SOLAR

СТАТЬИ SOLAR DOZOR

ПОД НАДЗОРОМ DLP

11 экспертных статей
по Solar Dozor за 2023 год

СОДЕРЖАНИЕ

ЭВОЛЮЦИЯ DLP: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБЛАКАХ

Инструменты предотвращения утечек данных (Data Leak Prevention, DLP) играют ключевую роль в реализации эффективных стратегий защиты информации. Эти решения могут быть настроены в соответствии с разнообразными требованиями и способствовать соблюдению стандартов по защите данных. Изучаем вопрос на примере DLP-системы Solar Dozor.

В условиях непрерывной трансформации киберпространства и эволюции информационных технологий решения по предотвращению утечек данных (DLP) становятся неотъемлемой частью стратегии безопасности для компаний по всему миру. Анализ текущих тенденций и динамики рынка позволяет выделить несколько основных направлений, формирующих будущее DLP и определяющих его развитие в ближайшие годы. А на фоне общемировых тенденций к максимальной миграции ресурсов и процессов в облачные среды приоритетным становится обеспечение безопасности данных. Требования к соответствующим продуктам и технологиям, таким как шлюзы облачной безопасности, шифрование данных и централизованное управление безопасностью облачных рабочих нагрузок, существенно возрастают. При этом, несмотря на общий западный тренд, российский рынок DLP продолжает выказывать предпочтение отечественным локальным (on-premise) решениям.

DLP-системы как зрелый класс решений продолжают стабильный рост, основанный на реальных потребностях компаний в обеспечении безопасности конфиденциальных данных. Прогнозируется, что в ближайшие годы этот рост будет обусловлен такими факторами, как, в частности, общая рецессия в экономике, которая вызывает активизацию мошеннических действий и намеренных утечек со стороны сотрудников, и повышенное внимание государства к проблеме утечки данных, о чем свидетельствует разрабатываемый сейчас ГОСТ по DLP (находится на публичном обсуждении в Росстандарте, инициатор разработки — ГК «Солар») и ввод оборотных штрафов за утечки данных. Важным трендом становится также гибридный или полностью удаленный формат работы, который влияет на требования к DLP. Компаниям необходимо контролировать активность дистанционных сотрудников, следить за новыми каналами передачи данных, что стимулирует развитие рынка DLP в условиях современной бизнес-среды (рис. 1).

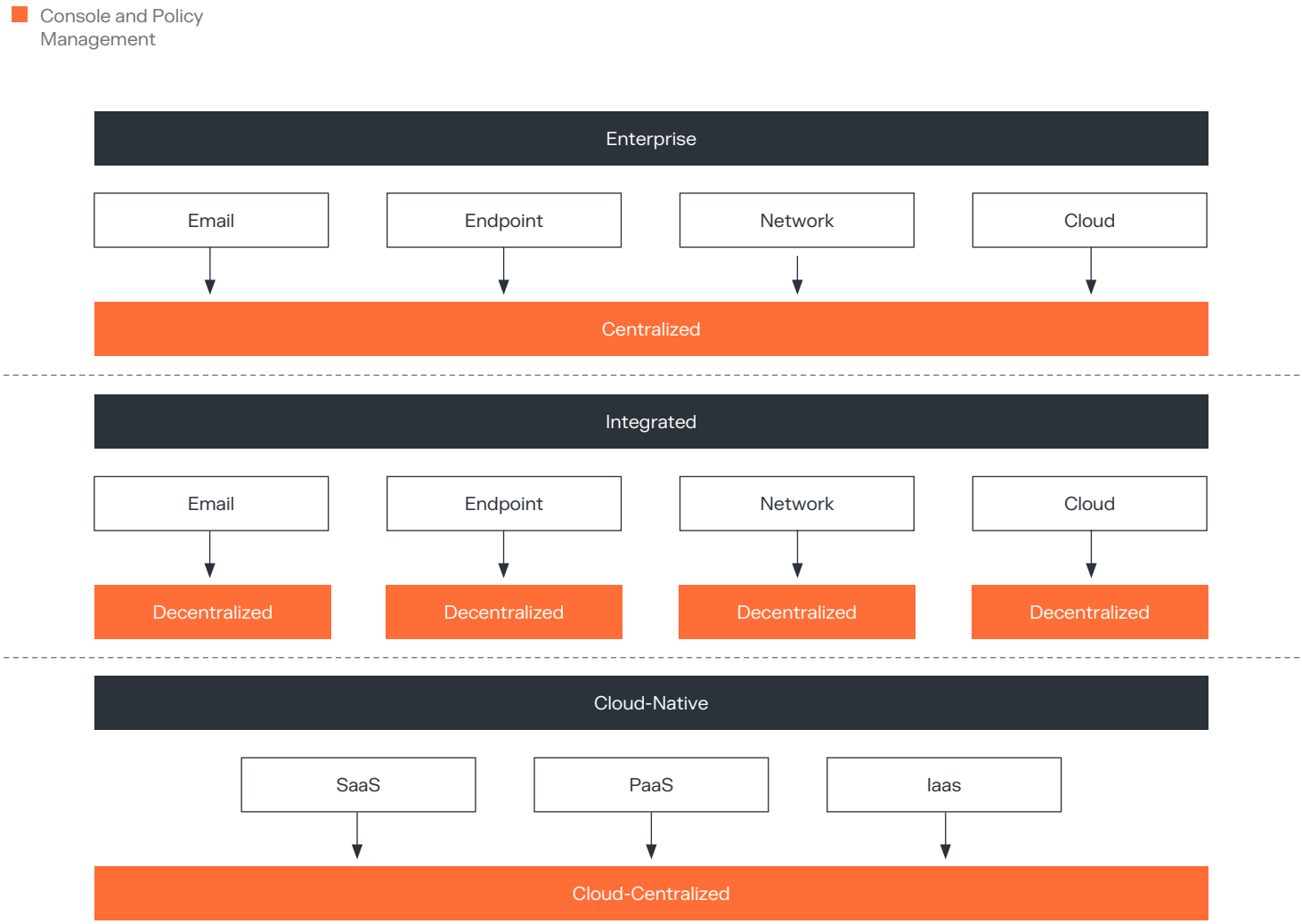


Рисунок 1. Будущие классы DLP-систем по версии Gartner

По данным международной и российской аналитики, в 2024 году предвидится неравномерный рост рынка DLP-решений по отраслевым сегментам — очевидный для коммерческих предприятий, тогда как в государственном секторе он может зависеть от законодательных и регулирующих инициатив. Миграция на российские решения, начавшаяся в предыдущем году, успешно прошла первый этап, создав основу для дальнейшего развития отечественного рынка. В свете дефицита ресурсов и кадрового голода DLP по модели «как услуга» (SaaS) обещает стать важным трендом в 2024 году.

Эффективное внедрение DLP-систем, а также их взаимодействие с другими технологиями, такими как защита данных в покое (DCAP), мониторинг активности баз данных (DAM) или управление идентификацией (IdM), станет важным фактором для компаний, стремящихся обеспечить полноценную безопасность данных в современной динамичной среде (рис. 2). Исходя из эволюции DLP-решений в качественно новый класс систем защиты данных, способность быстро реагировать на внутренние и внешние угрозы будет ключевым аспектом успешного развития в сфере ИБ-безопасности.

Adaptive
Risk-Based DLP

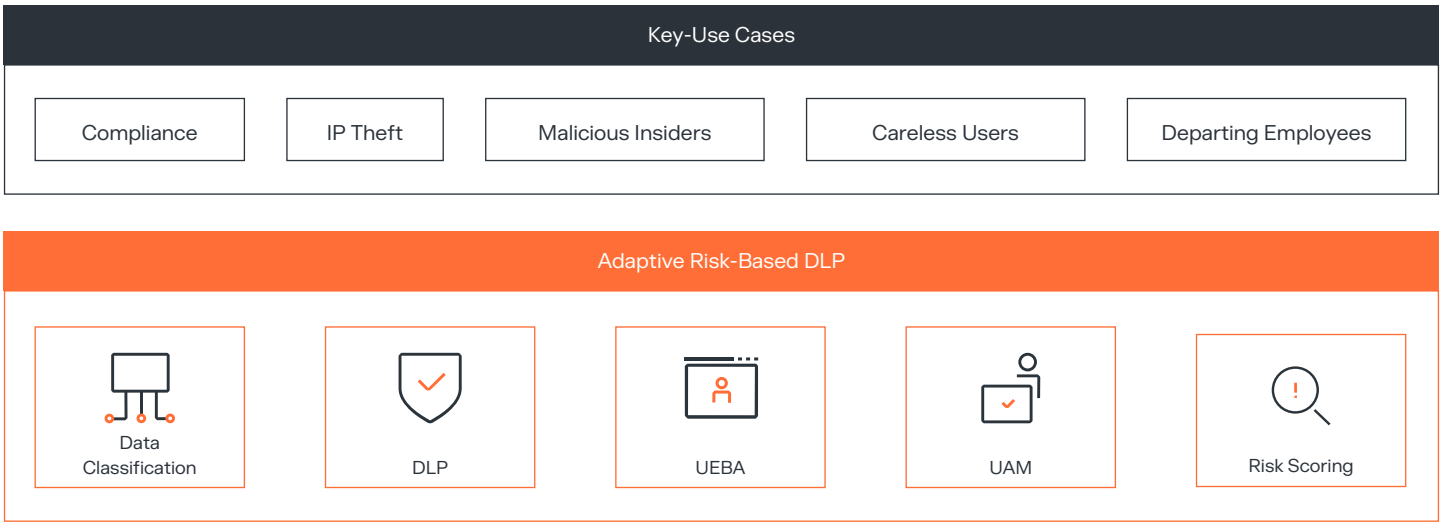


Рисунок 2. Адаптивный риск-ориентированный подход к DLP в связке с другими технологиями по версии Gartner

Международная аналитика по рынку DLP

В докладе Mordor Intelligence прогнозируется, что рынок средств предотвращения утечки данных (DLP) покажет заметный рост и достигнет объема в 6,22 миллиарда долларов США к 2028 году по сравнению с 2,28 миллиарда долларов в 2023 году. Таким образом, среднегодовой темп роста составит 22,29 %. Основной движущей силой этого процесса выступает внедрение новых средств безопасности предприятиями по всему миру в ходе их цифровой трансформации, что способствует увеличению доли рынка DLP и появлению новых подклассов DLP. Интерес к решениям этого класса усилился из-за кратного роста утечек данных и, как следствие, востребованности использования DLP в качестве сервиса (SaaS) и расширения функциональности DLP в облачных средах. Эти факторы стимулируют спрос на услуги по защите данных, особенно в тех организациях, что работают со значительным объемом структурированных и неструктурированных данных. Следует отметить, что многие крупные предприятия, включенные в перечень Fortune Global 500, вложились в рынок DLP более десяти лет назад. В настоящее время этот сегмент также приобретает популярность среди предприятий среднего бизнеса. Инструменты предотвращения утечки данных (DLP) играют ключевую роль во внедрении эффективных стратегий защиты данных.

Эти решения могут быть настроены в соответствии с различными требованиями и обеспечивать соблюдение законодательства о защите данных, в частности, общего европейского регламента по защите персональных данных (GDPR) или закона Калифорнии о защите конфиденциальных данных потребителей (CCPA). Позволяя организациям выявлять, отслеживать и контролировать передачу конфиденциальных данных извне и вовне их сетей, решения DLP поддерживают общие усилия по обеспечению безопасности данных.
Распространенность и глубина внедрения политик по использованию личных устройств на работе (BYOD) вызывают опасения у руководства многих ключевых предприятий. Согласно отчету по безопасности BYOD 2021 года от Forcepoint, значительное большинство компаний (82%) активно поощряют сотрудников применять свои личные устройства для работы.
В то же время BYOD обычно связывается с использованием неуправляемых устройств сотрудниками (70%), подрядчиками (26%), партнерами (21%), клиентами (18%) и поставщиками (14%). В результате возрос спрос на надежные меры по нейтрализации потенциальных рисков, связанных с практикой BYOD.

Ситуация на российском рынке DLP

Несмотря на санкции, российский рынок информационной безопасности остается открытым, ориентированным не только на национальные стратегии, но и на общемировые тренды. В условиях повсеместной цифровизации и развития облачных технологий вопросы информационной безопасности, включая борьбу с утечками, становятся важными на трансграничном уровне, поскольку, как показывает анализ трендов за пределами России, все ярче прослеживается тенденция к все более массовому распространению облачных технологий. Как следствие, встает необходимость обеспечения защиты на уровне облаков (рис. 3). Решением проблемы становится применение соответствующих продуктов и технологий, таких как шлюзы облачной безопасности, решения по обеспечению конфиденциальности данных в облачных средах, шифрование информации перед передачей в облако, централизованное управление безопасностью облачных рабочих нагрузок.

Вопрос о будущем DLP-систем возникает в контексте растущей угрозы утечек данных и ужесточения ответственности за них. Однако не вполне ясно, следует ли говорить о востребованности исключительно самих систем DLP или защиты данных в целом. Сегодняшний вектор развития указывает на необходимость обмена данными между различными системами для обеспечения полноты и эффективности защиты. В связи с этим продуктовые линейки крупных игроков отечественного рынка информационной безопасности начинают пополняться комплексными решениями, интегрирующими DLP-системы в более широкие экосистемы.
Это позволяет клиентам перейти от отдельных фрагментированных продуктов к моновендорным решениям, где DLP-системы играют ключевую роль в обеспечении целостности данных.

В частности, на российском рынке ГК «Солар» сформировала экосистему продуктов и сервисов, связанных общей логикой. Технологии, которые изначально были реализованы в одном продукте, со временем начинают обогащать другие. Так, модуль поведенческого анализа (UBA), первоначально появившийся в DLP-системе Solar Dozor, сейчас используется в аналитических подсистемах других продуктов компании. Оценивая перспективы, можно ожидать появления не только моновендорных решений, но и плодов сотрудничества различных производителей систем защиты.

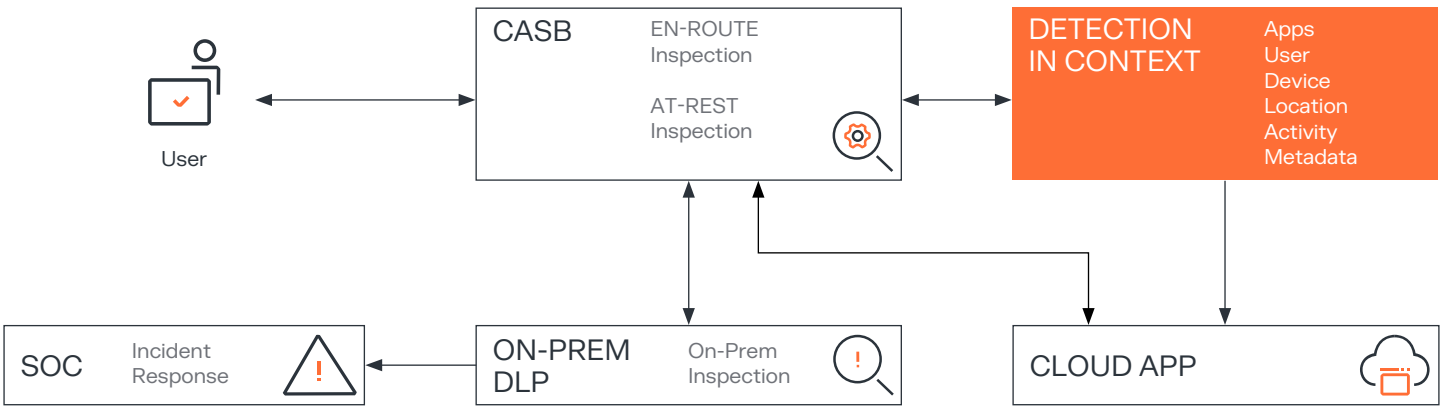


Рисунок 3. Пример архитектуры облачного DLP

2,28 МЛРД ДОЛЛ.

Составляет объем рынка предотвращения утечки данных (DLP) в 2023 году

6,22 МЛРД ДОЛЛ.

Прогнозируемый рост рынка средств предотвращения утечки данных (DLP) к 2028 году

По данным
Mordor Intelligence

Как показывает общемировая аналитика в области информационной безопасности, кооперация вендоров позволит создавать усовершенствованные и комплексные решения, в том числе и в классе систем DLP (рис. 4). Есть все основания полагать, что DLP-система может стать центральным элементом в комплексной стратегии обеспечения безопасности данных.

Долгая история DLP на российском рынке и устойчивость к изменениям делают логичным развитие DLP-решений в направлении расширения возможностей защиты конфиденциальных данных. Несмотря на стремление к интеграции и экосистемности, DLP сохраняет актуальность и привлекательность для пользователей.

Рисунок 4. DLP как элемент глобальной стратегии защиты данных

Возможные перспективы

Развитие DLP подразумевает двустороннее обогащение сведениями при взаимодействии с другими системами. При этом актуальным остается требование обеспечения постоянного контроля за действиями пользователей, сокращения числа ложных срабатываний и регулярного обновления политик безопасности. Аналитики подчеркивают важность не только технологического совершенствования, но и подготовки кадров, а также возможного применения искусственного интеллекта, хотя на данной стадии этот процесс представляет определенные трудности и требует дополнительных исследований.

Следующим шагом в развитии DLP-систем может стать их превращение в универсальный инструмент управления данными. Современная DLP-система не только обеспечивает безопасность данных, но также анализирует действия пользователей, фиксируя аномалии в их поведении и формируя их досье, выступая тем самым ценным источником информации для отделов кадров или руководителей среднего звена, которые заинтересованы в эффективности работы своих команд. Учитывая, как будет развиваться ситуация, можно ожидать, что к 2030 году DLP-система будет играть центральную роль в процессах совершенствования технологий управления данными. Она может выйти за пределы своей роли как защитного инструмента и стать ключевым элементом в управлении информацией о компании и ее сотрудниках.

Важно понимать, что революции в этой области не произойдет без существенных изменений в ответ на технологические вызовы, и в этом случае есть смысл пересмотреть в целом подход к DLP-решениям.

Вместо фокусировки на перехвате и фильтрации, возможно, стоит сосредоточить внимание на самих данных, на обнаружении и предотвращении ненадлежащего их использования независимо от мотивов или применяемых средств. Мандатные метки и метаданные могут стать ключевым инструментом для эффективного управления информацией.

Другим направлением развития DLP-систем может быть охват ею более широкой аудитории. В дополнение к разработкам для корпоративного сектора и государственных учреждений может появиться «нано-DLP» для индивидуального использования, что позволит реализовывать, например, контроль над коммуникациями в семье.

Одним словом, все то, что востребовано в мире смарт-технологий. В конечном счете можно смело предположить, что при нынешнем темпе роста рынка в недалеком будущем возобладает прогрессивное развитие систем DLP. Однако же в ожидании революционных прорывов внимание к инновациям, гибкость подхода и умение адаптироваться к изменениям будут ключевыми факторами успешного развития DLP-систем на российском рынке.

Выводы

В современном бизнес-мире анализ потребностей и рисков становится ключевым фактором при выработке стратегии внедрения DLP-систем. Оценка существующих инструментов, таких как безопасные почтовые шлюзы (SEG), периферийная защита (SSE) или облачные решения, играет важную роль в понимании того, как данные используются и передвигаются внутри организации. Программные средства классификации данных становятся основой обеспечения безопасности и соблюдения требований, помогают избежать ложных срабатываний и облегчают задачу управления политиками DLP, что, в свою очередь, способствует повышению эффективности профилактического контроля каналов передачи информации. Тренды развития DLP связаны с инвестициями в решения с широкой функциональностью, способные анализировать полный спектр данных и контекстно оценивать активность пользователей, в том числе в облачные DLP, которые становятся неотъемлемой частью стратегии развития, особенно в организациях с гибридными инфраструктурами.

Илья Лушин
Руководитель продукта Solar Dozor
Центр технологий кибербезопасности
ГК «Солар»

ДЖЕНТЛЬМЕНСКИЙ НАБОР ДЛЯ ЗАЩИТЫ ОТ УТЕЧЕК ИНФОРМАЦИИ: ВЫБИРАЕМ КОНФИГУРАЦИЮ DLP

Вот-вот будет принят законопроект, предусматривающий оборотные штрафы за утечку персональных данных. А помимо очевидных финансовых потерь пострадавшие компании также терпят колоссальный репутационный ущерб. Для защиты от утечек информации есть отдельный класс ИБ-решений — Data Leak Prevention. В этой статье расскажем, что это, как сделать правильный выбор конфигурации такой системы и определить «гигиенический» минимум функциональности конкретно для ваших задач.

385

российских организаций стали жертвами утечек за неполный 2023 год, по данным ГК «Солар»

Всего утекло:

4,84 МЛРД

строк данных

142 МЛН

адресов электронной почты

222 МЛН

телефонных номеров

Предположим, вы руководите предприятием, в котором работает энное число сотрудников. Предположим, предприятие это современное, находящееся на острие прогресса — в нем есть и CRM, и ERP, и доступ в интернет, и даже бесплатные печеньки на кухне. Разумеется, и коммерческие тайны, и персональные данные клиентов также имеются.

