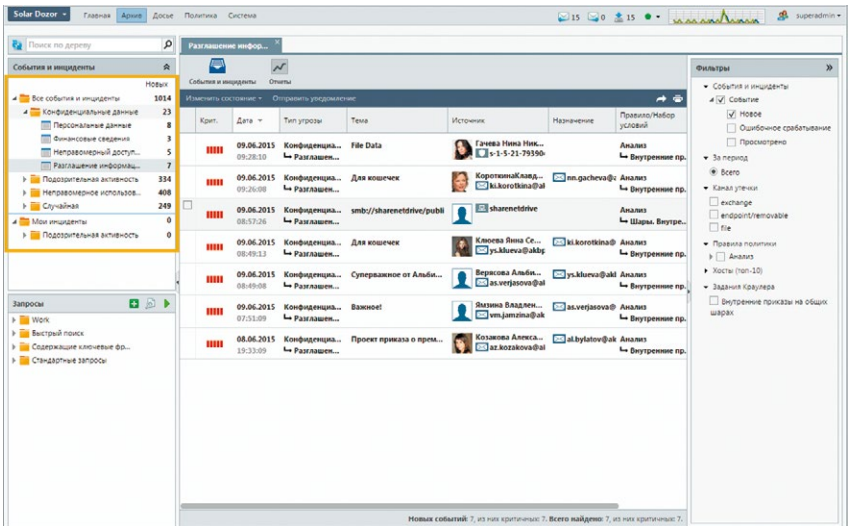


Рис. 1. Пример анализа архива коммуникаций сотрудника

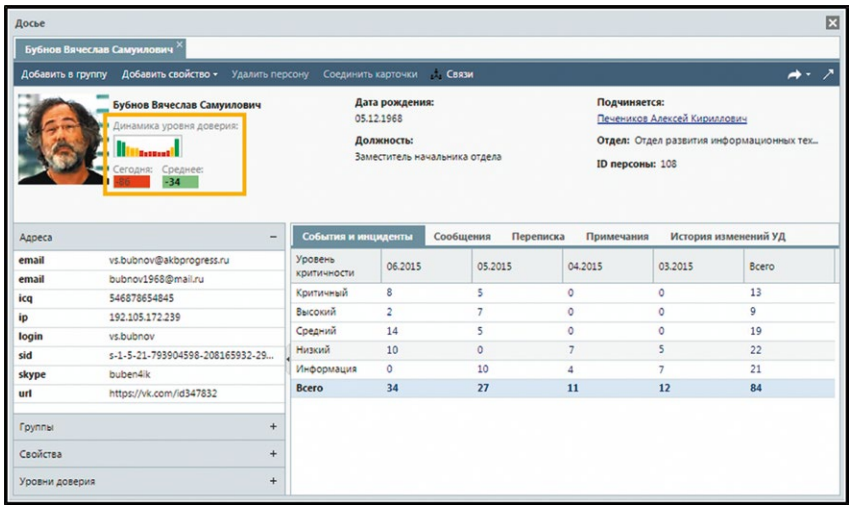


Рис. 2. Карточка досье персоны, хранящая всю необходимую информацию

событий ИБ и интерпретировать собранные события, автоматически соотнося их с определенным типом угроз, актуальным для организации. Зная тип угрозы, специалист может оценить её приоритет и ущерб, который она может принести.

Выявлен ли умысел сотрудника?

При расследовании того или иного инцидента аналитик службы ИБ в первую очередь обязан в кратчайшие сроки установить круг подозреваемых лиц и постараться определить, произошел ли инцидент случайно, так сказать, по недосмотру, или же он стал следствием осознанного, целенаправленного и, что еще хуже, систематического нарушения политик информационной безопасности компании. На данном этапе огромным подспорьем в работе аналитика будет являться реализованная в Solar Dozor возможность многофакторного анализа архива коммуникаций сотрудников (см. рис. 1).