Время сейчас непростое, тектонические изменения миропорядка сопровождаются настоящей кибервойной, и поэтому вы надежно защитились от разных неприятностей: внедрили межсетевой экран нового поколения, трафик у вас туннелируется, настроен поточный антивирус, работает система обнаружения и предотвращения вторжений, удаленный доступ осуществляется через надежное средство организации виртуальной частной сети (в народе — VPN). То есть периметр защищен полностью. Однако одним прекрасным утром весь новостной Telegram пестрит сообщениями об утечке данных из вашего предприятия.

Казалось бы, вы были защищены по всем современным правилам ИБ! Но дело тут вовсе не в хакерах, которые бродят вокруг периметра. Просто бухгалтер или специалист по кадрам отправил себе на почту выгрузку из базы данных в excel-формате. Может, он хотел поработать дома. А может — комфортно уволиться, захватив с собой контакты всех своих контрагентов. А может, даже для того, чтобы передать эту выгрузку злоумышленнику, который не стал тратить время на взлом вашей NGFW, а предпочел заплатить рядовому сотруднику необременительную сумму.

Подобным нехитрым образом утекает огромное количество данных — и это не преувеличение.

Каждая такая утечка сказывается на предприятии весьма болезненно: это и прямые финансовые потери, включающие штрафы от регуляторов, и потери, которые точно подсчитать невозможно, поскольку они репутационные, а репутация дорогого стоит.

Необходимо осознать, что угрозы существуют не только внешние, но и внутренние. Из этого следует важный вывод — любой организации необходимо средство, способное максимально защитить ее от внутренних угроз.

Отвечает за такую защиту отдельный класс решений — Data Leak Prevention (DLP), защита от утечек информации. Это программное решение, которое блокирует передачу конфиденциальных документов, помогает выявлять признаки корпоративного мошенничества, облегчает профилактику инцидентов безопасности.

Практически любая уважающая себя современная DLP имеет модульную структуру, то есть функционал ее можно конфигурировать под потребности конкретной компании и впоследствии удобно наращивать, докупая только те функции, которые реально необходимы. Давайте попробуем разобраться, каков же необходимый минимум функциональных возможностей DLP, который уменьшит риски утечек до приемлемого уровня. Для наглядности будем опираться на архитектуру DLP нашего производства — Solar Dozor (рис. 1).

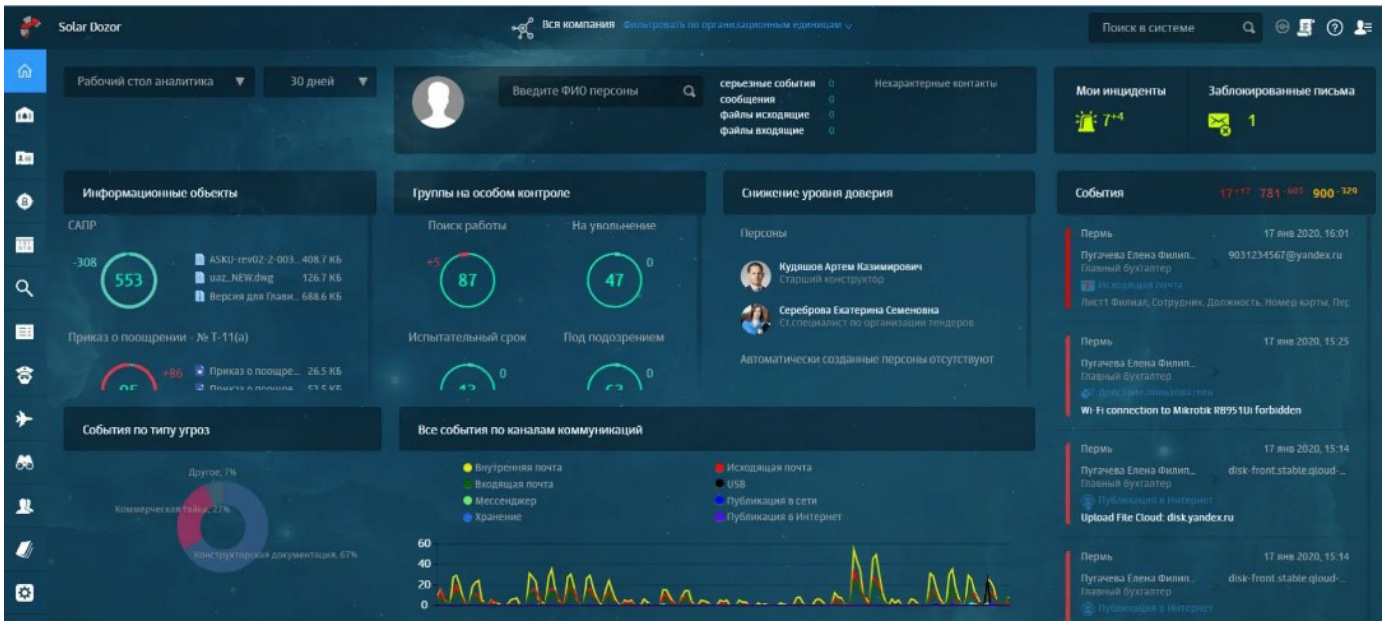


Рисунок 1. Дашборд Solar Dozor

Электронная почта — основной канал утечки конфиденциальной информации

Может показаться странным, но основная часть сотрудников свободно использует электронную почту вообще для всего: как для переписки по работе, так и для отправки себе или кому-то другому конфиденциальной информации (вплоть до коммерческой тайны компании). Поэтому первоочередным и важнейшим модулем DLP является средство контроля корпоративной электронной почты.

В нашем Solar Dozor этот модуль называется Mail Connector (рис. 2). Этот модуль умеет получать копии сообщений от сервера электронной почты (MS Exchange, Communigate, Zimbra и проч.) и фильтровать сообщения в соответствии с настроенной политикой безопасности. Можно проводить сквозные расследования на распределенном по всей организации архиве корпоративных переписок. При установке «в разрыв» сети модуль умеет блокировать отправку писем, помещать подозрительные отправления в карантин и даже изменять содержимое писем (например, в случае если офицерами безопасности задумана сложная операция по дезинформации конкурентов). Однако, принимая решение о способе внедрения, следует учитывать, что установка «в разрыв» может привести к незначительному увеличению сроков доставки.

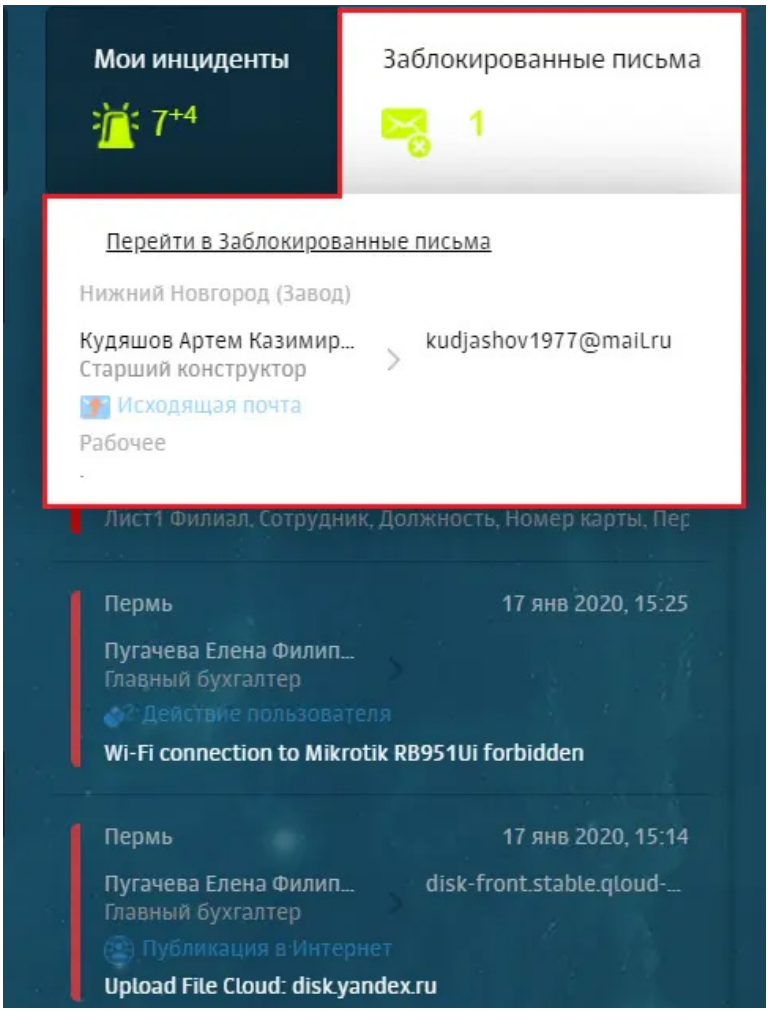


Рисунок 2. Mail Connector заблокировал подозрительное письмо

Более сложный случай: картинки и pdf-файлы

Обязательно нужно быть готовым к тому, что чувствительная информация может передаваться в графических форматах. DLP-системы используют технологию оптического распознавания символов — OCR. Очень рекомендую не забыть про этот модуль при выборе DLP-системы, его важность трудно переоценить.

Модуль Solar Dozor так и называется — OCR. Точность поточного распознавания текста из картинок составляет внушительные 98%, а его пропускная способность — 1 ТБ в сутки (рис. 3).

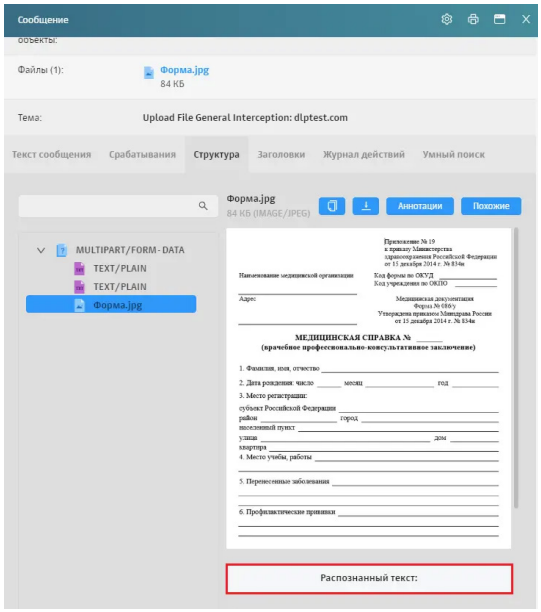


Рисунок 3. OCR переводит jpg в текст

Веб-трафик: банально, но очень важно

Отчасти вопрос контроля за действиями сотрудников в интернете закрывают решения SWG или NGFW (а в начале статьи мы условились, что периметр организации надежно защищен и, значит, такое решение уже внедрено). Для анализа трафика пользователей, проходящего через них, используется специальный модуль. С его помощью можно контролировать, что именно пишет сотрудник на форумах и в соцсетях, какие данные он передает в облака.

Наш модуль называется Traffic Analyzer. Модуль захватывает и входящий, и исходящий трафик, пересобирает пакеты, анализирует и разбирает захваченный трафик, отправляя полученные данные в ядро Dozor на проверку и фильтрацию согласно настроенным политикам. Напомню, что этот модуль в обязательном порядке требует наличия источника данных — лучше всего, если это будет Solar webProxy или Solar NGFW, но подойдет и любой другой прокси-сервер или маршрутизатор с поддержкой передачи трафика по протоколу ICAP или со SPAN-порта. Также источником трафика может служить наш Endpoint Agent, о котором поговорим ниже.

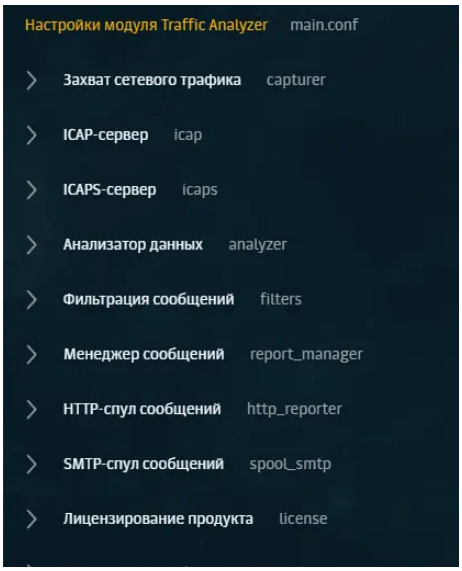


Рисунок 4. Настройки модуля для контроля веб-трафика

Что сотрудник делает на рабочем компьютере?

Для вышеупомянутого контроля существует специальная программа, которая устанавливается на рабочие компьютеры пользователей. Кроме действий непосредственно на компьютере, она должна отслеживать доступ к принтерам, внешним файловым хранилищам (в том числе к флешкам или USB-HDD), буферу обмена и так далее. Необходимо охватить мессенджеры — важнейший канал, через который утечки происходят чаще всего, наряду с электронной почтой. В идеале агент может отслеживать названия посещаемых сайтов и открытых приложений, время работы с ними, может записывать видео происходящего на экране пользователя и транслировать его в реальном времени офицеру безопасности, записывать звук с микрофона рабочей станции, делать скриншоты экрана.

Все это умеет программа в нашем Dozor — модуль Endpoint Agent. Причем неважно, под управлением какой ОС работают компьютеры ваших сотрудников: это может быть и Windows из откровенно недружественной страны, и MacOS из все той же недружественной страны, но уже с некоторым эстетским уклоном, а может быть и наш великий и могучий Линукс (поддерживаются практически все самые востребованные и популярные решения). Агент контролирует любые действия сотрудника, причем способен перехватывать данные, которые невозможно перехватить на шлюзе (например, переписку, защищенную end-to-end-шифрованием). Поддерживаются все наиболее популярные мессенджеры: Telegram, WhatsApp, Viber, Skype, Zoom, eXpress, TrueConf и прочие.

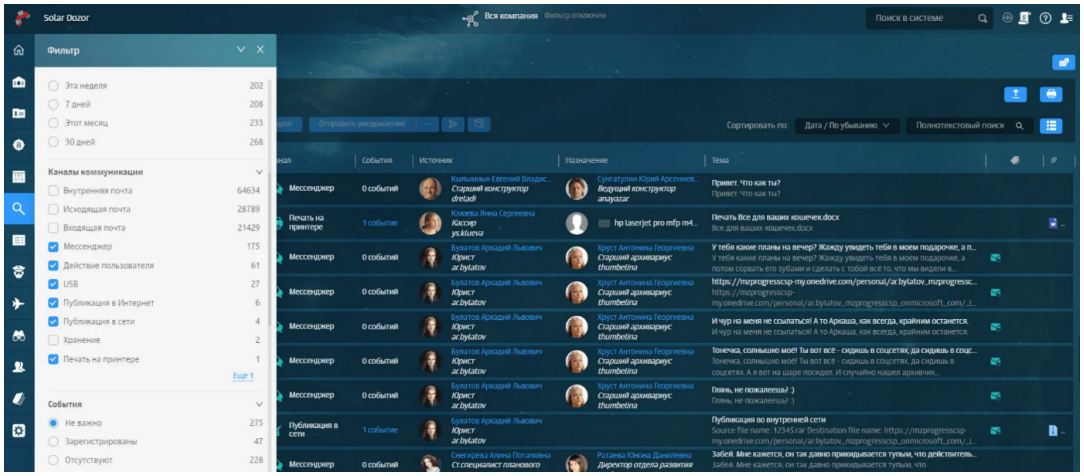


Рисунок 5. С помощью Endpoint Agent видим, что отправляется на печать и о чем переписываются сотрудники на рабочих компьютерах

Итак, вот наш необходимый минимум

Перечисленные модули — важнейшие, это и есть наш «гигиенический» минимум конфигурации DLP для обеспечения полноценной защиты от утечек. В порядке убывания важности их можно расставить так:

1. Модуль контроля почты (Mail Connector).
2. Модуль контроля активности на компьютере (Endpoint Agent).
3. Модуль анализа веб-трафика (Traffic Analyzer).
4. Модуль для распознавания графических форматов (OCR).

Однако DLP способна и на большее, поэтому нельзя не рассказать о других существующих модулях.

Контролируем данные в локальных хранилищах

Инвентаризировать данные, находящиеся в покое в хранилищах, нужно, чтобы:

- выявлять нарушения правил хранения конфиденциальной информации (например, документ, составляющий коммерческую тайну компании, лежит в общем доступе);
- контролировать содержимое локальных машин и сетевых ресурсов сотрудников;
- автоматически мониторить и классифицировать корпоративные данные на файловых ресурсах;
- контролировать файлообмен между сотрудниками и целыми отделами, сканировать сеть и строить ее дерево;
- обнаруживать неавторизованные запущенные сервисы.

В Solar Dozor этим целям служит модуль File Crawler (рис. 6), и он важнейший после вышеперечисленных четырех модулей. Модуль использует дата-центричный подход к ИБ предприятия и отчасти может заменить даже специализированные DCAP-решения.

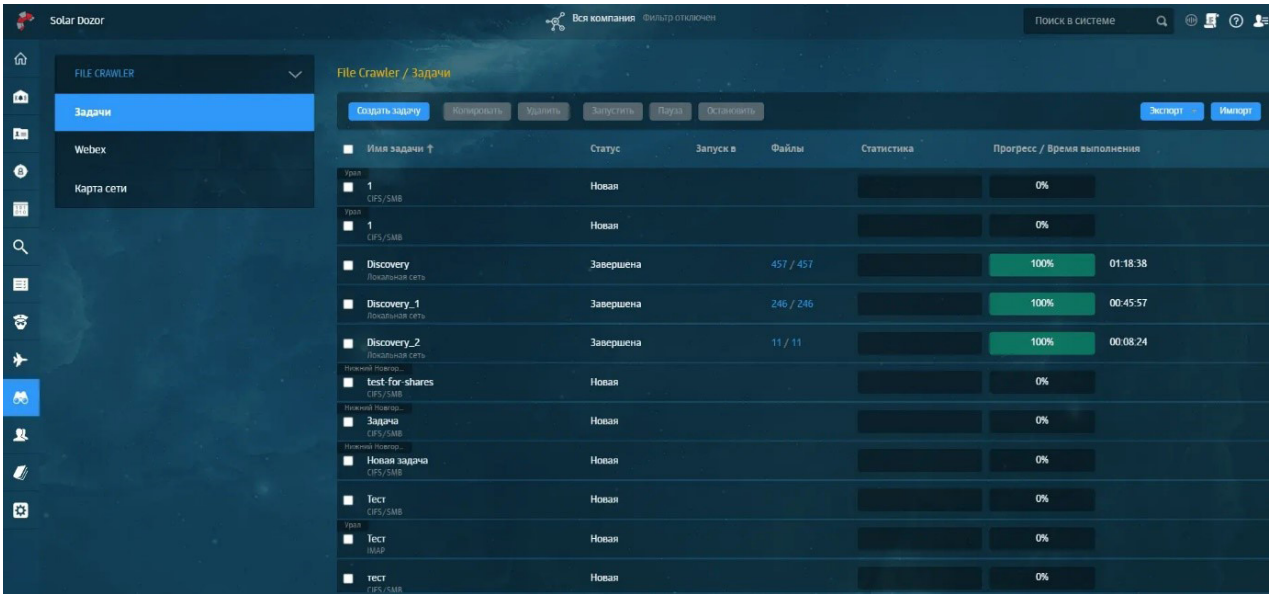


Рисунок 6. Модуль для анализа локальных хранилищ Solar Dozor

Оптимизируем хранение архивов

Для любого предприятия важно иметь архив электронной почты, однако хранить десятки и сотни гигабайт информации на боевых серверах довольно недешево. Поэтому необходимо специализированное средство, которое позволяет переносить архив (или его части) на более дешевые носители, например на ленты.

Специально для этого разработан модуль DLP Long-Term Archive. Название говорит само за себя. Он умеет управлять несколькими хранилищами, переносить данные на долгосрочное хранение и оперативно подключать обратно к DLP части базы данных сообщений (например, для проведения расследований).

Анализируем поведение

Чтобы обеспечить полнофункциональный контроль рабочего времени, что очень актуально в случае удаленной работы, DLP-система может быть оснащена аналитическими модулями. У нас есть модуль Dossier, который работает в сочетании с Endpoint Agent. Он умеет выявлять взаимосвязи между пользователями (в том числе скрытые), исследовать интенсивность коммуникации между сотрудниками и ее каналы, строить отчеты по конкретному человеку по расписанию, разово или регулярно. Благодаря этому модулю можно выстраивать уровни доверия к конкретным сотрудникам.

Dossier является средством для обработки и отображения данных, получаемых из самого инновационного модуля DLP. На сегодня он есть только в Solar Dozor и называется UBA (User Behavior Analytics) — анализ поведения пользователей (рис 7).

Простой пример: сотрудник всегда работает с 10:00 до 18:00, но внезапно в один из дней появляется на работе в 22:00. Не факт, что это что-то плохое, но это аномалия, на которую офицеру безопасности необходимо обратить внимание.

Пример посложнее: у сотрудника 99% корпоративной переписки происходит внутри периметра компании, но вдруг происходит всплеск email-активности с внешними получателями, и это серьезный повод для офицера безопасности присмотреться к этим письмам.

Модуль умеет строить индивидуальные профили поведения, автоматически выявлять поведенческие аномалии, профилировать сотрудников по паттернам поведения (поддерживается до 20 разных паттернов), выявлять опасные массовые тенденции, искать взаимосвязи между событиями ИБ и поведенческими аномалиями, сравнивать модели поведения разных сотрудников и многое другое.

Анализ поведения — передовая технология, за которой будущее современного кибербеза, и очень полезный инструмент, в том числе в расследовании инцидентов.

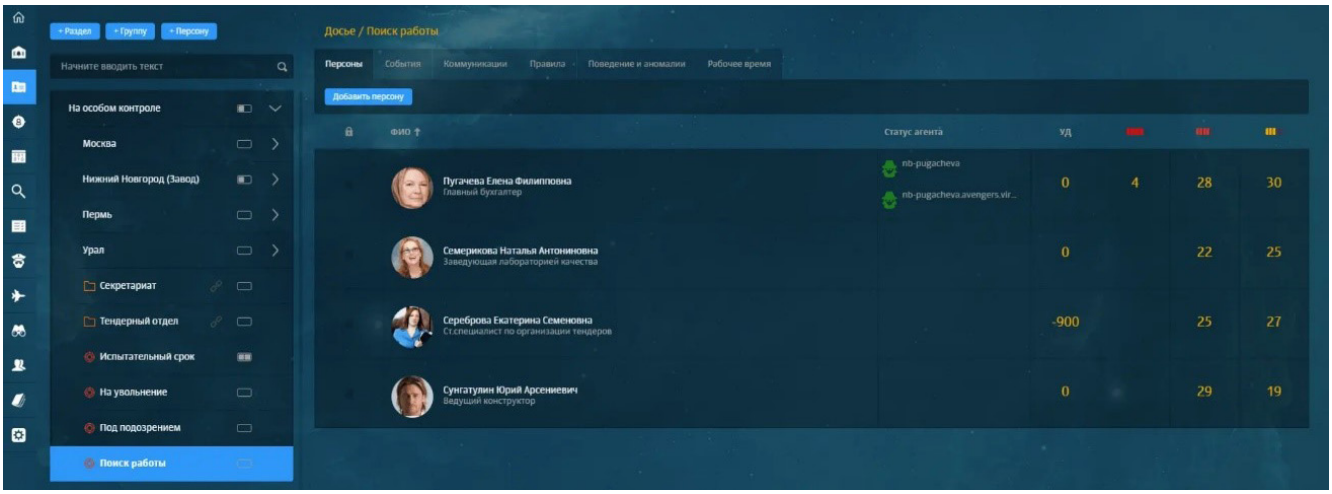


Рисунок 7. Среди сотрудников, планирующих увольнение, есть Екатерина с критически низким уровнем доверия

Управляем географически распределенной сетью

Еще один уникальный для DLP модуль, присутствующий в Solar Dozor, — MultiDozor. Он удобен, когда предприятие географически распределено, с большим количеством филиалов и ДЗО. Этот модуль объединяет разрозненные инсталляции в единое целое с минимизацией нагрузки на сеть передачи данных и позволяет проводить сквозные расследования по всей филиальной сети.

Если, например, локальные сотрудники ИБ и офицеры из центрального аппарата должны иметь разные права, MultiDozor позволяет разделить их уровни доступа к системе (рис. 8).

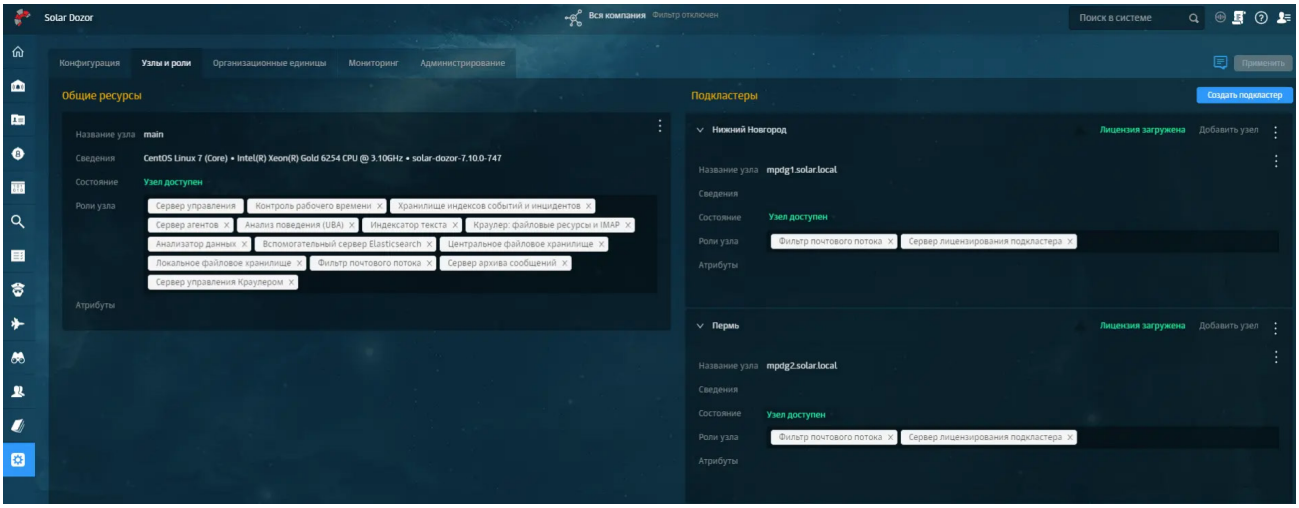


Рисунок 8. Разные роли для разных узлов в Solar Dozor

Выводы

Утечки изнутри компании могут происходить десятками и сотнями различных способов, поэтому их предотвращение — важнейший и непростой процесс информационной безопасности. Решения DLP — архитектурно сложные программные комплексы с огромным количеством самых разных функциональных возможностей. Принимая решение внедрить такую систему, очень важно разобраться в тонкостях ее эксплуатации и сделать правильный выбор конфигурации исходя из того, каков необходимый минимум для обеспечения внутренней безопасности на конкретно вашем предприятии.

Руслан Добрынин
Менеджер по развитию бизнеса Solar Dozor
Центр технологий кибербезопасности
ГК «Солар»

СТАНДАРТИЗАЦИЯ ПРОЦЕДУР ЗАЩИТЫ ОТ УТЕЧЕК ИНФОРМАЦИИ УСИЛИТ ЭФФЕКТИВНОСТЬ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

20 ЛЕТ

Утечки конфиденциальной информации из информационных систем как угроза ИБ существуют уже более 20 лет.

Не меньшую, если не большую, проблему, чем инсайдеры-злоумышленники, для информационной безопасности организации представляют просто недисциплинированные сотрудники — любители поработать из дома или сохранить у себя интересную рабочую информацию «на всякий случай».

На сегодняшний день нет стандартизированной, признанной рынком методологии организации процессов защиты конфиденциальной информации от утечек, поэтому операторы информационных систем организуют этот процесс исходя из своих знаний и опыта. Одни отталкиваются от уровня проработки модели угроз, связанных с утечками, другие — от уровня используемых методов защиты. Например, в одних организациях внутренними документами ограничена печать документов и использование съемных носителей, а в других — уже используются полноценные DLP-системы.

Практика внедрения систем защиты от утечек бизнеса принципиально отличается от внедрения таких решений в организациях госсегмента из-за их специфики. Для бизнеса важно правильно легитимизировать использование DLP-системы, чтобы минимизировать риски судебных исков со стороны сотрудников о «защите частной жизни».

Государственным заказчикам необходимо интегрировать решения для защиты от утечек в общий контур защиты информации государственных информационных систем, информационных систем персональных данных или субъектов критической информационной инфраструктуры, корректно обосновав выделение средств для их приобретения и эксплуатации, и регламентировать использование соответствующих средств в локальных нормативных актах.

При этом и многие коммерческие заказчики, и каждый ФОИВ и подведомственные ему организации являются операторами ГИСов или работают с хранящейся в них информацией. А это персональные данные граждан, данные первичного статистического учета, тайна следствия, врачебная, налоговая и прочая информация, за конфиденциальность которой оператор соответствующей информационной системы несет правовую ответственность.

Мы уже не первый год сталкиваемся с парадоксальной ситуацией: фактически ИБ-угроза и соответствующие инциденты есть, а вот формальных оснований и единообразных подходов для эффективного противодействия им нет. В результате компании, для которых проблема носит особенно острый характер, закупают и внедряют решения, в большинстве случаев не уделяя должного внимания грамотной интеграции правил использования DLP-системы в локальные нормативные акты.

Некорректное документальное оформление этого процесса может повлечь серьезные последствия в виде судебных разбирательств сотрудников с работодателями о законности сбора и использования информации об их активности на рабочем месте. С подобными проблемными вопросами потенциальные и действующие эксплуатанты специальных технических средств защиты информации от утечек часто обращаются к их производителям.

Как производитель специальных технических средств защиты, обладающий многолетней практикой внедрения собственной DLP-системы Solar Dozor в организациях самых разных масштабов и отраслей, мы инициировали разработку национального стандарта «Защита информации от утечки из программной среды информационных (автоматизированных) систем». Стандарт готовим совместно с Центром защиты информации, поскольку у него большой опыт в подготовке аналогичных документов, в частности ГОСТов. Разработка стандарта позволит синхронизировать терминологию и определить общие подходы к реализации мероприятий по защите от утечек с учетом лучших международных практик.

К разработке стандарта мы активно привлекаем других производителей средств защиты от утечек, эксплуатантов таких средств, а также прочие заинтересованные стороны, которые видят угрозу безопасности в утечках. Совместная работа над проектом стандарта позволит нам учесть все многообразие накопленного ими опыта.

При подготовке документа и его обсуждении с экспертами в области защиты от утечек появляется множество вопросов, требующих фиксации и методологической проработки. Надеемся, что эти документы в совокупности позволят учесть и нашу накопленную экспертизу, и опыт других участников рынка, чтобы помочь тем, кто только задумывается об использовании DLP-систем или хочет оценить эффективность работы и корректность внедрения уже используемой системы.

Чтобы сделать эти документы действительно объективными и полезными, мы также предлагаем всем заинтересованным сторонам присоединяться к обсуждению разных аспектов процесса защиты от утечек, делиться наработанными практиками и совместно искать ответы на злободневные вопросы, зафиксировав их в формате национального стандарта или, если потребуется, в других документах.

Елена Черникова
Руководитель направления по работе
с государственными структурами
Центр технологий кибербезопасности
ГК «Солар»

КАК ИСКАТЬ ПОВЕДЕНЧЕСКИЕ АНОМАЛИИ В КОМПАНИЯХ С ФИЛИАЛЬНОЙ СЕТЬЮ

Утечки конфиденциальной информации, коммерческий сговор, конфликт интересов, корпоративное мошенничество — все это неполный список внутренних угроз безопасности, с которыми сегодня сталкиваются российские компании. Особенно сложно противостоять таким угрозам в территориально распределенных организациях с множеством филиалов и большим количеством сотрудников.

Как работает UBA

В DLP-системе Solar Dozor разработки ГК «Солар» есть модуль анализа поведения пользователей (User Behavior Analytics, UBA). Его работа базируется на теориях вероятности, случайных процессов и графов. Модуль UBA в реальном времени анализирует историю коммуникаций каждого сотрудника и автоматически формирует личный профиль его нормального поведения. На основе собранной информации выявляются аномалии в поведении сотрудника. Оно описывается с помощью таких показателей, как внешняя и внутренняя активность, объем полученных и отправленных информационных объектов, круг общения, популярность. Также в системе есть показатель, который обобщает вышеназванные и отражает степень риска совершения сотрудником случайных или намеренных нарушений безопасности, — индекс уязвимости.

Кроме того, модуль «ищет» работников, которые попадают под значимые для безопасности паттерны поведения, например «Потенциальные инсайдеры», «Признаки увольнения», «Контакты с неизвестными», «Мертвые души» и т. д. — всего 20 паттернов. Проверка сотрудников по ним помогает предотвращать утечки и выявлять уязвимости в бизнес-процессах.

Для предварительного анализа достаточно накопить массив данных о коммуникациях сотрудников в электронной почте и мессенджерах за один месяц, для точного анализа — за два-три месяца.

UBA для организаций с филиалами

Несколько лет назад в DLP-системе Solar Dozor появился модуль MultiDozor. Он был разработан специально для территориально распределенных организаций. Модуль позволяет объединить разрозненные инсталляции Solar Dozor в единую систему, обеспечив централизованное управление и мониторинг инцидентов как во всей организации, так и в конкретных филиалах. По аналогии с этим мы разработали модуль анализа поведения пользователей специально для компаний с филиальной сетью (MultiUBA).

По сравнению со стандартной версией MultiUBA отличает акцент на коммуникационные сегменты компании с изолированным плотным взаимодействием сотрудников внутри каждого из них. В самой DLP-системе они называются организационными единицами — например, центральный офис, региональные филиалы, склады и т. п. Такая схема позволяет гораздо эффективнее анализировать поведение пользователей и делать на основе этого определенные выводы, в отличие от ситуации, когда единый модуль UBA развернут во всей организации.

Корректная оценка

Модуль UBA оценивает поведение сотрудников по ранговой шкале. Предположим, что мы сравниваем количество тех или иных действий пользователя за компьютером: у кого-то насчитали 62, у кого-то — 21, у кого-то — 0. Затем модуль UBA анализирует действия всех пользователей и строит гистограмму. У каждой организации она своя в зависимости от особенностей коммуникаций, их насыщенности. Допустим, пользователь, у которого 62 действия, имеет по ранговой шкале оценку 4,5 балла. Сотрудники, у которых действий значительно меньше, получают более низкую оценку. Если единый модуль поведенческого анализа развернут во всей территориально распределенной компании без разделения на организационные единицы, то филиалы, в которых коммуникации менее насыщенные, по этой шкале всегда будут иметь более низкие баллы.

Пример. В крупной производственной компании с большим центральным офисом в Москве, 35 региональными филиалами и 12 складами развернута DLP-система с модулем анализа поведения пользователей в его обычной (нераспределенной) версии. Анализируя коммуникации сотрудников, офицер безопасности обратил внимание на то, что сразу в нескольких филиалах, в том числе в складских подразделениях, очень много сотрудников попали в группы особого контроля, в том числе по паттерну «Признаки увольнения».

Более глубокий анализ показал, что, сравнивая активность коммуникаций всех работников компании, в том числе центрального офиса, система посчитала низкую активность в региональных подразделениях подозрительной и из-за этого ошибочно распределила сотрудников по соответствующим паттернам поведения. Если использовать модуль UBA для территориально распределенных компаний, такой ситуации не возникло бы.

В этом случае поведение пользователей анализируется отдельно в каждой организационной единице — к каждому филиалу применяется своя шкала, и баллы выставляются корректно. Поэтому мы не получим завышенные оценки в центральном офисе, где коммуникации сотрудников традиционно более интенсивные, заниженные оценки в региональных филиалах и особенно на складах, где коммуникационная активность работников, очевидно, значительно ниже.

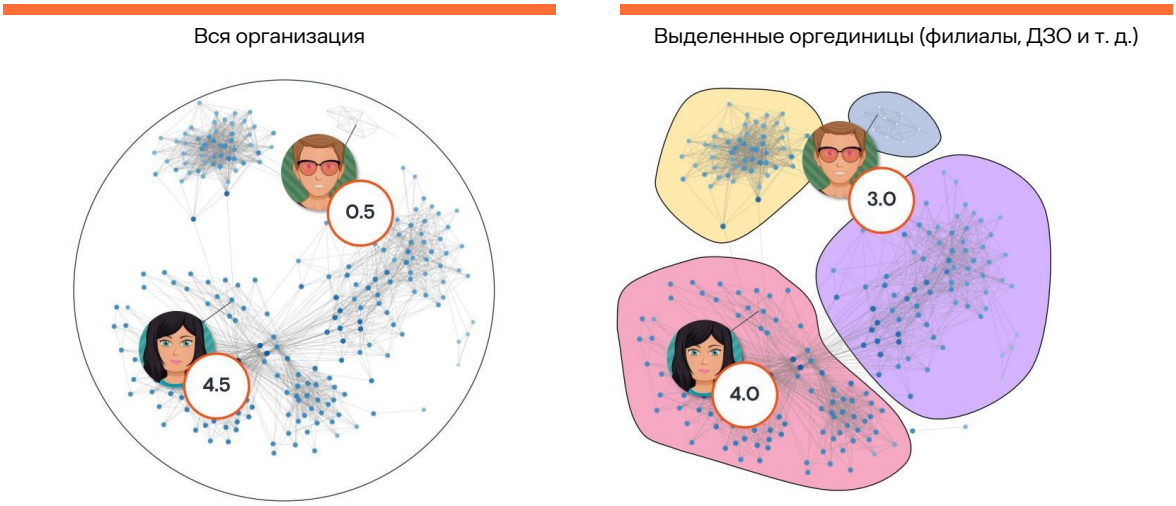


Рисунок 1. Ранговая шкала работников в зависимости от функционирования модуля UBA в территориально распределенной компании

Учет часовых поясов

Модуль MultiUBA позволяет задать для каждой организационной единицы свой часовой пояс. Это очень важно, так как в системе есть несколько поведенческих паттернов, связанных именно с суточной активностью пользователя. Среди них — признаки увольнения, работа ночью, работа в выходные дни и т. д. Для того чтобы проверять сотрудников территориально распределенных компаний по этим паттернам поведения, нужно учитывать местное время каждого филиала. Если система будет отслеживать начало и окончание рабочего дня, активность в ночное время или в выходные дни сотрудников сибирского филиала по московскому времени, мы получим распределение пользователей по паттернам, которое не соответствует действительности.

Пример. Офицер безопасности головного офиса крупной финансовой организации с отделениями по всей стране обращается к модулю UBA для ознакомления с ситуацией.

Он обратил внимание, что в паттерн «Работа в выходные дни» попал один из начальников отдела подразделения на Дальнем Востоке, что ранее было несвойственно для этой организационной единицы.

Зацепившись за этот факт, офицер безопасности проанализировал содержание писем, которые менеджер отправил субботним утром. Заподозрив признаки корпоративного мошенничества, ИБ-специалист передал информацию в отдел по экономической безопасности.

В итоге случайная находка, выявленная благодаря модулю анализа поведения пользователей, позволила предотвратить экономический ущерб организации, к которому могли привести недобросовестные действия начальника отдела в дальневосточном филиале.

Инцидент был выявлен именно благодаря тому, что в компании использовался модуль UBA для территориально распределенных организаций, который учитывал местное время.

Если бы система отслеживала действия пользователей, ориентируясь на часовой пояс головного офиса в Москве, она бы отметила, что начальник управления из этого примера засиделся допоздна в пятницу вечером, то есть в рабочий день.

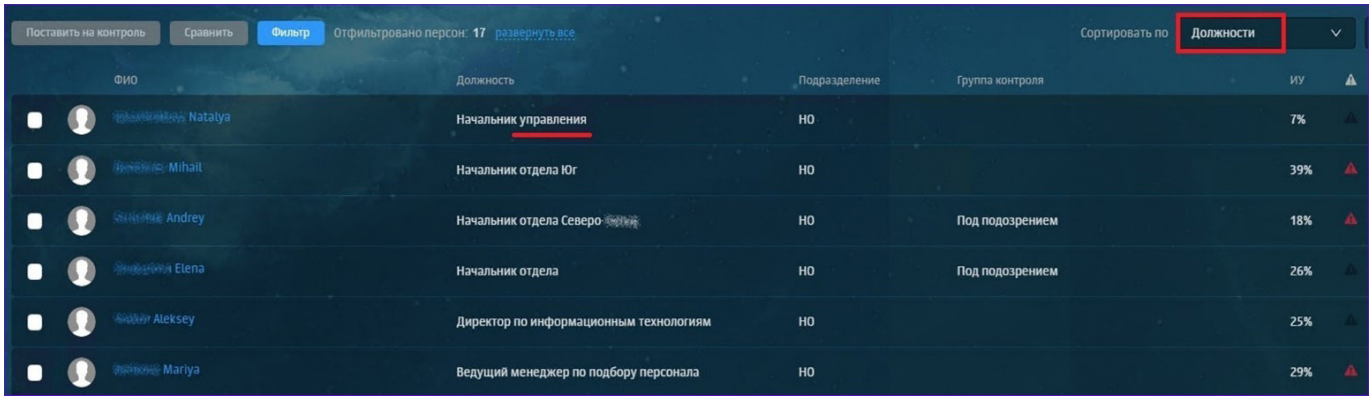


Рисунок 2. Паттерн «Работа в выходные»

Экономия ресурсов

Как правило, в территориально распределенной организации довольно много филиалов. Например, если компания представлена почти в каждом российском регионе, то их число может составлять несколько десятков. Чтобы офицеры безопасности имели возможность быстро работать с модулем UBA, в интерфейсе предусмотрен предварительный показ тех филиалов, где отмечено больше всего опасных и подозрительных тенденций по паттернам поведения и серьезных аномалий.