Помимо этого, аналитик ИБ имеет возможность напрямую из окна инцидента просматривать досье всех участников коммуникации и по данным «Досье» строить в графическом интерфейсе граф переписки той или иной персоны, выявляя круг неформального общения, проводить поиск неявных связей, выявлять скрытые связи между людьми, устанавливая в конечном счете круг причастных лиц.

Каков уровень доверия к сотруднику?

Определить уровень доверия к сотруднику буквально в один клик помогает одноименный функционал в Solar Dozor. Дело в том, что изначально все персоны и адреса в Solar Dozor имеют числовой показатель «Уровень доверия». Он создается автоматически на основе статистики нарушений и позволяет находить и выявлять явных и скрытых нарушителей, проводить поведенческий анализ, а также определять соответствие поведения сотрудников правилам компании.

Для персон и адресов считаются среднее значение (среднее арифметическое) и стандартное отклонение (среднеквадратическое) уровня доверия за последние 30 дней.

Были ли у сотрудника инциденты до этого?

Опираясь на функционал «Досье», аналитик безопасности может видеть сводную информацию по истории всех произошедших инцидентов того или иного сотрудника по уровням их критичности. Тем самым в один или два клика он может ответить на четвертый вопрос предлагаемой нами методики.

Какова вероятность, что инцидент у этого сотрудника повторится?

Данный вопрос, пожалуй, является самым сложным, ответить на него можно только экспертно, опираясь как на совокупность выявленных фактов о деятельности сотрудника (история его нарушений, уровень доверия к нему и т.п.), так и на контекст инцидента (например, круг вовлеченных лиц и скрытые связи внутри организации).

Таким образом, опираясь на предлагаемый в Solar Dozor функционал, аналитик службы безопасности может осуществлять глубокий анализ и расследование инцидента, в том числе на основе выявленных системой внутренних взаимосвязей между участниками подозрительной коммуникации (как внутри компании, так и вовне). Результат этой работы – эффективное расследование и классификация инцидента ИБ, выявление причастного к нему круга лиц.

ЗАКЛЮЧЕНИЕ

Конечно, если эта модель кажется вам слишком простой, вы всегда можете усложнить и адаптировать ее под контекст конкретной организации. Для этого может быть пересмотрен перечень вопросов и/или весовых значений ответов на них. Однако, по нашему опыту, представленная модель является достаточно удобной и сбалансированной. Поэтому рекомендуем ориентироваться именно на нее.

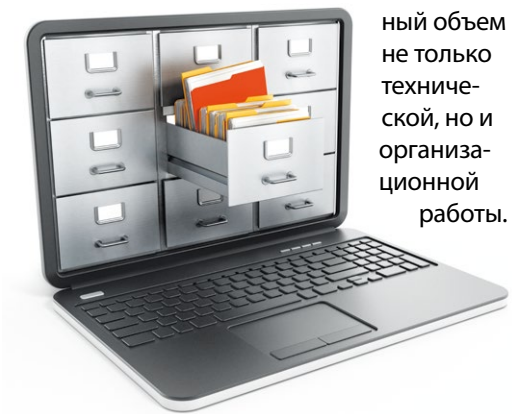
DLP: СИНЕРГИЯ ТЕХНИКИ И ПСИХОЛОГИИ

Мне сверху видно все – ты так и знай.
Из известной песни

ВАСИЛИЙ ОКУЛЕССКИЙ,
начальник отдела защиты информации,
«Банк Москвы»

Для банка DLP – одна из трех-четырех систем, иметь которую необходимо. Вопрос – для чего или, вернее, как ее правильно использовать. В свое время, когда на российском рынке появилась технология, позиционировавшаяся как средство контроля сотрудников и предотвращения утечек информации, она вызывала большой энтузиазм. Но на поверку все оказалось не так просто.