К серьезным аномалиям мы относим всплеск внешней активности и всплеск отправки информационных объектов, то есть писем с вложениями. Под тенденцией система понимает недельное изменение в паттерне поведения. Например, в филиале работали по ночам 25–27 сотрудников, и вдруг стали работать 60. Это подозрительная тенденция: может быть, крупный проект, а может, и признаки зарождающегося мошенничества. А если в паттерне «Признаки увольнения» было пять человек, а стало 25, то это опасная тенденция.

Специальный дашборд, на котором выводятся филиалы с такими тенденциями и аномалиями, позволяет офицеру безопасности более оперативно отреагировать на потенциально опасную ситуацию и вовремя принять меры. Кроме того, это бережет ресурсы службы ИБ, позволяя экономить время, которое могло быть потрачено на изучение десятков филиалов.

MultiUBA экономит не только ресурсы персонала, но и аппаратные мощности. Создание подкластера позволяет быстрее производить расчеты для модуля анализа поведения. Это особенно актуально для очень больших компаний, где десятки или даже сотни тысяч сотрудников и в обычной конфигурации модулю UBA приходится проводить анализ в огромной базе данных.

Кроме того, благодаря наличию организационных единиц мы можем разграничить права доступа офицеров безопасности и они будут видеть информацию только по своим филиалам.

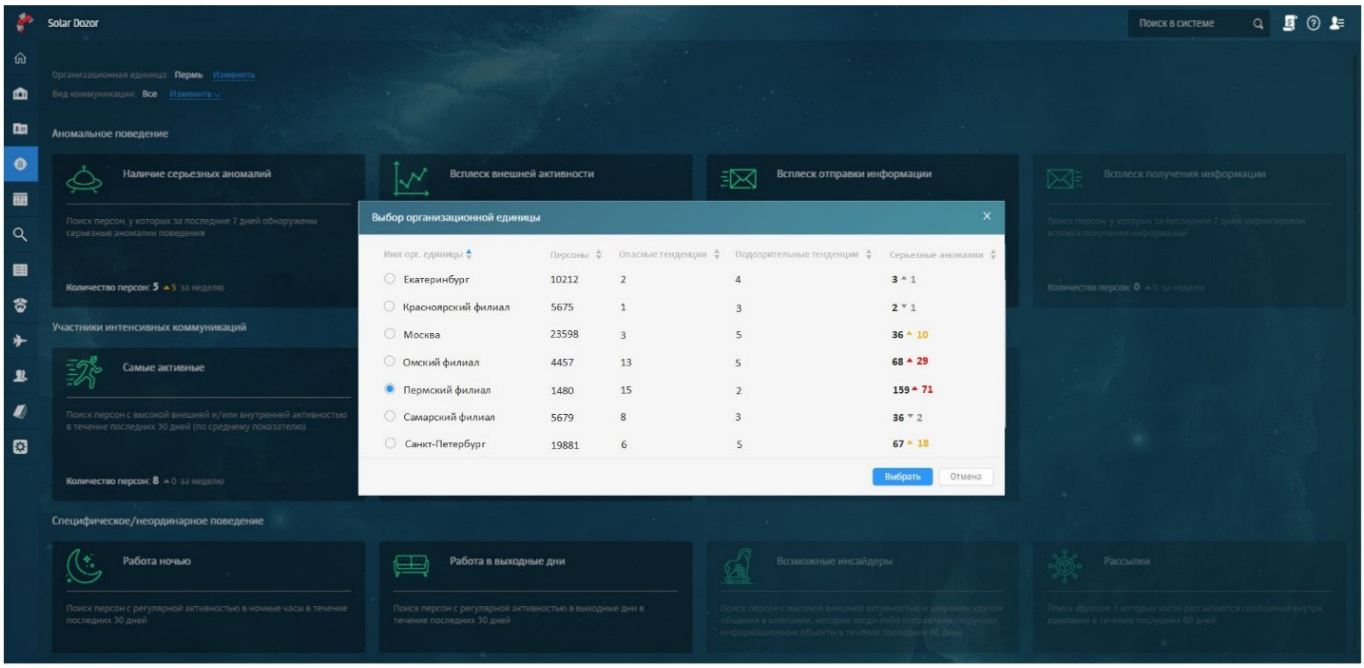


Рисунок 3. Дашборд с верхнеуровневой аналитикой по филиалам

Коммуникации между филиалами

При анализе коммуникаций в модуле UBA отдельное внимание мы уделяем так называемым особым контактам пользователя. К ним относятся:

- рабочая эго-сеть — плотный круг общения сотрудника внутри компании;
- неизвестные контакты — внешние контакты, которые есть только у данного сотрудника;
- приватная эго-сеть — контакты, с которыми сотрудник регулярно ведет переписку один на один, при этом больше никто в компании с ними не взаимодействует.

В случае с MultiUBA у нас появляется такая сущность, как кросс-филиальные особые контакты. То есть у сотрудника могут быть рабочие и приватные эго-сети с другим филиалом. Если рассматриваемый работник не единственный в своем филиале, кто взаимодействует с контактом из другой организационной единицы, мы получаем рабочую эго-сеть. Если же никто из его коллег с этим контактом из другого филиала не взаимодействует, формируется приватная эго-сеть. В случае с обычной версией модуля UBA у нас нет возможности фильтровать контакты по филиалам и отслеживать кросс-филиальное взаимодействие. А в некоторых ситуациях именно факт коммуникаций между сотрудниками из разных филиалов позволяет выявить возможные нарушения.

Пример. Перед выездом с рядовой проверкой в региональный филиал сотрудники службы безопасности производственного холдинга предварительно проводили оценку ситуации с помощью анализа данных DLP-системы в целом и модуля UBA в частности. Внимание специалистов привлек сотрудник экономического блока, активность которого сильно отличалась от общей по департаменту и филиалу в целом. Дополнительное изучение документов показало, что работник был принят в компанию вопреки отрицательному отзыву службы безопасности о нем.

Анализ контактов сотрудника выявил приватные эго-сети, в частности, он единственный из этого филиала регулярно переписывался с секретарем одного из топ-менеджеров компании из головного офиса. Дальнейшее расследование показало, что указанный сотрудник регулярно допускал нарушения, наносящие финансовый ущерб компании. А личные связи он использовал, чтобы руководство закрывало глаза на его действия.

Выводы

Чтобы эффективно анализировать поведение сотрудников и выявлять внутренние нарушения в территориально распределенной организации, нужно соблюдать ряд правил:

- Паттерны поведения нужно рассчитывать в разрезе филиалов, а не по всей компании в целом. Важно учитывать специфику коммуникаций в каждом филиале.
- Нужно учитывать часовые пояса — это позволит сократить число ложных срабатываний.
- Видение общей картины аномалий по всем организационным единицам помогает грамотно распределить ресурсы службы ИБ и сосредоточиться на наиболее опасных филиалах.
- Необходимо настроить ролевую модель для распределения областей видимости между офицерами безопасности.
- Важно учитывать коммуникации как внутри одного филиала, так и межфилиальные связи.

Максим Бузинов
Руководитель исследовательской группы
Центр технологий кибербезопасности
ГК «Солар»

СЮРПРИЗЫ АКЦИОНЕРНОГО ОБЩЕСТВА, ИЛИ КАК UBA ОБОГАЩАЕТ DLP

Метод анализа поведения применяется в самых разных сферах нашей жизни, от медицины и защиты природы до спорта и автомобилестроения. Действительно, о нас многое можно сказать по нашим поступкам. В информационной безопасности (ИБ) этот метод реализован в системах анализа поведения пользователей (UBA), появившихся на рынке около пяти лет назад. Эти технологии востребованы, поскольку основным источником угрозы в сфере ИБ считаются именно действия человека.

Пока на российском рынке существуют единицы подобных систем с подтвержденной практикой успешной эксплуатации.

Однажды в акционерном обществе

Этот случай произошел в карантинные годы. От генерального директора пришел запрос к модулю Dozor UBA нашей системы защиты от утечек (DLP) Solar Dozor на поиск выгорающих сотрудников. Та история, о которой пойдет речь ниже, была выявлена как бы побочно, но она очень показательна, так как то, о чем в ней говорится, актуально для многих организаций (особенно акционерных обществ).

Руководитель компании проводил поиск сотрудников, которые, с одной стороны, демонстрировали аномалию в поведении, выражавшуюся в резком и продолжительном снижении внутренней активности, а с другой стороны, имели отношение к критическим событиям, зарегистрированным DLP-системой. Такой поиск можно осуществить в паттерне «Риски», обладающем широким набором удобных фильтров. Таким образом, из 800 сотрудников организации генеральный директор отобрал трех человек.

Одна из них — сотрудница департамента по связям с общественностью Александра — имела в своем профиле много зарегистрированных событий безопасности именно за последние 3 недели. Частая проблема при использовании DLP-систем заключается в том, что зарегистрированные события безопасности (они, например, могут быть как ложноположительными, так и ложноотрицательными срабатываниями) отрабатываются специалистами служб безопасности по отдельности, и никто не ведет статистику, сколько событий было зафиксировано у каждого сотрудника компании. Благодаря же применению технологии UBA выяснилось, что за Александрой числится слишком много событий безопасности.

Специалисты службы безопасности знали, кто такая Александра, и посчитали, что для нее такая картина нормальна в связи с ее профессиональной спецификой: она периодически публиковала различные документы в СМИ и соцсетях. Однако если бы события регистрировались постоянно в ходе выполнения служебных обязанностей сотрудницы, то они бы обнаружились на протяжении всей ее работы, а не только за последние 3 недели.

Углубившись в изучение коммуникаций Александры, сотрудники службы безопасности установили, что та сливала ценную информацию, например содержание внутренней документации PR-службы компании, сопровождающей подготовку к тендерам PR-агентств. Сотрудница начала себя так вести, потому что собиралась увольняться и решила таким образом подзаработать.

Второй человек, попавший в настроенные фильтры, — юрист Анна. Как правило, юристам в организации очень сильно доверяют — чувствительность политик DLP-системы для их отделов снижена, так как они постоянно отправляют и получают важную информацию. Увидев Анну в списке отобранных системой сотрудников, специалисты службы безопасности не удивились, сославшись на то, что для юристов такая картина активности нормальна. Однако если бы это было так, то фильтр показал бы несколько юристов, а не одного. Тем более что для такой должности не характерно резкое продолжительное снижение внутренней активности.

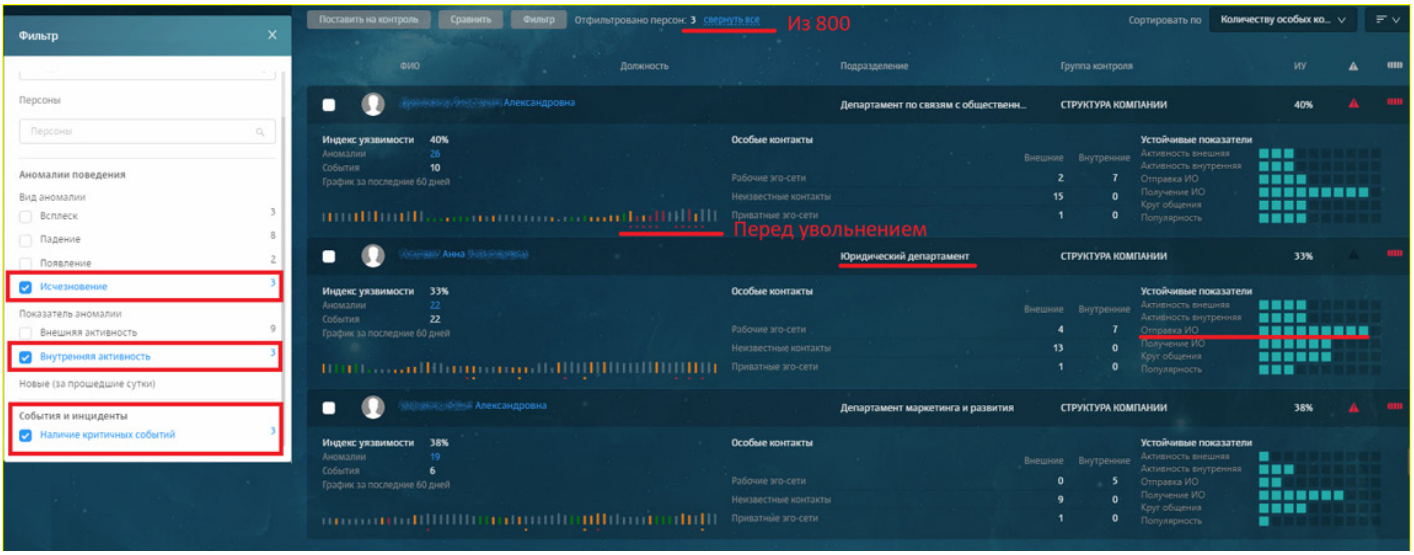


Рисунок 1. Регистрация событий перед увольнением

Когда стали изучать действия Анны, то обнаружили факт раскрытия ценной информации о досрочном погашении биржевых облигаций — для акционерных обществ это очень чувствительная информация. 13 августа Анна сначала отправила имеющуюся у нее информацию на согласование 15 законным инсайдерам, а через несколько минут переслала ее на личную почту. И только через четыре дня Анна официально отправила эту информацию на раскрытие.

Что произошло за это время? Оказывается, Анна продала информацию о раскрытии, так как мечтала погасить свою ипотеку за 3 года, а не за 30 лет. Третьи лица с использованием этих данных смогли отыграть торги ценных бумаг, из-за чего организация, в которой работала Анна, понесла большие убытки. Руководство организации не обращалось по этому поводу в правоохранительные органы, так как было очевидно, что в компании внутренние проблемы, а для акционерного общества признать такое — удар по репутации. После проведения расследования с применением Dozor UBA ситуация прояснилась, и менеджмент смог выдохнуть.

Почему Анна так себя повела? На самом деле она на протяжении длительного времени нарушала сначала менее критичные внутренние регламенты организации, потом — более критичные. И постепенно поняла, что такие действия остаются незамеченными и безнаказанными, поэтому окончательно осмелела и осуществила раскрытие очень ценной информации.

Как правило, такие проблемы часто возникают в крупных организациях, где очень много регламентов, а требования политик DLP для некоторых отделов смягчены, чтобы не дергать сотрудников службы ИБ каждый день по поводу отправки и получения информационных объектов.

Чем эти расследования оказались полезны сотрудникам службы безопасности? Во-первых, так как инциденты не регистрировались, заметить махинации с ценными бумагами без Dozor UBA было бы невозможно. Во-вторых, Dozor UBA позволила сотрудникам службы безопасности обратить внимание на тех сотрудников, которые на основании одной лишь DLP-системы никаких подозрений не вызывали.

Кроме того, при сливе ценной информации (о партнерстве со СМИ, досрочном погашении биржевых облигаций) не регистрировались события, то есть эти сливы прошли мимо DLP-системы из-за неточностей в настройках политик. Такое бывает, потому что регламенты и типы документов в компании постоянно изменяются, о чем службу безопасности уведомляют не всегда. Благодаря обнаруженным инцидентам в организации были изменены настройки действующих DLP-политик и они стали более точными и чувствительными. Все это — отличная демонстрация того, как анализ поведения пользователей обогащает DLP-систему.

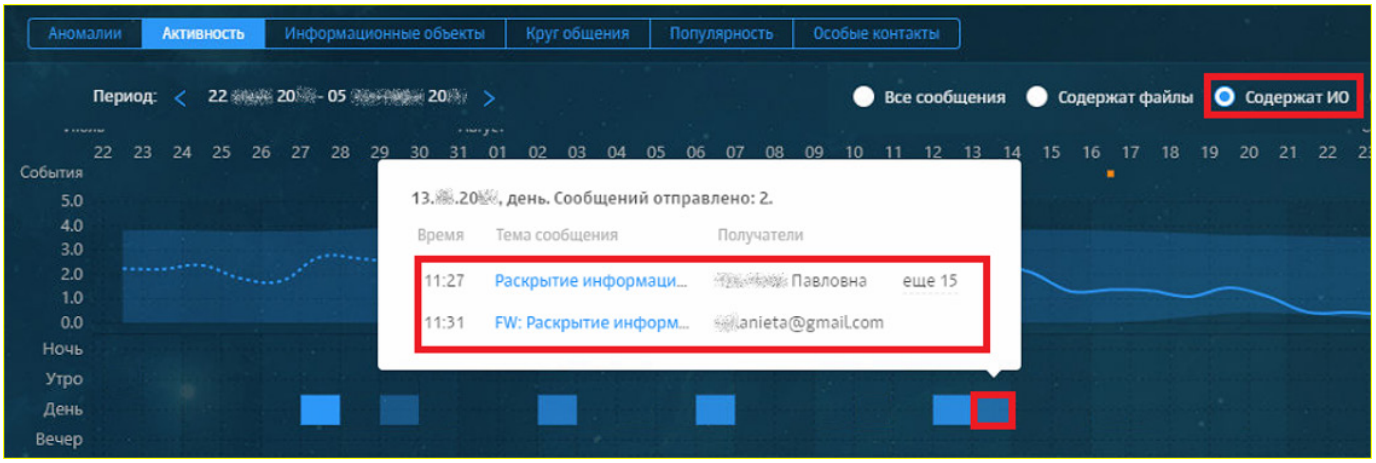


Рисунок 2. Коммуникация от случая к случаю

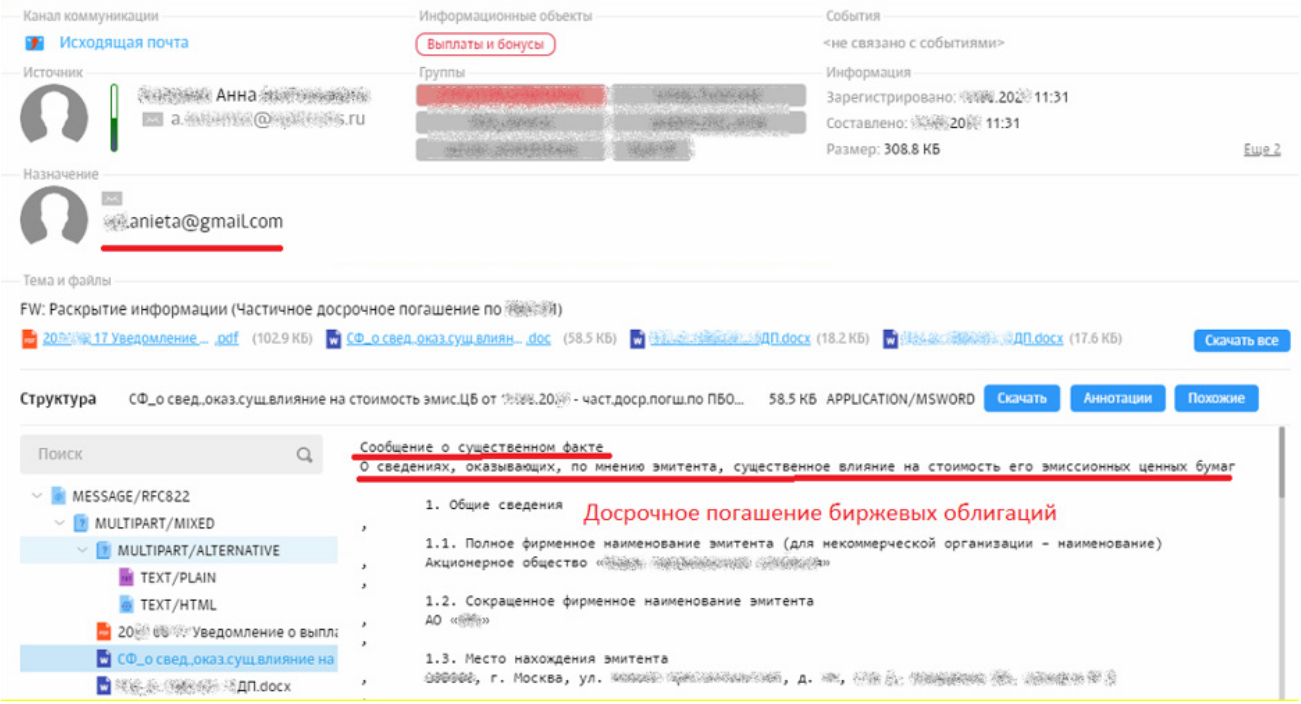


Рисунок 3. Слив ценных данных

Как правильно работать с UBA

Опираясь на реальный кейс, попробуем выделить оптимальную стратегию использования модуля поведенческого анализа Dozor UBA, работающего в синергии с DLP-системой Solar Dozor.

Сначала следует выделить крупные факторы риска, такие как всплеск отправки информационных объектов или внешней активности. По ним вы получите выборку объемом примерно в 50 человек. Сделать это можно с помощью паттернов или досье. Например, в кейсе, который мы обсудили в рамках этой статьи, был использован паттерн «Риски» — очень удобный и многофункциональный инструмент модуля Dozor UBA.

Затем нужно провести фильтрацию по специальным, более узким, рискам. Например, по рискам в области HR — используя анализ активности и популярности персон, или по рискам в области экономической безопасности — используя анализ особых контактов персон. Это ограничит выборку примерно до 10–15 человек, которых следует поставить на некоторое время на контроль. Сделать это можно с помощью настройки дополнительных фильтров. Например, в кейсе, который мы обсудили ранее, использовались фильтры «Исчезновение внутренней активности» и усиливающий фактор «Зарегистрированы критические события».

И наконец, следует найти самых выделяющихся сотрудников и провести расследование выявленных у них аномалий, сопоставить их с зарегистрированными инцидентами — это позволит сузить круг «подозреваемых» до 1–3 человек. Данный шаг уже требует ручного изучения суточной активности наиболее опасных с точки зрения безопасности сотрудников. В кейсе, о котором рассказывалось в этой статье, сотрудники службы безопасности просматривали исходящую коммуникацию сотрудницы департамента по связям с общественностью Александры и юриста Анны.

Выводы

Модуль Dozor UBA — это ценный инструмент обеспечения безопасности, функционал которого сфокусирован на аналитике действий человека. Свыше 40 российских компаний с числом пользователей более 36 000 человек в настоящий момент успешно применяют его для анализа поведения пользователей. Кроме того, модуль Dozor UBA — единственная на рынке запатентованная технология в этой области.

Она позволяет:

1. Полностью контролировать перемещение информации с ограниченным доступом, в том числе отслеживать неочевидные пути ее движения.
2. Контролировать внутренний климат в коллективе в рамках отдельных подразделений и в организации в целом, а значит, прогнозировать увольнения, замечать выгорание сотрудников и другие кадровые риски.
3. Выявлять среди сотрудников мошенников, участников сговора, инсайдеров и другие опасные группы.

Анастасия Тимошина
Аналитик данных
Центр технологий кибербезопасности
ГК «Солар»

НЕТИПИЧНЫЕ СЦЕНАРИИ ПРИМЕНЕНИЯ ПОВЕДЕНЧЕСКОГО АНАЛИЗА: РАЗБОР КЕЙСОВ

Как известно, в последние годы возможности присутствующих на российском рынке DLP-решений в части мониторинга поведения людей, а также выявления их эмоциональных особенностей и черт личности постоянно расширяются.

Каждое из представленных решений имеет ряд своих характерных особенностей, качественно отличающих его от аналогичного. Лишь опытный пользователь, опираясь на свой опыт и персональные приемы и установки в зависимости от условий труда и характера деятельности организации, способен безошибочно определить, насколько ему необходим и полезен определенный набор функций, присутствующих в том или ином решении.

Причем ввиду продолжительности присутствия на рынке DLP-систем с модулями поведенческой аналитики сформировалась и общность специалистов, успевших поработать за время своей профессиональной деятельности с различными решениями. Некоторые из них готовы не только высказывать свои предпочтения, но и, делясь актуальными кейсами, предлагать свои подходы.

Условно всех специалистов, имеющих опыт эксплуатации различных по типу модулей поведенческой аналитики, можно разделить на 2 категории:

01

Пилотировали/эксплуатировали все или некоторые из представленных основных решений и в каждом из них отмечают полезные для себя функции. Тем самым специалисты подтверждают целесообразность применения различных подходов, но отдают предпочтение какому-то конкретному.

02

Пилотировали/эксплуатировали все или некоторые из представленных основных решений, но приняли решение не вводить их в практику либо исключить из практики организации по различным причинам (указание руководства, отсутствие острой необходимости в анализе дополнительных данных, нехватка средств, времени, персонала и т. д.).

Если вторая категория пользователей — это работники и организации, которые в последующем наверняка вернутся к практике использования данных поведенческой аналитики, то первая категория — это лица и организации, вырабатывающие свой неповторимый и уникальный опыт работы с данными поведенческой аналитики.

Давайте рассмотрим эволюцию практического использования данных поведенческой аналитики, с согласия активных пользователей, разумеется.

Первоначально по итогам проведенных пилотов и проверенных методик осуществлялся мониторинг отдельных объектов — подконтрольных работников, групп работников (подразделений), лиц, включенных по поведенческой особенности (паттерн) в определенный список.

Такая практика безусловно давала свои положительные результаты, которые значительно улучшались по мере более полного понимания эксплуатирующими решение специалистами специфики внутренних процессов организации. В ряде случаев анализ данных позволял, что вполне закономерно, работать на предупреждение неблагоприятных последствий. Этому способствовало использование паттернов поведения (преобладание внешней активности, возможное инсайдерство, контакты с неизвестными и пр.) или специальных маркеров личности, применяемых в иных DLP-системах, благодаря психолингвистическому анализу, типизации характеров и пр.

Далее, по мере совершенствования практических навыков построения версий и их проверки, специалисты, например, стали причислять персону к категории «лидеры мнения/коллектива» только лишь из-за частого упоминания в переписке слова «срочно». Дело в том, что указание в переписке на срочность позволяет себе не только руководитель (лидер), но и рядовой сотрудник, который просит коллегу не тормозить рабочий процесс.

По той же аналогии примером будет дифференциация персон, включенных в паттерн «работа ночью». Сопоставление списка этих лиц и реальной ситуации в организации дает основание полагать, что люди, включенные в паттерн, — не потенциальные нарушители, а работники ночных смен (на производстве) или, например, бухгалтеры, которые сильно задержались на работе впервые за длительный период времени в таком большом составе, потому что «латали дыры» или «закрывали хвосты» перед длительными праздничными днями или в конце отчетного периода.

С приходом понимания, что между происходящими в организации рабочими процессами и предложенными к анализу поведенческими характеристиками существует очевидная связь, специалисты по безопасности «пристреливают прицел» в отношении способов интерпретации самих данных. Так, в ряде организаций — заказчиках DLP Solar Dozor с модулем поведенческой аналитики UBA — специалисты по безопасности до того четко связывают внутренние процессы организации, списки лиц, включенных в паттерны, должности, стаж работы, специфику условий труда и перечень решаемых работником вопросов, что порой выявляют нарушения в огромном массиве неочевидных и на первый взгляд незначимых явлений.

Так, например, произошло, когда в ходе профилактических мероприятий очередь дошла до целого подразделения — бухгалтеров отдельно взятого и достаточно удаленного филиала. В общем списке работников подразделения внимание привлек не тот, кто возглавляя список, числился во множестве паттернов, имел разнообразные персональные особенности, а, наоборот, тот, кто не был включен в значимые паттерны, не проявлял себя никаким особым образом, но выделяется из общего массива работников подразделения своей «монотонной идеальностью» на протяжении длительного времени. Таким работником оказался мужчина — рядовой бухгалтер со стажем работы в организации более семи лет.

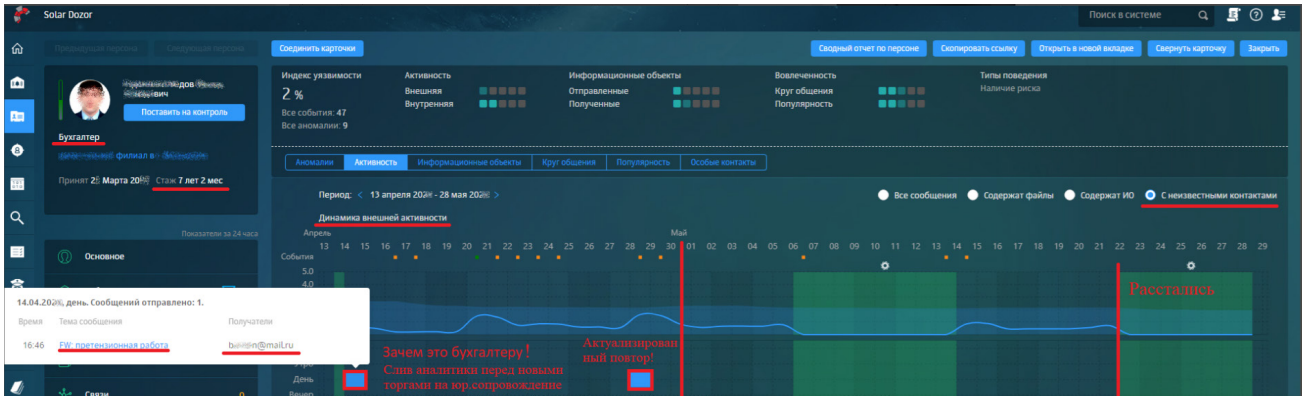


Рисунок 1. «Монотонная идеальность» рядового бухгалтера

Предположим, что бухгалтер организации ведет переписку со множеством контактов как внутри организации, так и вовне (контрагенты). Вычленить из большого массива данных ту переписку, которая могла бы вызвать подозрение, затруднительно. Полагаясь на это, вышеупомянутый бухгалтер осуществил пересылку на адрес электронной почты бесплатного сервиса файл, на содержание которого DLP-система просто не имела никакого шанса отреагировать, потому что соответствующий класс защищаемых сведений не был предварительно описан.

Файл содержал сведения о работе адвокатской конторы из Москвы, привлекавшейся для защиты интересов организации в региональном филиале (итоги работы, количество споров, их продолжительность, понесенные расходы, в том числе и командировочные). Данная информация была полезна получателю письма — адвокату региональной адвокатской конторы — для более успешного участия в ежегодных торгах на представление интересов. Располагая подобного рода сведениями, региональные адвокаты могли подготовиться к торгам, понимая, до какого предела может быть понижена цена контракта московских юристов.

Однако при обработке общего массива размером в 200 отправленных писем с помощью фильтра «С неизвестными контактами» на графике внешней активности отобразились только 2 письма, при идентификации получателя которых и был установлен местный адвокат. Очевидно, что после изобличения феерическая 7-летняя карьера бухгалтера прервалась.

Не стоит удивляться легкости и наглости реализации выявленной схемы. Опытные специалисты всегда негласно подтвердят, что чем крупнее организация, тем больше и нарушений.

В другом случае довольно длительной эксплуатации модуля UBA специалист по безопасности сумел правильно оценить объективную реальность: не сидел сложа руки в ожидании, когда технологии достигнут того уровня, что модуль UBA сможет контролировать большее количество каналов, или искусственный интеллект выставит его с работы. Специалист работал с тем, что есть здесь и сейчас, потому что приказы отдают и заработную плату платят тоже здесь и сейчас. В его распоряжении имелась связка DLP+UBA.
В отличие от DLP, которая ловит нарушения только по уже описанным правилам и словарям, мониторинг действий в UBA позволяет выявить и пресечь на ранней стадии потенциальные вредоносные действия.
В работе с модулем UBA этот специалист использовал свой собственный прием, знать о котором полезно и нашим читателям. Особенность подхода заключалась в использовании сразу двух графиков с привязкой к общим датам: внешней активности в корпоративной почте и внешней активности в мессенджере.

На графике внешней активности в корпоративной почте внимание безопасника привлекла дата — 1 августа, в которую работником было отправлено большее количество писем, чем в другие дни контролируемого периода. На графике же внешней активности, но уже в мессенджере в этот же день обнаружились коммуникации «С неизвестными контактами», чего ранее не наблюдалось.

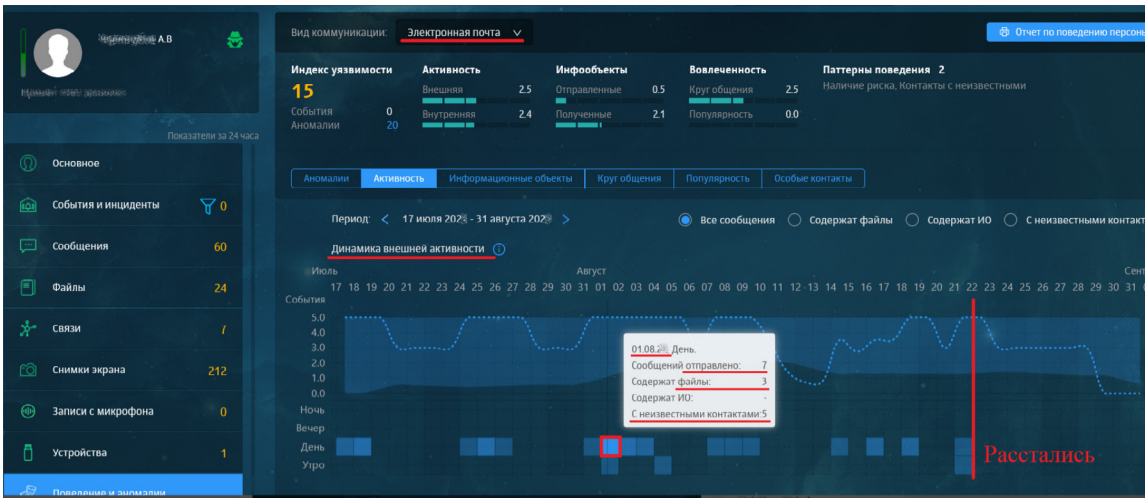


Рисунок 2. Показатели внешней активности в корпоративной почте. По состоянию на 1 августа

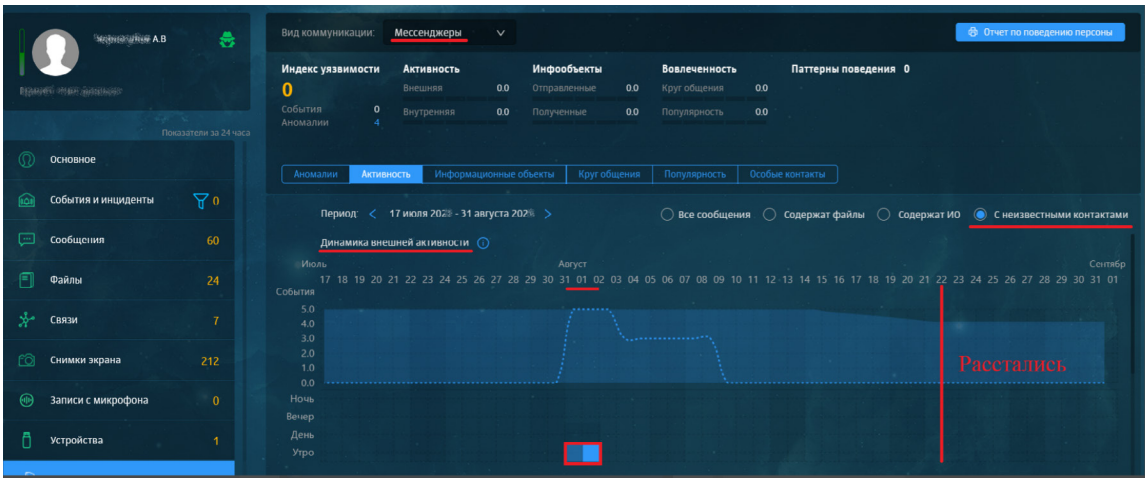


Рисунок 3. Показатели внешней активности в мессенджере «с неизвестными контактами».
По состоянию на 1 августа

В корпоративной почте обсуждались, с соблюдением правовых норм и корпоративных стандартов, механизмы выявления потенциальных коррупционноемких контрактов. В мессенджере же речь шла о тех же сделках, но уже неприкрыто говорилось о способах «дополнительного нетрудового заработка».

С учетом отдельных изъятий иллюстрируемый материал определенно указывает на наличие умысла совершения неправомерного действия. Но здесь важно не само нарушение, а способ его выявления: одновременный анализ данных двух графиков — внешней корпоративной почты и мессенджера — с привязкой к общим датам.

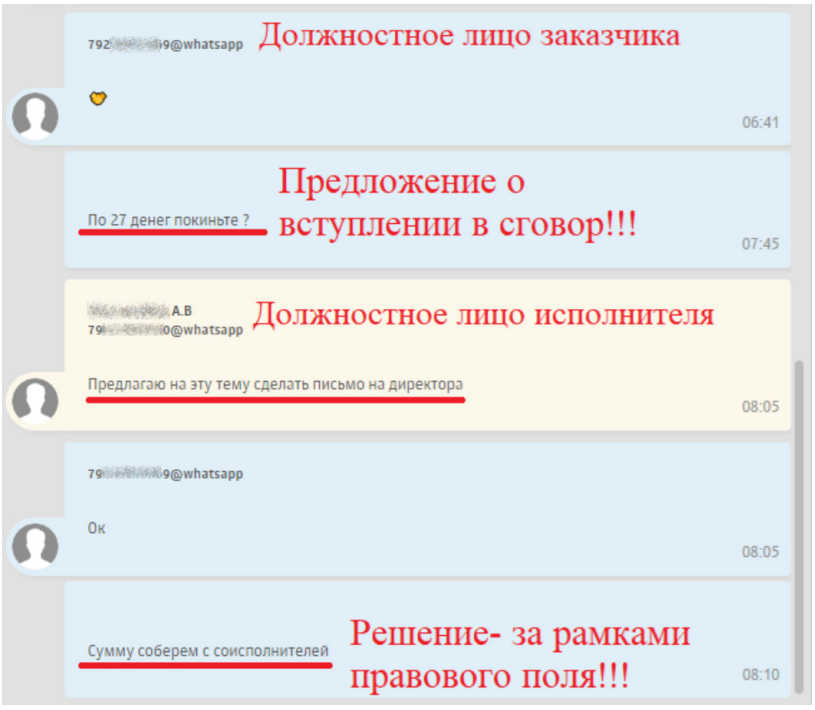


Рисунок 4. Способы «дополнительного нетрудового заработка»

Может сложиться ошибочное представление, что все системы контроля и мониторинга нужны лишь для наказания и изобличения нарушителей. В некоторых организациях — наших заказчиках — компетенция специалистов по безопасности, их опыт, в том числе взаимодействия с иными подразделениями, адекватная оценка происходящих в организации событий, дают возможность использовать их и с целью выявления положительных явлений: взаимовыручки, усердия, добросовестного отношения к общему делу.

Так, с учетом недопустимости публикации служебных материалов мы все же сможем на одном примере, весьма наглядном, продемонстрировать, как модуль UBA позволил выявить случай добросовестного отношения к труду.

В процессе мониторинга действий одного ответственного работника безопасники обратили внимание на факт, выбивающийся из общей картины его персональной практики, — получение писем в ночное время.

Увидев в необычной ситуации потенциал для выявления проблем на рабочем месте, сотрудники службы безопасности просмотрели ночное сообщение сотрудника и обнаружили неожиданный и приятный факт: этот сотрудник, и не только он, проявил усердие в работе.

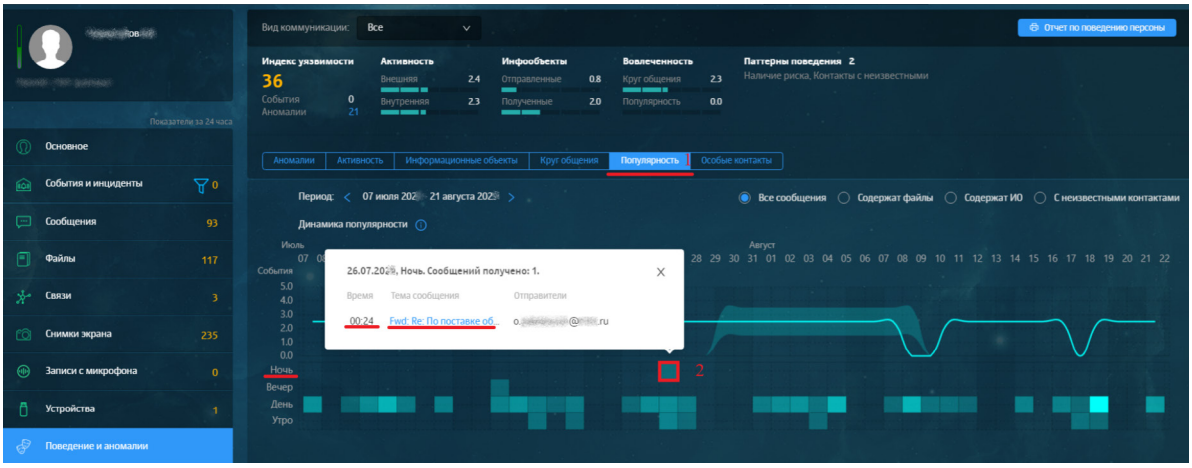


Рисунок 5. Получение сообщения в ночное время

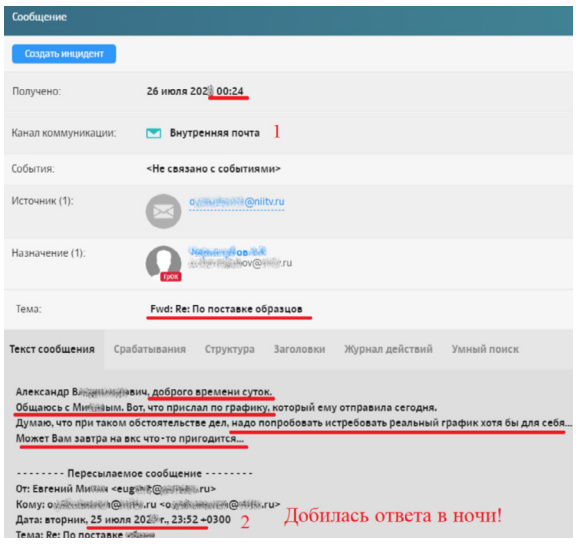


Рисунок 6. Ночное сообщение работника

Из ленты переписки (рис. 7) видно, что группа работников организации для решения срочной задачи дает реальную оценку ситуации, оперативно предпринимает массу возможных действий, в инициативном порядке информирует руководителя подразделения. Притом многие из действий они производят за рамками служебного времени.