Чтобы DLP-система могла предотвращать утечки информации, она должна быть установлена в разрыв сети. Но такая схема чревата блокированием всего потока информации, и крупнейшие банки принципиально этого не делают, считая, что надежность важнее безопасности. Есть и другая сложность: чтобы система могла с высокой достоверностью фильтровать информационный поток и автоматически определять, какое сообщение нужно заблокировать, а в каком случае достаточно предупредить пользователя, системе должны быть заданы очень четкие правила. Для задания правил можно, например, использовать интеграцию с системой документооборота. Однако это предполагает принципиальное изменение существующей системы документооборота: во-первых, документ не должен содержать ничего лишнего – только «квант» нужной информации, во-вторых, все документы должны быть маркированы, учтены, для них должны быть прописаны регламенты хранения, распространения и т. д. Это колоссальный объем не только технической, но и организационной работы.



Изменение системы документооборота требует в буквальном смысле революции в сознании, но большинство организаций в нашей стране пока не являются настолько зрелыми, чтобы эту революцию осуществить.

DLP-система, поставленная не в разрыв сети, выполняет функцию Data Leak Prevention не напрямую – она не совершает никаких действий с выявленными событиями, лишь собирает информацию о них и производит первичную фильтрацию. Совершать действия должен человек – администратор безопасности, руководитель подразделения и т. д.

Вопрос – как человек должен реагировать, что делать с нарушителем? Чтобы предъявить ему формальную претензию, информации об инциденте нужно придать юридическую силу, а для этого выполнить ряд дополнительных процедур (например, непосредственно на рабочем месте сотрудника актом зафиксировать факт использования служебного компьютера для личной переписки). Человеку, уполномоченному принимать решения по инцидентам, должно быть понятно, какие нужны процедуры, как можно распорядиться информацией, полученной из DLP-системы, в рамках существующих законов и нормативов. Должны существовать регламенты реагирования, типовые сценарии. Люди задумываются об их выработке уже после внедрения DLP, и это следствие того, что DLP неправильно позиционируется на рынке.

DLP не следует рассматривать как самостоятельное законченное техническое решение. Этот инструмент должен быть частью комплексной системы обеспечения безопасности, включающей технические средства, организационные мероприятия, нормативное обоснование. Именно в таком виде DLP-решение должно предлагаться заказчикам.

КУЛЬТУРА БЕЗОПАСНОСТИ ИЛИ DLP-МОДУЛЬ «СЕКРЕТАРША»

Итак, если DLP не занимается прямым предотвращением утечек, то для чего она нужна? Ответ: для того, чтобы дисциплинировать сотрудников.

Любой уважающий себя банк заботится о том, чтобы мотивировать сотрудников к соблюдению правил информационной безопасности с первых дней работы. В первую очередь проводится подробный инструктаж, после чего сотрудник подтверждает своей подписью знакомство с правилами безопасности. Но одного инструктажа недостаточно, сотрудников нужно постоянно держать в тонусе. В Банке Москвы, например, разработаны веб-курсы, посвященные правилам работы с информацией – их все сотрудники проходят ежегодно. Прохождение веб-курсов завершается зачетом, результаты которого учитываются при начислении годовой премии.

Но и регулярным обучением ограничиваться не стоит. Нужно создавать в организации атмосферу, способствующую развитию самоконтроля сотрудников. По статистике, 80% утечек конфиденциальной информации допускаются людьми случайно – по рассеянности, недомыслию и пр. Чтобы этого не происходило, в голове у человека должен быть «стоп-кран», который не позволит писать лишнего в соцсети или откровенничать не с теми людьми. «Стоп-кран» будет работать, если сотрудникам постоянно напоминать, что их действия находятся под контролем. В этом как раз и поможет DLP-система.

Во-первых, сотрудники должны знать, что DLP-система в организации есть – так же как и видеонаблюдение, и другие средства безопасности. Во-вторых, результаты ее работы должны периодически становиться известны коллективу. Для этого совершенно не обязательно доводить дело до увольнения

провинившегося сотрудника, а тем более до судебного разбирательства: выговор с лишением премии действует на коллектив доходчивее. А вот как донести эту информацию до коллектива – вопрос изобретательности руководителя. Можно устроить виновнику инцидента публичную выволочку. А можно – шепнуть секретарше, что такого-то застукали за недозволенными действиями в сети и теперь лишают премии. Секретарский корпус – это своего рода сеть распространения неофициальной информации в организации. Так что можно быть уверенным, что информация о проступке и его последствиях вскоре будет известна всем сотрудникам. Психологический эффект получается очень хороший.