Демонстрируемый случай свидетельствует о благоприятном климате в коллективе, высоком уровне профессионализма, ответственности, правильном распределении ролей и даже, на будущее, хорошем кадровом потенциале, перспективах карьерного роста работников и безусловной обоснованности их материального поощрения.

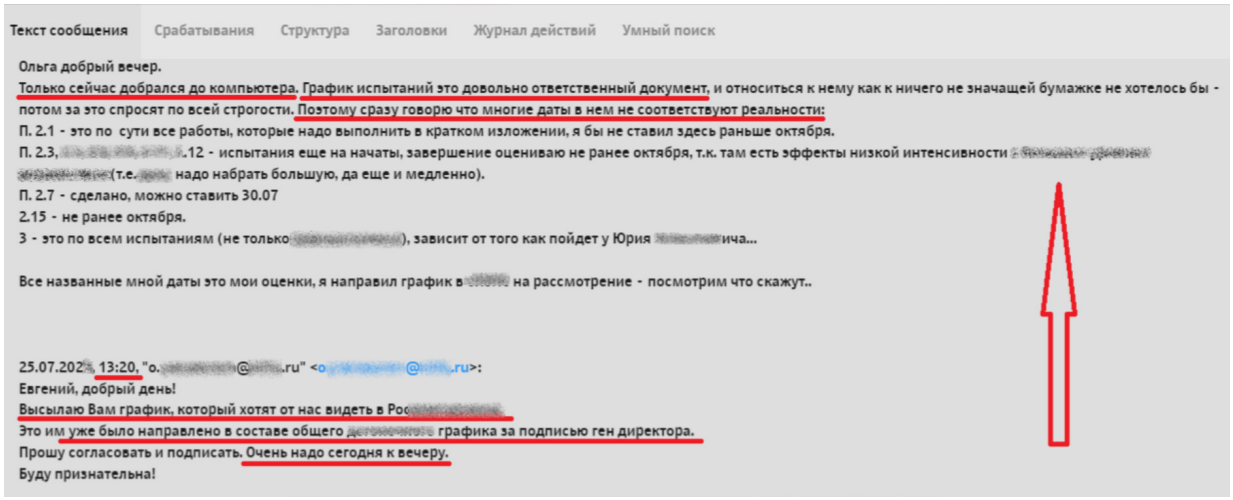


Рисунок 7. Оперативное информирование руководителя вне рабочего времени

Выводы

Предлагаемый на сегодняшний день модуль поведенческой аналитики — рабочий инструмент специалиста, желающего работать и выдавать результат здесь и сейчас. Специалиста, который понимает, что технологии развиваются и совершенствуются постепенно, и процесс этот бесконечен, а работа, протекающая в данный момент, требует не простого номинального мониторинга по массе параметров, а эффективного выявления и реагирования. В этой связи специалисты по безопасности применяют, проверяют и совершенствуют не просто шаблоны, но и свои личные наработки, часть из которых мы и попытались вам продемонстрировать.

Виталий Петросян
Эксперт группы анализа и методологии
Центр технологий кибербезопасности
ГК «Солар»

КАК АГЕНТСКАЯ ПОЛИТИКА В SOLAR DOZOR ПОМОГАЕТ БОРОТЬСЯ С УТЕЧКАМИ ИНФОРМАЦИИ

Как известно, в общей массе утечек информации велика доля тех, которые происходят непосредственно с рабочих компьютеров. Рассказываем, как правильная настройка агентской политики помогает эффективнее бороться с такими утечками в компании.

Из недавних исследований ГК «Солар» видно, что более половины всех выявленных в российских компаниях утечек информации происходит с рабочих станций пользователей. Нарушители либо отправляют конфиденциальную информацию за периметр организации через личную электронную почту, либо выкладывают ее в облако, скажем на «Яндекс.Диск», либо выносят физически, записав на флешку или распечатав документ на принтере. Основным «лекарством» для сокращения таких утечек является, безусловно, ограничение этих каналов. Что, конечно же, нереализуемо в полной мере, да и введенные ограничения имеют пределы: не всегда можно полностью запретить запись на флешку или печать — это прямое вмешательство в бизнес-процессы, а бизнес очень не любит, когда ему мешают. Получается, что угроза утечки есть, полностью убрать ее нельзя. Зато можно снизить риск ее возникновения. Для этого следует внедрять ИБ-решения, которые будут эффективно обрабатывать информационные потоки непосредственно на рабочих станциях сотрудников.

Немного агентской теории

Именно для этих целей производители DLP-систем активно развивают функциональность агентов для конечных точек. Да, агент, установленный на автоматизированном рабочем месте (АРМ) пользователя, уязвим для действий злоумышленника: при наличии у того определенных знаний в ИТ, а тем более при имеющихся изъянах в обеспечении безопасности АРМ, появившихся по вине нерадивых системных администраторов, агент можно удалить или повредить.

Тем не менее попытки его удаления хоть и могут привести к кратковременному снятию защиты, но не останутся незамеченными офицерами ИБ, при этом сам агент обладает рядом уникальных свойств, позволяя перехватывать практически любую информацию с контролируемой рабочей станции, что делает его незаменимой частью любой уважающей себя DLP-системы. Но написать и предоставить заказчику агент, перехватывающий трафик, — только полдела. Еще надо создать механизм управления агентскими политиками — правилами, с помощью которых агент будет выявлять и эффективно блокировать действия пользователя, несущие прямую либо потенциальную угрозу организации.

Такие политики должны быть:

а) гибкими и точными,

б) удобными в настройке.

Точность и гибкость политики необходимы для гарантированного выявления попыток утечки информации, но не только. Еще они нужны для снижения (а в идеале — исключения) ложноположительных срабатываний (ЛПС) агента, ведь каждая агентская блокировка — это прерывание бизнес-процесса, и если это прерывание произошло из-за ЛПС, то есть ошибочно, то каждая такая ситуация, конечно, выставляет DLP-систему (да и ИБ в целом) не в лучшем свете.

Удобство, простота настройки политики нужны для того, чтобы работа с ней не превратилась для офицера ИБ в отдельный трудоемкий процесс, требующий специальных академических знаний, длительной переписки с вендором и большого количества времени. Известно, что во «взрослых» DLP-системах агент для конечных точек — это программа, устанавливаемая на подконтрольное АРМ единым пакетом.

При этом, если заглянуть агенту «под капот», мы увидим, что за различные перехваты в системе отвечают отдельные модули — перехватчики, к которым применимы разные условия политики, иногда совершенно несовместимые между собой. Так, например, при блокировке запуска нежелательного приложения политике надо сообщить его имя, а при блокировке записи информации на внешний носитель — текст, содержащийся в копируемом файле.

Иначе говоря, каждый перехватчик в агенте нужно настраивать отдельно. Но в декабре 2022 года «РТК-Солар» выпустил новую версию своего флагманского продукта Solar Dozor 7.8, в которой представлена переработанная агентская политика: настройка всех перехватчиков происходит в одной точке по единым стандартам. Делается это в обновленном интерфейсе, а сам процесс настройки политики стал еще более простым и удобным (рис. 1).

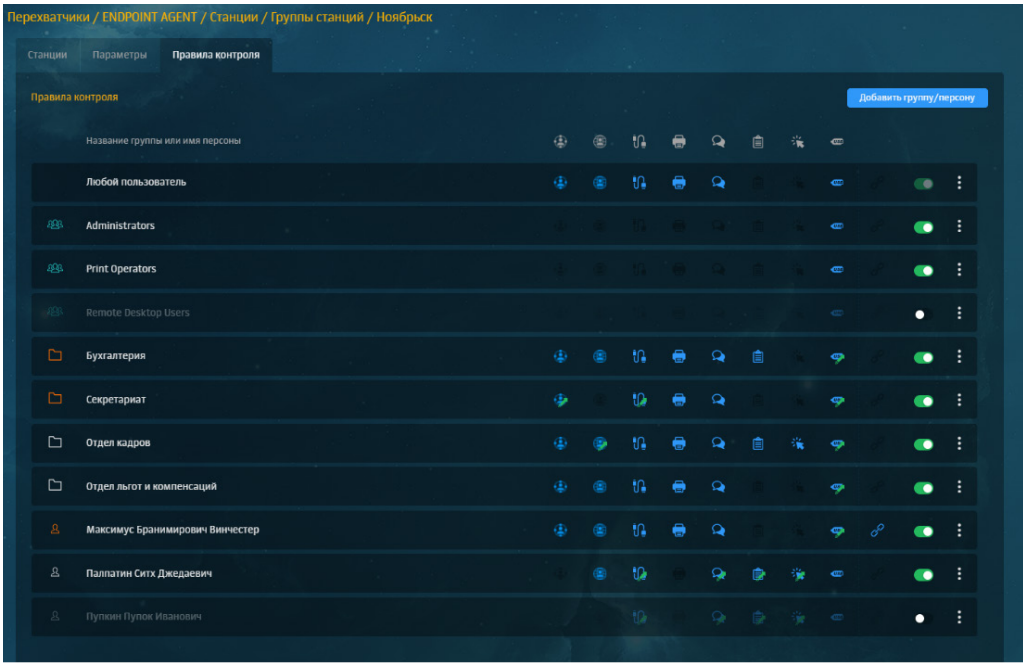


Рисунок 1. Настройка правил контроля информации

Агентские политики в Solar Dozor описываются в специальных правилах контроля и настраиваются применительно к пользователям и их группам. Это могут быть как группы Active Directory (AD) — OU (Organizational Unit) или безопасности, — так и группы, созданные непосредственно в DLP-системе. В каждом правиле контроля описывается набор правил для всех доступных каналов агентского перехвата: условия блокировки печати на принтер, записи на съемный носитель, публикации информации в сети и т. д. При этом в политике разрешено использование только тех правил и условий, которые применимы для конкретного канала перехвата. Если же контроль какого-то канала для группы пользователей не требуется, его можно легко отключить. Для удобства настройки эти правила можно копировать. Это полезно в том случае, если есть необходимость использования похожих правил контроля для разных пользователей/групп. Но если одно и то же правило контроля планируется без изменений применять для множества групп, тогда, чтобы не дублировать одинаковые правила, не тратить время на их копирование и постоянную поддержку, можно назначить нужное правило контроля как шаблон и определить его для контроля действий других пользователей/групп либо использовать в других группах станций. Тогда разовое изменение правил в шаблоне приведет к соответствующему изменению всех связанных с ним правил контроля. Важно отметить, что один пользователь может присутствовать в различных группах AD, а в процессе эксплуатации DLP-системы правил агентской политики может быть настроено много, в том числе для разных групп, куда могут входить одни и те же пользователи (например, если на контроль поставлены группы OU разной вложенности). В Solar Dozor предусмотрен специальный механизм, исключающий конфликт применения политик из разных групп: для каждого пользователя применяется конкретная политика, скомпилированная по понятной логике.

И много агентской практики

Теперь о практике. Как уже было сказано, агентская политика в Solar Dozor применяется к пользователям/группам, то есть пользователь, к какому бы АРМ он ни подключился, получит агентскую политику, которая предназначена именно ему. Рассмотрим подсказанные жизнью примеры. Можно настроить такую политику, когда сотрудник отдела кадров, подключившись к любому АРМ своего подразделения, будет иметь одинаковые правила и ограничения.

При этом если такой сотрудник подключится к АРМ, скажем, бухгалтерии (то есть чужому для него), то он получит крайне ограниченные права, не разрешающие ему какую-либо активность. В случае же если сотрудник отдела кадров посетит филиал своей организации в другом регионе, он, подключившись там к АРМ филиального отдела кадров, получит точно такие же разрешения, как если бы он работал в своем офисе — ведь это такой же отдел кадров с теми же разрешениями (рис. 2). Либо наоборот: для него в филиале можно настроить ограниченные права как для гостя.

Рисунок 2. Настройка шаблона правил контроля для отдела кадров

Другой пример. Для системного администратора, который в силу своих обязанностей может заходить на АРМ любых пользователей, можно разрешить запуск на них любых процессов, при этом запретить для него запись информации на съемные носители.
Еще один сценарий. Сотрудник переводится из одного подразделения в другое — скажем, из отдела кадров в отдел льгот и компенсаций — со своим ноутбуком. Набор информации (в том числе и конфиденциальной), с которой будет работать сотрудник, несколько отличается от того, с чем он работал раньше. Следовательно, и ограничения в агентской политике для другого подразделения должны быть иными.

Тем не менее при переводе сотрудника с одной должности на другую (и, соответственно, смене OU в AD) на ноутбуке пользователя автоматически заработает агентская политика, определенная уже для отдела льгот и компенсаций, а не для отдела кадров.
При этом офицеру ИБ в DLP-системе никаких специальных действий производить не потребуется (рис. 3).

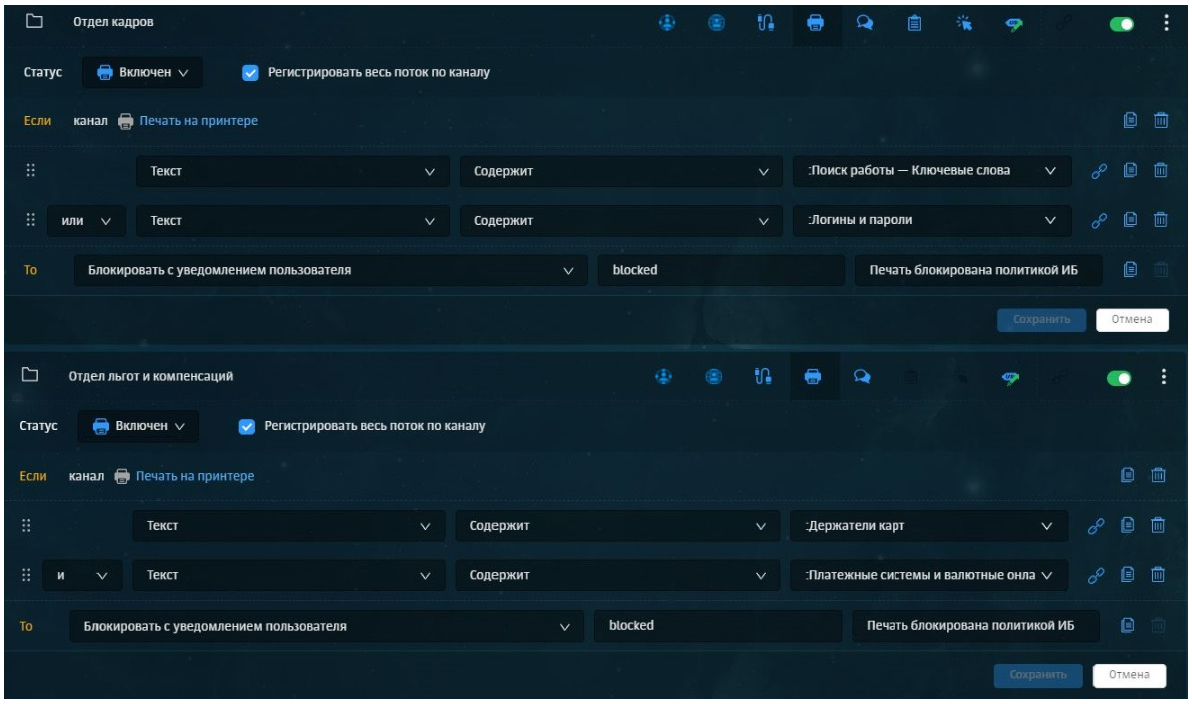


Рисунок 3. Настройка правил контроля при переводе между подразделениями

Таким образом, в Solar Dozor агентская политика по группам/пользователям работает схоже с групповыми политиками AD, но настраивается непосредственно в DLP-системе. При этом агентская политика даже частично дублирует системные функции.

Так, с ее помощью, например, можно ограничивать использование съемных носителей информации: наличие сотрудника в той либо иной группе может означать для него разрешение (либо наоборот — запрет) на использование флешки. Это особенно полезно в ситуациях, когда подразделению ИБ по каким-то причинам затруднительно взаимодействовать с отделом системного администрирования либо такое взаимодействие недостаточно оперативно. В этом случае подразделение ИБ может самостоятельно управлять некоторыми правами, назначая пользователям либо группам какие-либо правила и ограничения только за счет ресурсов своей DLP-системы.

Здесь уместно рассмотреть еще один кейс. Сотрудник пытается совершить некое нарушение, настолько серьезное, что требуется не только пресечь это действие, но и незамедлительно принять меры по ограничению активности этого пользователя для недопущения рецидивов. Для этого в политике Solar Dozor есть специальное правило, по заданному условию помещающее нарушителя в группу особого контроля, для которой в агентской политике прописаны свои особые правила, полностью блокирующие взаимодействие подконтрольной рабочей станции с внешним миром. Что важно, все это происходит в автоматическом режиме.

В итоге нарушитель не сможет повторить нарушение, что дает офицеру ИБ время отреагировать на инцидент. Мы видим, что настройка агентской политики в зависимости от конкретных пользователей или групп значительно повышает эффективность работы агентов. Но что делать офицеру ИБ, если он хочет использовать одну политику для всех агентов? В таких случаях можно использовать политику «Любой пользователь», которая будет применяться для всех агентов Solar Dozor по умолчанию.

Передача и хранение данных

Теперь немного о передаче и хранении агентских данных. Вся информация об активных действиях агентов (например, о том, что агент заблокировал попытку записи на носители файла с информацией, составляющей коммерческую тайну) в любом случае должна передаваться в DLP-систему для дальнейшего разбора. В Solar Dozor так и есть. Но для обеспечения оптимального использования объемов файлового хранилища DLP-системы Solar Dozor можно управлять объемом поступающего от агентов трафика. На больших инсталляциях такой трафик достигает значительного объема и нагружает не только систему хранения данных, но и сеть. В Solar Dozor с помощью специальной настройки можно ограничивать поток событий отдельно по каждому каналу агентского перехвата.

Так, агент может отправлять в DLP-систему все события, обработанные перехватчиком, — например, по любым файлам, записанным на съемный носитель; тогда оператор системы будет иметь полное представление обо всех операциях записи на флешку, совершенных пользователем. Если же такой необходимости нет, то агент следует настроить на передачу в Solar Dozor только ограниченного числа событий, например связанных с записью на флешки технической документации. Данную настройку можно менять для различных пользователей/групп в зависимости от критической значимости данных, ими обрабатываемых.

Выводы

Размеры статьи, к сожалению, не позволяют рассказать обо всех возможностях новой агентской политики: представленные сценарии раскрывают только некоторые из них. Но из написанного видно, что в Solar Dozor политику можно настроить весьма гибко. Вообще, чем качественнее в DLP настроена политика, тем меньше рисков утечки конфиденциальной информации из компании.

И это касается не только лишь агентской части, но и всей системы в целом. А для настройки такой качественной политики от DLP требуется наличие развитых аналитических возможностей — правил и условий. Solar Dozor этими возможностями обладает. Как, собственно говоря, и положено одной из передовых российских DLP-систем.

Дмитрий Мешавкин
Руководитель группы продуктовой аналитики
Центр технологий кибербезопасности
ГК «Солар»

РАЗВЕРТЫВАЕМ ENDPOINT-АГЕНТЫ ЛЕГКИМ ДВИЖЕНИЕМ РУКИ

Любая DLP-система имеет серверную и агентскую часть, а значит, при ее внедрении в крупных организациях приходится разворачивать агенты мониторинга на большом количестве рабочих станций. Часто у компаний возникают вопросы: как упростить процедуру управления агентами и их развертывания? И какие нестандартные сценарии при этом должен предусмотреть вендор?

Рассмотрим нюансы развертывания агентов, контроля их состояния и диагностирования возникающих проблем на примере нашей системы предотвращения утечек информации Solar Dozor.

Для начала посмотрим, как устроены сопряженные с процедурой развертывания инструменты и процессы. Здесь можно открыть для себя немало интересного, в особенности если вы уже являетесь пользователем аналогичных систем и сталкивались со сложностями при развертывании агентов.

Итак, агенты DLP-системы Solar Dozor контролируют такие каналы передачи данных, как мессенджеры, съемные носители, облачные сервисы, принтеры и другие. В нашей практике Dozor Endpoint Agent не раз предотвращал утечки через эти каналы. Например, сотрудник перед увольнением решил «прикопать» себе с десяток документов для дальнейшего использования на другом месте работы.

Другой захотел обогатиться и слить базу клиентов конкурентам. А третий при копировании фотографий с корпоратива на флешку «случайно» прихватил и папку с фотографиями паспортов клиентов.

Для администраторов DLP-системы важно, чтобы все задачи решались предельно просто и легко можно было понять, все ли сделано корректно. Ведь, как правило, работают с системой от одного до нескольких десятков человек, обеспечивая безопасность конфиденциальных данных компании с численностью сотрудников от 10 до нескольких сотен тысяч(!) человек. Согласитесь, весьма не просто было бы выполнять такую работу, не используя подобные системы.

Информация о станциях и управление агентами

Агент DLP-системы Solar Dozor является клиентским приложением. Перед тем как начать процедуру развертывания агента, нам необходимо «познакомить» серверную часть с рабочей станцией, которую предполагается взять под контроль. И это самое знакомство не должно оказаться для станции, ее пользователя и администратора системы чем-то шокирующим. Все должно пройти максимально деликатно.