КРИТЕРИИ ВЫБОРА

Рассматривая возможность покупки чего-нибудь, принято подсчитывать экономический эффект: когда и сколько будет прибыли/экономии на рубль затрат. Однако эффект от наличия системы безопасности определяется не рублями, а самим существованием этой системы. Есть вещи, без которых бизнес просто не может функционировать, информационная безопасность – одна из таких вещей для банка. Говорить об «экономике» того или иного DLP-решения бессмысленно. Безопасность – это стратегия и стиль работы организации, которые позволяют сотрудникам и руководству чувствовать себя уверенно. Хотя, возможно, экономически обосновать внедрение DLP могла бы организация, обладающая некими ноу-хау, утечка которых может свести на нет конкурентные преимущества.

Для DLP (как и для любого другого решения по информационной безопасности) критерием выбора является не стоимость, а степень удобства работы пользователей. Решение не должно

им мешать! Важно, чтобы DLP-система не затрудняла выполнение сотрудниками штатных операций и не тормозило работу прикладного ПО. Если вам предлагают очень хорошую (отлично себя зарекомендовавшую) систему, которая рассчитана на современные рабочие станции и конкретные версии антивируса, а в вашей инфраструктуре «зоопарк», – не берите. Если предлагают недорогую («выгодно!») систему, которая заставляет сотрудника долго ждать загрузки рабочей программы, – ни в коем случае не берите. Не прямо, но косвенно удобство работы пользователей сказывается на общей эффективности работы организации.

ЕЩЕ РАЗ О ПРАКТИЧЕСКОМ ЭФФЕКТЕ

Кто-то может спросить: а зачем вообще тратиться на DLP-систему? Может, просто заняться воспитанием сотрудников, повышением их лояльности? Или застраховать свои риски? Да и какую информацию можно увести у банка? Базу клиентов? А смысл? Если банк хорошо работает, клиенты все равно останутся с ним, если плохо – и так уйдут.

На это можно ответить, что в банке есть конфиденциальная информация, утечка которой, возможно, не нанесет прямого материального ущерба, но нанесет ущерб репутации. Очевидный пример – персональные данные. Контроль их отправки внешним адресатам – постоянный процесс.

Случаются попытки отправки конфиденциальных документов. В Банке Москвы такая попытка была выявлена вскоре после установки DLP-системы. Была реакция, и впредь попытки не повторялись.

Когда DLP работает в комплексе с другими системами, это дает синергетический эффект. В нашем случае комплексная система позволила обнаружить подложные письма, содержащие троян. Антивирус реагировал на них только после того, как получатель открывал письмо. Комплекс, включающий DLP, делал это раньше.

DLP-система будет тем эффективнее, чем лучше проработаны организационные вопросы – подготовлены и занесены в базу данных контентной фильтрации шаблоны документов, налажена регулярная подготовка отчетов, проработаны алгоритмы реакции на инциденты, организована обратная связь для администраторов системы. Совершенствование и адаптация DLP-системы – процесс постоянный и непрерывный.

ПОДВЕДЕМ ИТОГ

Опыт говорит о том, что DLP – система полезная, а для многих организаций даже обязательная. Но не стоит ожидать от нее чудес – технология сама по себе не решит за администратора/руководителя все проблемы. Это всего лишь инструмент, которым человек либо сумеет грамотно воспользоваться, либо нет. Извлечь максимум пользы из DLP поможет в первую очередь тщательная организационная проработка процессов, в которых система задействована. А также – творческий подход к использованию полученных результатов.

DLP КАК ПАЗЛ, КОТОРЫЙ ДОЛЖЕН СЛОЖИТЬСЯ

О практике использования DLP-решения беседуем с **Алексеем Фроловым, руководителем Департамента по безопасности и режиму ПАО «Корпорация Иркут»**

J.I.: Давно ли используется в корпорации система DLP? Что послужило мотивом к ее внедрению?

А.Ф.: Первая версия решения появилась у нас почти 10 лет назад. Хотя тогда оно еще не было DLP-системой (тема DLP в ту пору вообще не поднималась), это было средство контроля контента почтового трафика. В процессе развития решения, выхода новых версий, подключения дополнительных модулей оно превратилось в ядро нашей системы DLP, которая позволяет анализировать и контролировать различные виды трафика с единой консоли и с использованием единых политик. Сейчас весь трафик, который может содержать какую-либо конфиденциальную информацию, контролируется DLP-системой.

Наша система DLP в ее нынешнем виде – результат многолетней работы. Безопасность складывается из множества элементов – как пазл. Думаю, мы близки к тому, чтобы в корпорации этот пазл сложился.

J.I.: Как принимается решение о внедрении того или иного модуля, функционала? Вы как-то оцениваете точки риска?

А.Ф.: Конечно, мы понимаем существующие угрозы и риски, знаем, где у нас есть слабые места. Исходя из этого решаем, что нам больше всего нужно в данный момент.

К теории риск-менеджмента мы не прибегаем, а принимаем решения на основании внутренней экспертизы в организации. Наши работники хорошо ориентируются и в своей области деятельности, и в делах компании в целом. Они понимают, что важно для компании и какой участок нуждается в контроле.

J.I.: Каков алгоритм работы с DLP-системой? Получают ли какие-то оповещения рядовые пользователи, или это инструмент исключительно для руководителей?

А.Ф.: Оповещения о событиях система выдает в режиме онлайн специалистам по безопасности. Дополнительно уведомления дублируются на рабочие станции нескольких руководителей, поскольку компетенций одного человека зачастую недостаточно, чтобы рассмотреть их все. Каждое событие анализируется, и если выясняется, что это заслуживаю-

щий внимания инцидент, он эскалируется руководителю более высокого уровня для принятия дальнейших управленческих решений. Есть и такие, которые заслуживают полноценного служебного расследования и серьезных мер дисциплинарного воздействия.

В целях предотвращения случайных утечек информации в действия работника внесены элементы осознанности – он должен подтвердить, что хочет сделать именно это. Если система подозревает попытку отправить конфиденциальную информацию, она задерживает письмо и сообщает об этом работнику.

Работа системы дает реальные результаты, многие неприятные ситуации нам удалось предотвратить.

J.I.: Вы сказали, что безопасность в компании – это пазл, который должен сложиться. Значит должна существовать интеграция между подсистемами безопасности – элементами «пазла». С какими информационными системами интегрируется DLP?

А.Ф.: В корпорации используется широкий набор средств безопасности, каждое из них – самостоятельный продукт со своим функционалом, своей консолью управления и системой отчетности. Агрегировать текущую информацию из всех систем, чтобы построить оперативный отчет вручную – трудоемкая задача. Для этого мы создали специализированную BI-систему, одним из источников которой является DLP-система. BI-система используется как агрегирующая среда контроля состояния элементов информационной безопасности.

Таким образом мы получаем наглядную картину состояния безопасности в корпорации. Для высшего руководства разработан специальный интерфейс, отображающий общий уровень безопасности в целом по организации. Система находится в постоянном развитии, каждый новый инструмент обеспечения безопасности будет в обязательном порядке интегрироваться с ней.

J.I.: Кто пользуется этой системой в корпорации? Это только ваш департамент?

А.Ф.: Созданная модель пока охватывает только вопросы безопасности. Однако в системе предусмотрен мандатный доступ к информации, и мы предполагаем предоставить ее и ИТ-специалистам – в части, касающейся их области ответственности. Учитывая, что система агрегирует информацию от СКУД корпорации, планируется открыть ее для руководства отдела кадров, а в перспективе, думаю, доступ к информации BI-системы получат и руководители подразделений корпорации, которые смогут лучше контролировать своих работников.