В нашей DLP-системе предусмотрено несколько способов провести удачное «знакомство». Самым быстрым является добавление АРМ (автоматизированное рабочее место) вручную по IP-адресу или hostname. Используя этот метод, пользователь получает возможность сразу отнести АРМ к нужной группе с необходимыми настройками и дистрибутивами агента.

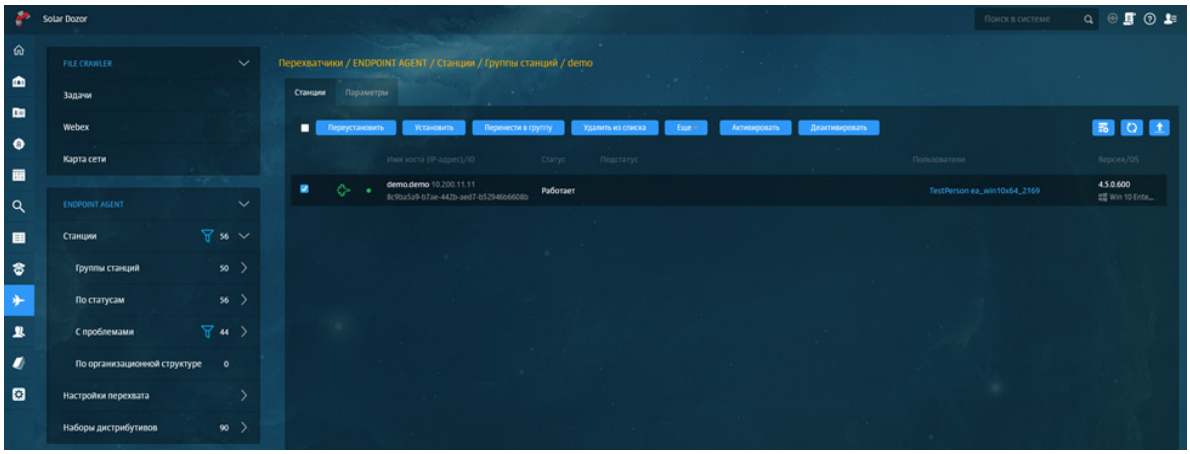


Рисунок 1. Внешний вид интерфейса системы, зона «Перехватчики: Endpoint Agent»

Предварительная настройка серверной части позволяет синхронизироваться с Active Directory (AD) и добавлять станции в пару кликов. Конечно же, предусмотрен вариант и для небольших компаний, которые не имеют в своем арсенале AD. Они могут проделать данную операцию, явно указывая имя хоста или IP-адрес АРМ.

Однако наша DLP-система этим способом не ограничена. Разработанный ГК «Солар» специальный модуль развертывания может попасть на подконтрольную АРМ несколькими способами на выбор. Это могут быть сторонние средства, такие как групповые политики AD, корпоративное ПО, способное выполнять функцию установки/удаления ПО, или же можно установить модуль вручную.

После установки и запуска модуль отправляет в Solar Dozor необходимую для регистрации АРМ информацию. Серверная часть ее обрабатывает и регистрирует АРМ во временной группе в списке станций. При этом запись получает статус «Ожидает распределения по группам», который подсказывает администратору дальнейшие шаги для выполнения установки Dozor Endpoint Agent.

Администратору системы доступна следующая информация по добавленной станции:

- имя хоста и IP-адрес,
- имена сотрудников, использующих станцию,
- информация об установленной ОС (в том числе ее версия),
- версия установленного агента.

Замечу, что при необходимости можно экспортировать информацию о рабочих станциях в виде файла.

Если говорить о способах установки агента, то здесь предусмотрен весьма широкий спектр разнообразных вариантов. Самые основные:

- Установка вручную.
- Установка через пользовательский интерфейс Solar Dozor.
- Установка с помощью сторонних средств централизованного развертывания ПО.

Отдельно отмечу, что предусмотрено все необходимое для установки и использования агента в VDI-среде.

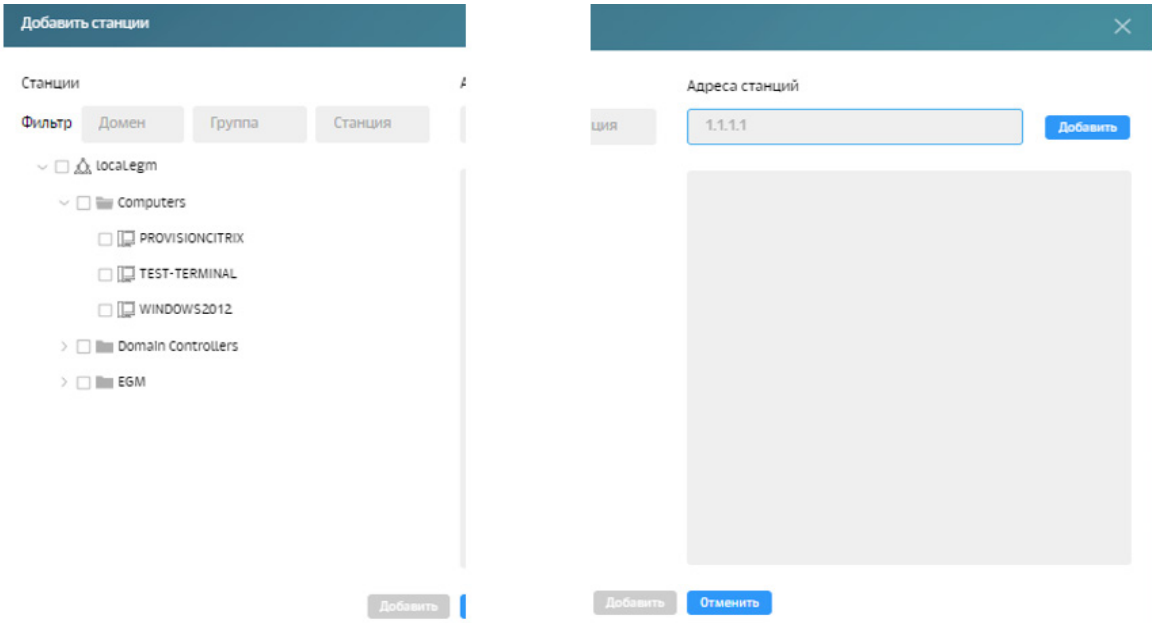


Рисунок 2. Инструмент для добавления рабочих станций

Диагностирование проблем и рекомендации по их решению

Часто в случае возникновения каких-либо ошибок при работе с программным обеспечением (ПО) пользователю достается в лучшем случае всплывающее окно с кратким описанием проблемы.

Бывает, что вместо понятной ошибки выдается только код этой самой ошибки. При этом для разбора проблемы пользователь вынужден либо анализировать журналы ПО, либо искать ответы где-то еще (техническая поддержка, интернет и т. д.).

Но есть и еще один важный нюанс — это локализация выводимой информации. Надо учитывать, что пользователи могут испытывать сложности в разборе ошибки, описанной на иностранном языке, да еще и словами, понятными только ИТ-специалисту.

Агенты DLP-системы — это такое же ПО, при работе с которым могут возникать различные проблемы. И часто с такими системами работают сотрудники, у которых могут возникать сложности с анализом ошибок технического плана.

Проблемы могут быть разного характера. Например, такие, как:

- проблемы с доступностью станции при развертывании агента (отсутствует доступ к станции по протоколам SMB или WinRM);
- проблемы с учетной записью администратора, используемой для доступа к станции (некорректные учетные данные, отсутствие необходимых прав);
- наличие компонентов конфликтного ПО;
- отсутствие необходимых обновлений ОС или неподдерживаемая версия ОС.

Для выявления, решения и предотвращения таких и аналогичных проблем необходимо, чтобы система могла их корректно диагностировать.

Но выявить проблему — это лишь часть задачи. Нужно также предложить пользователю способы ее решения. Ну или хотя бы предоставить максимум информации, благодаря которой пользователь мог бы сам решить, какие действия необходимо предпринять.

Надо понимать, что инфраструктуры компаний очень сильно различаются. И при разработке DLP-системы необходимо учитывать множество факторов и условий, при которых система и все ее компоненты должны функционировать корректно. Очевидно, что не всегда удается предусмотреть все случаи. Не говоря уже о непредвиденных обстоятельствах, когда компании вынуждены крайне оперативно вносить изменения в существующую инфраструктуру.

Когда возникает проблема, которую решить силами заказчика невозможно (отсутствие возможности внесения изменений в инфраструктуру), можно попробовать найти обходной путь решения исходя из имеющегося функционала. Если и тут ничего не помогло, то остается только один вариант — доработка продукта.

При возникновении нестандартных ситуаций, когда не ясно, где именно «прячется» проблема с развертыванием агента (проблема с подключением к станции, проблемы с самой станцией и т. д.), для пользователя произошедшее выглядит как «установка агента прервана по неизвестным причинам», и для выяснения истинных причин ему приходится тратить немало времени.

С целью минимизации возникновения подобных ситуаций необходимо улучшать и развивать имеющуюся систему диагностирования проблем.

Диагностика проблем доступности станции

Бывает так, что станция, на которую необходимо установить агент, по тем или иным причинам оказывается недоступна для подключения по протоколу, выбранному пользователем. Например, отсутствует связь по протоколу SMB.

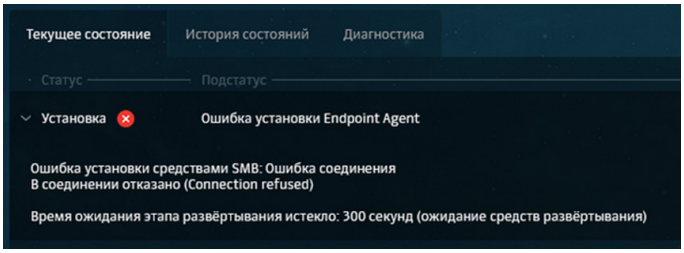


Рисунок 3. Ошибка установки Endpoint Agent из-за отсутствия доступа к станции по протоколу SMB

Часто встречаемая проблема, и необходимо максимально понятным языком ее обозначать.

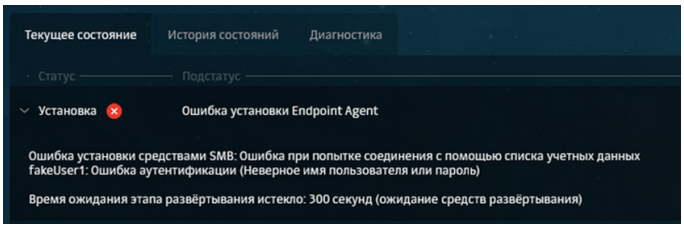


Рисунок 4. Ошибка установки Endpoint Agent из-за неподходящей пары логин/пароль

Может оказаться, что на станции присутствует ПО, которое вызывает проблемы при работе агента. Например, агент будет работать некорректно. А может и вовсе привести к тому, что операционная система (ОС) начнет «уходить» в т. н. «синий экран» (он же «экран смерти»).

Самое лучшее — это выявлять наличие такого ПО еще до начала установки агента. Таким образом, удастся не допустить возникновения описанных выше проблем (а главное — их последствий).

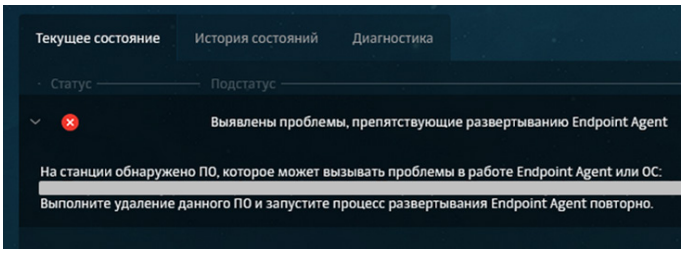


Рисунок 5. На станции выявлено конфликтное ПО

Еще один важный момент — это наличие необходимых обновлений ОС. Часто для исправной работы ПО необходимо наличие тех или иных обновлений ОС. Отсутствие таких обновлений может вызывать проблемы при работе ПО или самой ОС. Агенты DLP-систем в данном случае не исключение, поэтому также необходимо уметь выявлять отсутствие критичных обновлений.

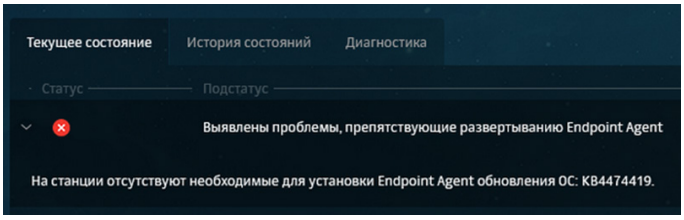


Рисунок 6. На станции отсутствуют необходимые обновления ОС

Что бывает, когда выполняется попытка установки ПО на неподдерживаемую версию ОС? Правильно — можно столкнуться с последствиями, которые потом придется устранять (возможно, долго). Поэтому инструмент диагностирования также должен выявлять и такие нюансы.

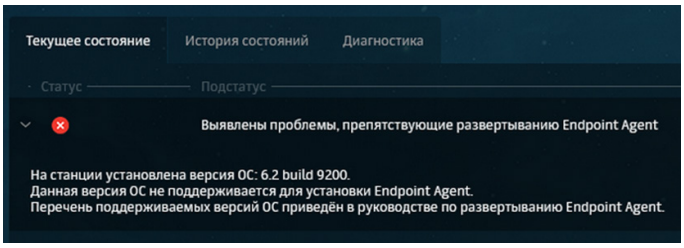


Рисунок 7. Неподдерживаемая версия ОС

Может случиться, что установка агента была выполнена корректно, а затем по тем или иным причинам что-то произошло с его компонентами. Возникает риск потери важных перехватов.

В таком случае поможет диагностирование нарушения целостности агента и своевременное информирование об этом пользователя для принятия решения о дальнейших действиях в отношении станции, а возможно, и сотрудника, который за ней работает.

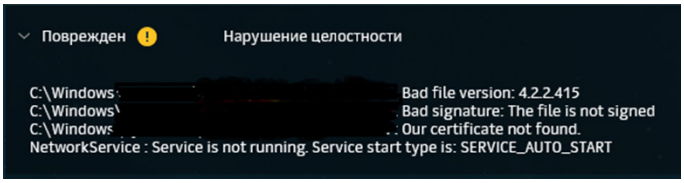


Рисунок 8. Нарушение целостности Endpoint Agent

А что, если агент молча перестал выходить на связь? Да, сотрудник мог уйти в отпуск или на больничный, поэтому его станция продолжительное время не включается, а соответственно, и агент не выходит на связь с «командованием». Но что, если за станцией работает злоумышленник, которому каким-то образом удалось выполнить удаление/поломку агента с целью ухода от контроля? Или удаление агента может быть обусловлено банальной переустановкой ОС службой технической поддержки компании? В любом случае необходимо «сигнализировать» о таких станциях своевременно.

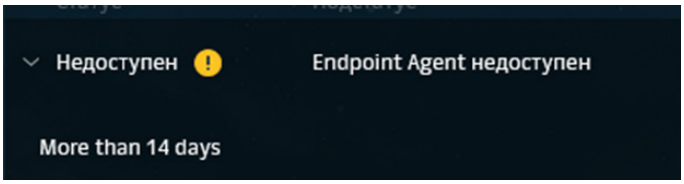


Рисунок 9. Endpoint Agent недоступен

Выводы

Присутствие агента DLP-системы на станции не должно негативно сказываться на рабочих процессах сотрудников компании. Поэтому крайне желательно уметь выявлять возможные проблемы еще до установки такого сложного ПО. По сути, необходимо действовать предиктивно, не давая тем самым возникнуть этим самым проблемам. Но одного выявления — мало. Нужно, чтобы пользователь, работающий с DLP-системой, понимал, что именно пошло не так, а вендор мог предложить ему способы решения этой проблемы. Ну или хотя бы предоставить максимум информации, благодаря которой он мог бы сам решить, какие действия необходимо предпринять. Надо понимать, что перечень возможных проблем может пополняться в зависимости от инфраструктуры площадок, следовательно, нужно постоянно развивать инструмент диагностирования проблем.

Михаил Моисеев
Ведущий аналитик
Центр технологий кибербезопасности
ГК «Солар»

Евгений Гришкин
Руководитель группы поддержки продуктов
Центр технологий кибербезопасности
ГК «Солар»

КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ ДАННЫХ НА MACOS-УСТРОЙСТВАХ?

Для контроля действий на рабочих станциях в Solar Dozor применяется отдельный модуль — Dozor Endpoint Agent (агент), с помощью которого можно своевременно отследить и при необходимости заблокировать передачу данных. Этот модуль адаптирован для работы под управлением разных операционных систем — компания-разработчик ГК«Солар» предлагает версии для Windows, Linux и macOS.

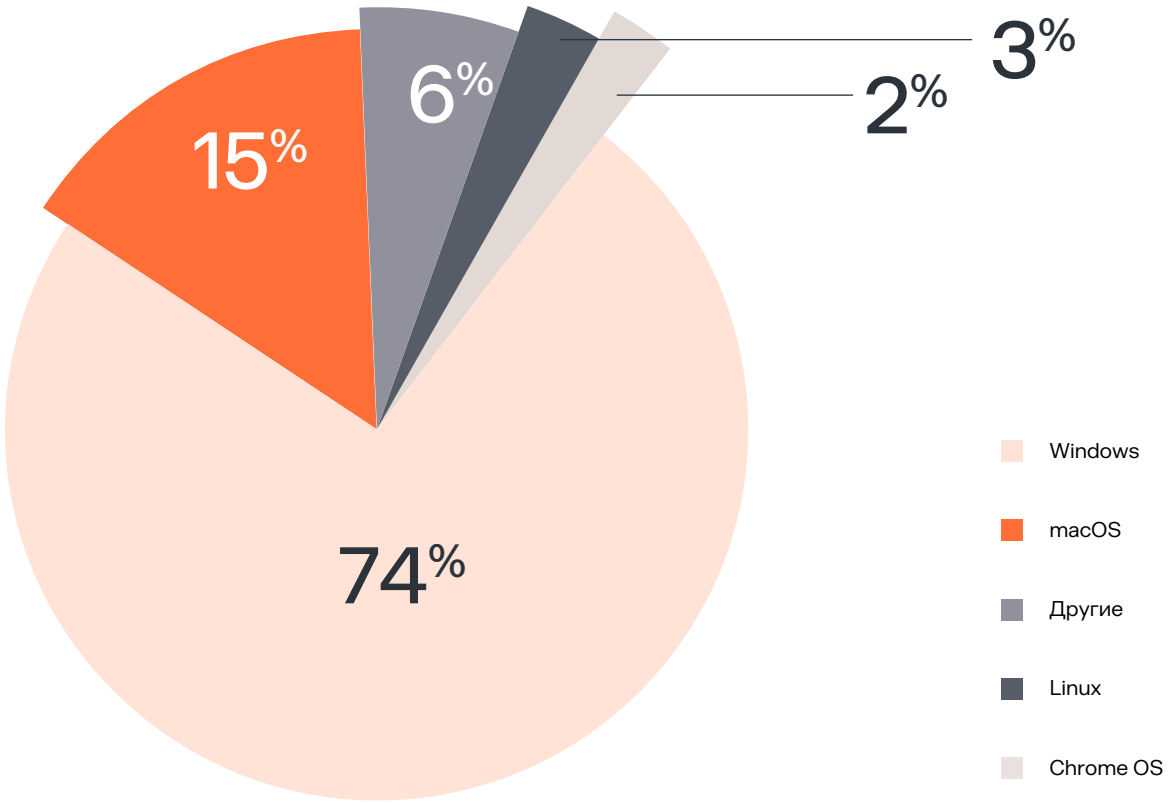
На портале Anti-Malware уже приводились обзоры модуля Dozor Endpoint Agent для Linux и Windows. В этой статье речь пойдет о модуле Dozor Endpoint Agent для macOS, который разрабатывается с 2021 г. Он стал флагманом движения российского рынка DLP-систем к полнофункциональному мониторингу рабочих мест на базе устройств Apple и по сей день занимает на нем лидирующую позицию.

Об операционной системе macOS: немного статистики

Macintosh Operating System (macOS, до 2016 г. — OS X) представляет собой семейство операционных систем, созданных специально для компьютеров Apple Macintosh. Считается, что именно в macOS впервые была применена технология GUI — графический интерфейс пользователя.

По данным платформы мировой статистики Statista.com, за 10 лет доля пользователей ОС Windows в мире сократилась на 17%. Самую большую часть рынка у Windows перетянула на себя именно операционная система от компании Apple. В начале 2023 г. macOS сумела захватить и удержать 15% мирового рынка.

Статистика использования ОС в мире, январь 2023



В России, по данным сервиса StatCounter GlobalStats, на май-июнь 2023 г. доля компьютеров, работающих под управлением Windows, тоже сократилась и составляет всего 83,55% (еще несколько лет назад система от Microsoft занимала почти 100% рынка), в то время как количество компьютеров на macOS (OS X) — уже 6,27%.

83,55 %

Windows

6,27 %

macOS (OS X)

На июнь 2023 г. семейство операционных систем macOS по распространенности в РФ занимает 3 место, оставив позади себя ОС семейства Linux. Это неудивительно, ведь macOS славится своей надежностью, стабильной работой программ, написанных специально под конкретные конфигурации ОС, а также лучшей по сравнению с другими ОС защищенностью от вирусов. На высоте и удобство использования системы (usability) — macOS отличается очень продуманным интерфейсом.

По данным ГК «Солар», в российских компаниях рабочие станции под управлением macOS использует в среднем от 5% до 50% сотрудников (в зависимости от специфики деятельности организации):

- Топ-менеджмент, чьи макбуки содержат ключевую финансово-экономическую информацию и сведения по стратегическому развитию бизнеса.
- ИТ-специалисты, владеющие конфиденциальной технической информацией, базами данных, планами стратегического развития ИТ-продуктов и услуг компании.
- Дизайнеры, маркетологи и другие специалисты, работающие с договорами, конкурсной документацией, базами данных клиентов, информацией о рыночном развитии продуктов и услуг и т. п.

Утечка подобных сведений может привести к довольно ощутимым последствиям для компаний, включая штрафы и репутационные потери.

Использование Dozor Endpoint Agent для macOS: решаемые задачи

С помощью DLP-системы Solar Dozor и ее модуля Dozor Endpoint Agent для macOS специалисты служб безопасности компаний могут, как минимум, получать и просматривать сведения о действиях сотрудников на рабочих станциях. Также можно настроить и применить правила политики безопасности так, чтобы система автоматически блокировала подозрительные операции. Таким образом, контролируются:

- обмен сообщениями и файлами в веб-почте;
- общение в социальных сетях и блогах;
- передача данных в мессенджерах Telegram (веб-версия), WhatsApp (веб-версия) и Skype;
- публикация данных в облачные хранилища:
  - Облако Mail.ru, Яндекс.Диск, OneDrive, Google Drive, Dropbox и iCloud — в веб-браузерах,
  - Яндекс.Диск и Mail.Cloud — в соответствующих десктоп-приложениях;
- подключение внешних устройств (флеш-накопителей, внешних дисков и т. п.) к рабочим станциям через USB;
- копирование информации в буфер обмена;
- операции с файлами (включая архивы): копирование/перемещение на съемные носители, сетевые диски и веб-ресурсы (в том числе с использованием технологии AirDrop);
- отправка данных на печать;
- использование поисковых запросов.

Также Dozor Endpoint Agent для macOS может предоставлять:

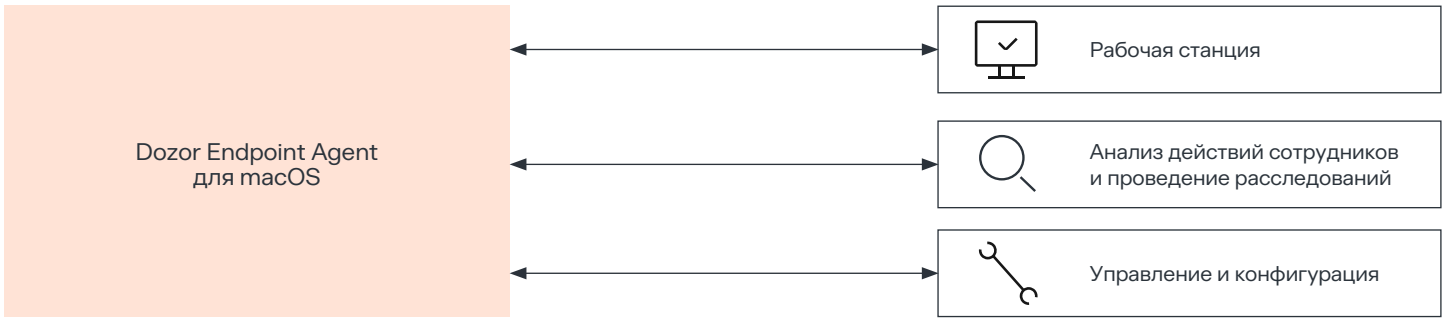
- созданные им снимки (скриншоты) экранов рабочих станций;
- информацию, которая вводится сотрудниками с клавиатуры;
- данные о проведенном сотрудниками времени в приложениях и в интернете.

Все собранные агентом сведения сохраняются в системе и отображаются по запросу пользователя как в текстовом, так и в графическом виде. Есть возможность получать отчеты за большой период, наглядно показывающие всю активность сотрудника на рабочем месте. В конечном счете это позволяет не только противодействовать утечкам информации и предотвращать их, своевременно приняв необходимые меры, но и проводить служебные расследования инцидентов ИБ, выявлять нелояльных и плохо работающих сотрудников и т. п.

ФУНКЦИЯ (КАНАЛ ПЕРЕХВАТА)	MACOS
Разрешение и блокировка подключения USB-устройств по заданным категориям и экземплярам	+
Перехват сетевого трафика по протоколу HTTP(S), включая веб-почту и облачные хранилища	+
Контроль почтовой переписки по протоколам SMTP, POP3, IMAP, в том числе с шифрованием SSL/TLS	+
Контроль и блокировка печати	+
Снятие снимков с экрана	+
Перехват нажатия клавиш (кейлогер)	+
Контроль передачи данных через буфер обмена (текст, изображения)	+
Контроль копирования файлов на USB-устройства и сетевые диски	+
Контроль рабочего времени пользователей: название сайтов и приложений, время работы с ними, аналитика по сотруднику и отделу	+
Запись звука с микрофона рабочей станции	+
Перехват сообщений и файлов в мессенджерах	WhatsApp, Telegram, Skype

Таблица 1. Функции Dozor Endpoint Agent для macOS

В таблице функций Dozor Endpoint Agent можно увидеть заметный прогресс по сравнению с первым релизом macOS-агента в сентябре 2021 г. (в тот релиз вошли: контроль интернет-трафика, перехват локальной почты и контроль передачи данных в WhatsApp и Skype), что говорит о высоком темпе развития модуля.



Рабочая станция

- Контроль действий пользователей
- Мониторинг каналов передачи данных
- Блокирование утечки данных (USB, HTTPS, снимки экрана, почта, кейлогер, облачные хранилища, отправка в печать, мессенджеры)

Управление и конфигурация

- Единый центр управления агентами
- Гибкая настройка каналов перехвата и политик безопасности
- Скрытое развертывание посредством MDM/EMM-систем

Анализ действий сотрудников и проведение расследований

- Подключаемые устройства
- Почтовая переписка и переписка в мессенджерах
- Выгрузка файлов на веб-ресурсы, включая облачные хранилища
- Отправка информации на печать
- Снимки экрана, журнал клавиатурного ввода
- Активность в социальных сетях, блогах, на форумах

Новейшая версия Dozor Endpoint Agent для macOS:

- функционирует на рабочих станциях под управлением macOS самых современных версий — 11.x (Big Sur),12.x (Monterey), 13.x (Ventura);
- поддерживает работу на устройствах как с архитектурой x86-64, так и с Apple M1/M2;
- совместима с антивирусом Kaspersky Endpoint Security для macOS.

Агент можно легко установить локально на конкретную рабочую станцию с помощью графического инсталлятора или развернуть одновременно на группу макбуков, используя специальные средства — MDM/EMM-системы (например, VMware AirWatch или Microsoft Intune). Управлять рабочими станциями с установленными агентами можно в веб-интерфейсе Solar Dozor.

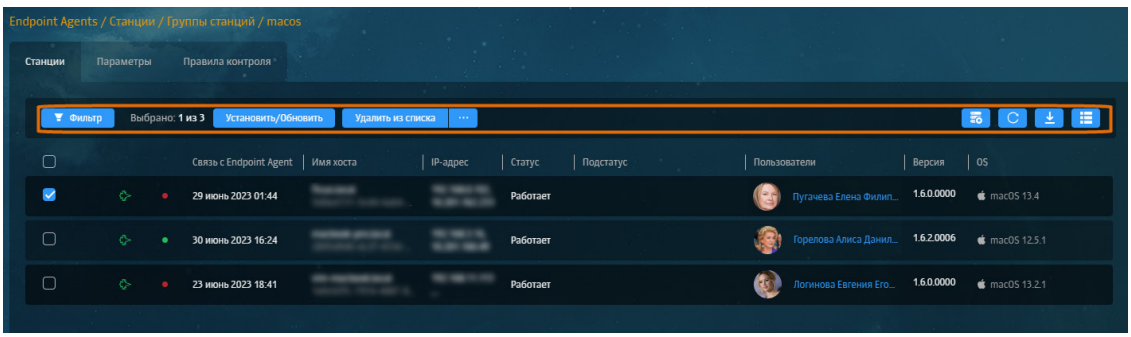


Рисунок 1. Интерфейс Solar Dozor, список функционирующих на macOS рабочих станций с установленным агентом: элементы управления

Dozor Endpoint Agent для macOS: ключевые функции

Спрогнозировать, какие функции агента будут наиболее востребованы, можно, отслеживая и понимая тенденции, касающиеся каналов утечек данных. По данным исследования, которое было проведено аналитиками ГК «Солар», за последний год наиболее распространенными каналами утечки, например, в финансовых организациях стали облачные хранилища, флеш-накопители и веб-версии мессенджеров. Это явное отражение общероссийской политики ужесточения правил использования средств онлайн-коммуникации на рабочих местах сотрудников. Соответственно, контроль передачи данных в облачные хранилища и в мессенджерах (особенно в их веб-версиях) и контроль копирования файлов на USB-носители являются приоритетными направлениями защиты от утечек.

Еще одно важное для macOS-агента направление — обеспечение контроля AirDrop-передачи файлов. AirDrop-технология была разработана компанией Apple специально для обмена документами, изображениями и иными данными между устройствами Apple, находящимися поблизости (используются Wi-Fi или Bluetooth-подключения).

Кроме того, стоит сказать о контроле печати — модуль Dozor Endpoint Agent для macOS умеет не только перехватывать, но и блокировать печать документов.

Контроль передачи информации в мессенджерах: получение данных переписки в веб-версиях Telegram и WhatsApp, а также Skype.

Как сообщает информагентство ТАСС, по данным «Лаборатории Касперского» в 2023 году по сравнению с предыдущим годом злоумышленники сместили фокус внимания, сосредоточившись на крупном бизнесе. Об этом говорят цифры за аналогичные периоды 2022 и 2023 гг.:

- для крупного бизнеса: в 2022 г. попавших в Сеть сведений было 28 млн строк, в текущем — уже 163 млн;
- для малого и среднего бизнеса: 70 млн строк в 2022 г. против 20 млн в 2023.

Отмечается, что половина всех утечек была опубликована в течение месяца после выгрузки данных, при этом чаще всего данные попадали в Сеть через мессенджер Telegram.

С помощью Dozor Endpoint Agent для macOS на рабочих станциях под управлением macOS контролировать передачу данных в веб-версии мессенджеров Telegram и WhatsApp можно уже сейчас — обеспечен перехват отправленных и/или полученных сообщений и файлов. Кроме того, агент перехватывает входящую и исходящую переписку в мессенджере Skype, причем как в приложении, установленном на рабочей станции, так и в веб-версии.

Все перехваченные данные можно просмотреть в веб-интерфейсе Solar Dozor в карточке сформированного агентом сообщения о переписке в конкретном мессенджере.

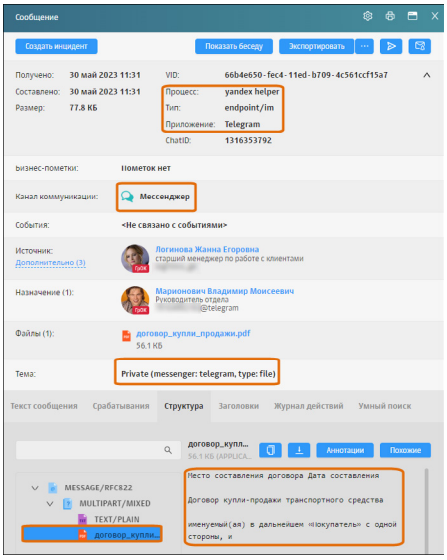


Рисунок 2. Интерфейс Solar Dozor, карточка сообщения: сведения о файле, отправленном в Telegram Web

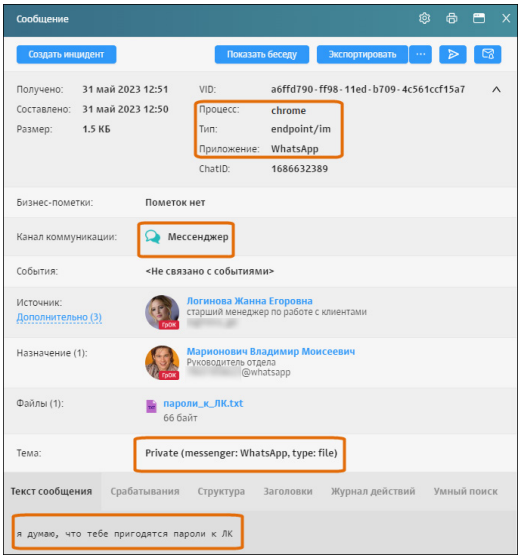


Рисунок 3. Интерфейс Solar Dozor, карточка сообщения: сведения о данных, отправленных в WhatsApp Web

Отслеживание публикации данных в облачные хранилища

С помощью новейшей версии модуля Dozor Endpoint Agent для macOS, установленного на рабочих станциях под управлением macOS, возможно полностью контролировать передачу файлов в облачные хранилища Яндекс.Диск и Облако Mail.ru, выполненную через соответствующее приложение. Можно, например, настроить правила политики безопасности так, чтобы при отправке сотрудником файла, содержащего критичные для компании данные, система блокировала операцию отправки, создавала событие или инцидент с высоким уровнем критичности и оповещала специалистов службы безопасности.

Также можно указать, уведомлять ли сотрудника о нарушении им правил политики, и задавать текст этого уведомления. Сведения об успешных и неуспешных попытках пользователей рабочих станций отправить данные на Яндекс.Диск или в Облако Mail.ru фиксируются в Solar Dozor и их можно посмотреть в веб-интерфейсе системы. В частности, можно получить информацию об успешности/неуспешности попытки такой передачи: запрещено/разрешено.

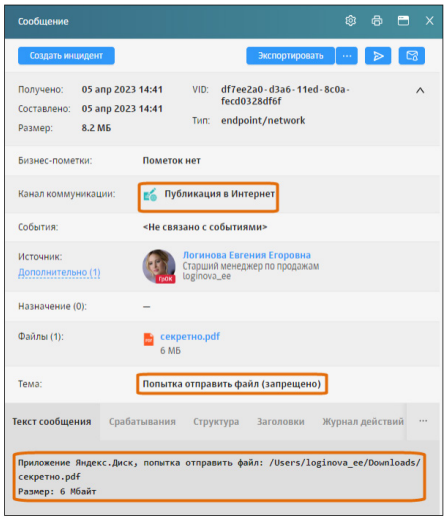


Рисунок 4. Интерфейс Solar Dozor, карточка сообщения: сведения о заблокированной попытке публикации файла на Яндекс.Диске

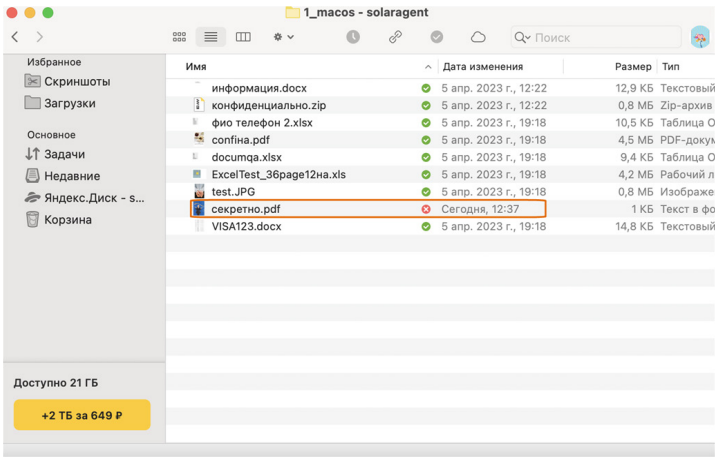


Рисунок 5. Экран рабочей станции: результат блокировки отправки файла на Яндекс.Диск — файл не был отправлен

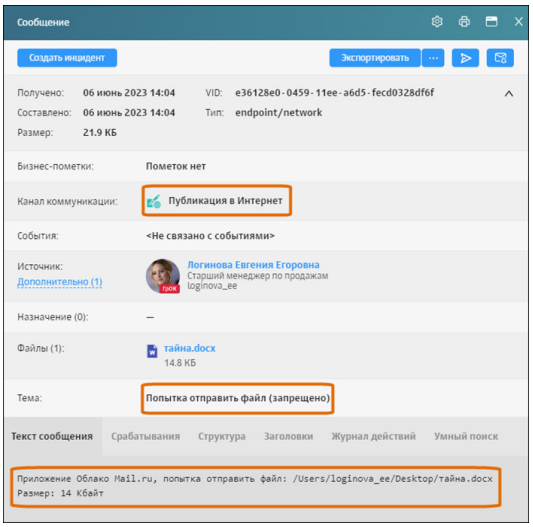


Рисунок 6. Интерфейс Solar Dozor, карточка сообщения: сведения о заблокированной попытке отправки файла в Облако Mail.ru

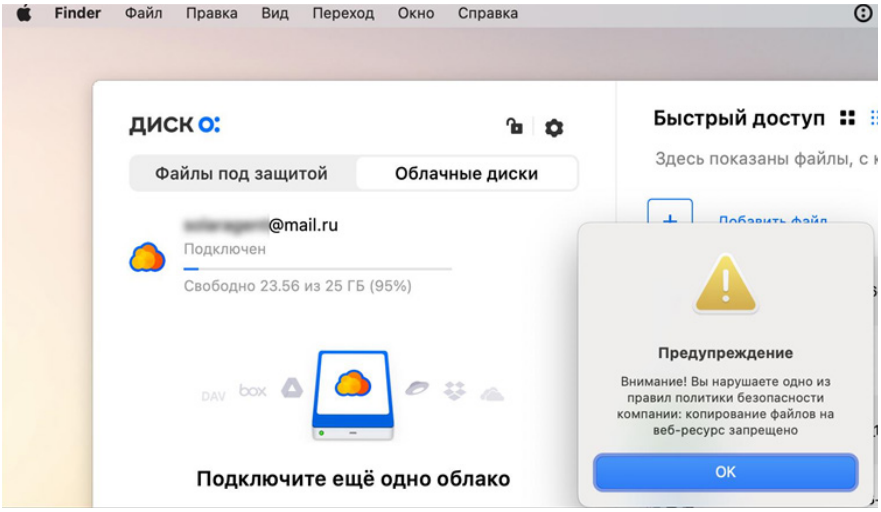


Рисунок 7. Экран рабочей станции: результат блокировки отправки файла в Облако Mail.ru — файл не был отправлен, пользователь рабочей станции получил уведомление о нарушении правил политики безопасности

Кроме того, с помощью Dozor Endpoint Agent для macOS можно отслеживать факты веб-браузерной передачи в облачные хранилища Облако Mail.ru, Яндекс.Диск, OneDrive, Google Drive, Dropbox и iCloud.

Если, к примеру, настроить систему так, что она при регистрации факта такой передачи будет моментально оповещать специалистов службы безопасности, это позволит своевременно отреагировать, принять соответствующие меры и тем самым предотвратить дальнейшую утечку информации.

Контроль копирования/перемещения файлов на съемные носители и сетевые ресурсы: перехват и блокировка операций

С помощью Dozor Endpoint Agent для macOS и настроенных в Solar Dozor правил политики безопасности можно автоматически отслеживать и при необходимости блокировать выполняемые сотрудниками операции копирования или перемещения файлов на съемные носители и/или сетевые ресурсы.

При этом на соответствие политике безопасности проверяется содержимое как самих файлов, так и архивов (проверяются docx/pdf/pdf/txt-файлы и содержимое zip/7z/arj/rar/tar-архивов).

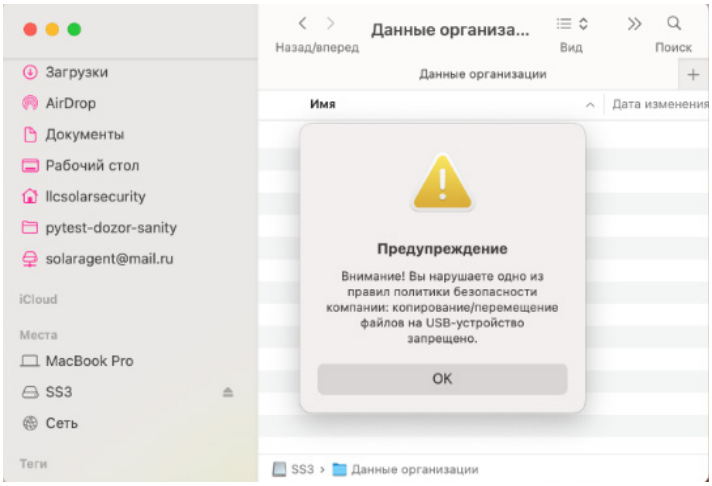


Рисунок 8. Экран рабочей станции сотрудника компании при заблокированной попытке копирования файла на USB