> Разработчикам DLP-систем стоит уделить больше внимание различным механизмам контроля форм представления информации. Например, один и тот же документ можно отправить либо в текстовом формате, либо в виде скана pdf или jpg – и все это должно одинаково хорошо контролироваться. Сейчас попытки контролировать отправку картинок приводят к большому количеству ложных срабатываний

J.I.: Как, на основании чего вы оцениваете эффективность работы средств безопасности, в частности системы DLP? Существуют ли какие-то критерии?

А.Ф.: BI-система как раз и выполняет эту функцию. Мы провели большую аналитическую работу и ранжировали вклады источников данных в итоговый уровень безопасности. Так была создана система KPI, которая нашла свое отражение в интерфейсе BI-системы.

J.I.: Какого функционала DLP вам не хватает, что хотелось бы получить от разработчиков?

А.Ф.: Большие потоки информации ежедневно вливаются

в корпоративную сеть и снижают уровень ее защищенности. В связи с этим было бы уместно контролировать информацию по контексту и типам приложений.

Разработчикам DLP-систем стоит уделить больше внимание различным механизмам контроля форм представления информации. Например, один и тот же документ можно отправить либо в текстовом формате, либо в виде скана pdf или jpg – и все это должно одинаково хорошо контролироваться.

Сейчас попытки контролировать отправку картинок приводят к большому количеству ложных срабатываний. Зачастую система не может отличить снимок домашнего питомца в графическом файле от скриншота чертежа. Похожая проблема возникает с отслеживанием рассылки официальных писем организации. Официальный бланк – это картинка. Подписывать письмо на официальном бланке уполномочен ограниченный круг руководителей. Если письмо подписывает другое лицо – это должностное нарушение, мы должны это отслеживать и пресекать. Но сделать это проблематично. Модуль цифровых отпечатков в своем нынешнем виде тут слабый помощник.

Нередко в подписи электронных писем и в «подвалы» текстовых документов автоматически вставляется дисклеймер, сообщающий, что письмо может содержать конфиденциальную информацию. Содержимое письма или вложения таковой не содержит, но DLP-система все равно реагирует на такие письма, опять же порождая множество ложных срабатываний. Как научить систему правильно реагировать на такие письма, пока не ясно.

J.I.: Замечаний довольно много…

> К теории риск-менеджмента мы не прибегаем, а принимаем решения на основании внутренней экспертизы в организации. Наши работники хорошо ориентируются и в своей области деятельности, и в делах компании в целом. Они понимают, что важно для компании и какой участок нуждается в контроле

А.Ф.: Скорее пожеланий. В целом мы DLP-системой довольны, в сочетании со всей «обвязкой» она доказала свою эффективность и результативность. Единственное неудобство – большое количество «ручного труда» по анализу ее уведомлений. Обойтись без него пока не получается. Хотелось бы, чтобы DLP-система стала более интеллектуальной и могла взять на себя еще большую долю первичного анализа информации.

J.I.: Была ли у вас практика юридического использования результатов работы DLP? Позволяют ли настройки политик учитывать требования законодательства?

А.Ф.: В корпорации проводится работа по каждому инциденту. Результатом ее является нахождение виновного и принятие решения о мерах дисциплинарного воздействия. До суда дело ни разу не доходило, но увольнения были.

Режим коммерческой тайны в корпорации установлен. Разработан ряд нормативных документов, которыми мы руководствуемся в работе со средствами DLP.

Если говорить об отношениях с другими компаниями, то со всеми, с кем мы работаем, имеется соглашение о неразглашении (Non-Disclosure Agreement, NDA), и мы следим, чтобы информация, которой мы с ними обмениваемся, обрабатывалась по условиям этого соглашения.

J.I.: Алексей, большое спасибо за беседу!

В ГЛАВНОЙ РОЛИ – DLP

Почему работа с DLP-системой напоминает просмотр сериала «Санта-Барбара», повлиял ли экономический кризис на типы и количество выявляемых в компаниях инцидентов, успевают ли технологии за изобретательностью современных нарушителей.
Эти и другие аспекты жизни DLP-решений в компаниях мы обсудили с Анатолием Скородумовым, заместителем директора, начальником отдела информационной безопасности Банка «Санкт-Петербург», и Константином Коротневым, менеджером по информационной безопасности компании «Эльдорадо».

АНАТОЛИЙ СКОРОДУМОВ, заместитель директора, начальник отдела информационной безопасности Банка «Санкт-Петербург»

J.I.: Коллеги, как выстроен процесс работы с DLP-системой в вашей компании, какие подразделения в нем участвуют?

Анатолий Скородумов: DLP в нашей организации применяется в режиме Prevention, поэтому «используют» DLP-систему все подразделения банка. Любому сотруднику может прийти уведомление, что он выполняет определенные действия, которые нарушают существующую политику информационной безопасности организации. Дополнительно соответствующая информация будет направлена его руководителю.

Константин Коротнев: DLP-система контролирует передачу информации. В случае обнаружения попыток несанкционированной передачи конфиденциальных данных генерируется инцидент ИБ и происходит оповещение заинтересованных сотрудников. Впоследствии инцидент расследуется и в отношении нарушителей политики ИБ применятся дисциплинарные меры.

J.I.: С какими системами интегрировано DLP-решение в вашей компании, есть ли среди них специфические, отраслевые системы?

Константин Коротнев: DLP интегрировано с системой сбора информации о событиях Splunk. Это позволяет, используя язык поисковых запросов, коррелировать события, генерируемые различными средствами защиты, и осуществлять необходимую при расследовании инцидентов ИБ выборку.

Анатолий Скородумов: Для «понимания» структуры организации система DLP интегрирована с MS AD. Необходимости интеграции DLP с бизнес-приложениями на данный момент мы не видим.

J.I.: Каким образом в вашей компании измеряется эффективность DLP-решения?

Константин Коротнев: У нас внедрена система управления ИБ, сертифицированная на соответствие международному стандарту ISO 27001:2013. Для каждого процесса управления ИБ определены KPI, на основании которых оценивается его эффективность. При оценке экономической эффективности той или иной системы ИБ производится сравнение денежного выражения рисков ИБ, которые снижаются с ее помощью, с затратами на ее приобретение и эксплуатацию.

Анатолий Скородумов: Эффективность DLP-решения оценить достаточно сложно. У руководства банка есть понимание, что утечка данных несет в себе серьезные финансовые и репутационные риски и применение средств защиты от утечек необходимо. Доверие клиентов бесценно, и банк прилагает серьезные усилия и тратит значительные ресурсы для его сохранения.

КОНСТАНТИН КОРОТНЕВ,
менеджер по информационной безопасности компании «Эльдорадо»

J.I.: Существует ли у вас практика юридического использования результатов работы DLP-системы? Если да, с какими трудностями вы сталкивались на этом пути?

Константин Коротнев: Практика юридического использования имеет место. В большинстве случаев сотрудники признают наличие инцидента и нарушение политики ИБ, конструктивно воспринимая применяемые к ним меры.

Анатолий Скородумов: На данный момент у нас в организации такая практика отсутствует.

J.I.: Изменились ли типы и количество инцидентов в связи с экономическим кризисом?

Константин Коротнев: Мы не зафиксировали значительного изменения количества инцидентов.

Анатолий Скородумов: Я бы не сказал, что в связи с экономическим кризисом что-то кардинально изменилось. Последние годы наблюдается устойчивый тренд увеличения количества инцидентов и их разнообразия, который, видимо, сохранится в ближайшее время.

J.I.: Практикуется ли у вас обучение бизнес-пользователей этике информационной безопасности?

Анатолий Скородумов: Да, в банке действует политика повышения осведомленности сотрудников по вопросам ИБ. Для этого применяется практически весь спектр возможных методов, вплоть до разработки специализированных flash-игр по теме ИБ. Что касается DLP-системы, ее использование в режиме Prevention, на наш взгляд, несет в себе серьезный потенциал по выработке у сотрудников правильных навыков работы с информацией.

Константин Коротнев: Все пользователи информационных систем компании проходят регулярное общее или специализированное обучение по ИБ. При приеме на работу сотрудники знакомятся под подпись с документами, регламентирующими ИБ в компании. После этого им назначаются учебные курсы в системе дистанционного обучения, завершающиеся контрольными вопросами на знание материала. Для групп пользователей, наиболее критичных с точки зрения ИБ, разрабатываются и назначаются специализированные учебные курсы, а также проводится регулярное очное обучение.

J.I.: Способны ли сегодняшние DLP-решения отлавливать современных нарушителей? Успевают ли технологии за их изобретательностью? Если нет, чего, на ваш взгляд, не хватает подобным системам?

Константин Коротнев: DLP-решения не являются панацеей от всех рисков ИБ, скорее, это одна из ступеней в эшелонированной защите. Идеализированную задачу по отлову всех нарушителей они не решают, но совместно с другими средствами защиты информации помогают снизить риски ИБ до приемлемого для компании уровня.

Анатолий Скородумов: Эффективность DLP-решений для предотвращения умышленного копирования информации не очень велика. Функциональность агентов, устанавливаемых на рабочие станции сотрудников, на данный момент недостаточна. Охват мобильных технологий также оставляет желать лучшего. А если вы активно используете аутсорсинг и облачные сервисы, и понятие ИТ-периметра организации достаточно размыто, то достаточно сложно организовать эффективный контроль над информацией исключительно с использованием DLP-системы. Для выявления внутреннего злоумышленника необходим целый комплекс мероприятий и средств безопасности, в состав которого, безусловно, должна входить DLP-система. В то же время очевидно, что для несанкционированного копирования небольшого объема данных пользователь может использовать неконтролируемые методы (запомнить, записать на бумаге (личном коммуникаторе), сфотографировать с экрана). Поэтому важно отслеживать каналы не только копирования, но и получения этих данных. JI

КРИЗИС DLP-ТЕХНОЛОГИЙ: А БЫЛ ЛИ МАЛЬЧИК?

АВТОР: МИХАИЛ АНОШИН

С технологической точки зрения DLP-продукты достигли (или в ближайшее время достигнут) потолка в своем развитии – все возможные «фишки» в части способов контроля информации средствами DLP уже придуманы, и с 2011 г. никаких технологических прорывов в этой сфере по большому счету нет. Можно ли считать это кризисом? Каковы его последствия и надо ли их минимизировать? На эти и другие вопросы в своей статье отвечает **Михаил Аношин, руководитель направления DLP Центра информационной безопасности компании «Инфосистемы Джет».**

Источник: «Информационная безопасность», № 3, июнь 2015 г.

ЧТО ЗАКАЗЧИКИ ОЖИДАЮТ ОТ DLP-СИСТЕМ?

АВТОР: МИХАИЛ АНОШИН

О том, что ожидают заказчики от DLP-систем, на что необходимо обратить внимание при выборе решения и что еще, кроме DLP, можно использовать для повышения эффективности управления доступом к информационным ресурсам, на экспертном круглом столе рассказывает **Михаил Аношин, руководитель направления DLP Центра информационной безопасности компании «Инфосистемы Джет».**

Источник: «Информационная безопасность», № 3, июль 2015 г.

Jet Info
ИЗДАЕТСЯ КОМПАНИЕЙ «ИНФОСИСТЕМЫ ДЖЕТ»

Главный редактор Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1,
тел. (495) 411 76 01, факс (495) 411 76 02, e-mail: Jetinfo@jet.msk.su, www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем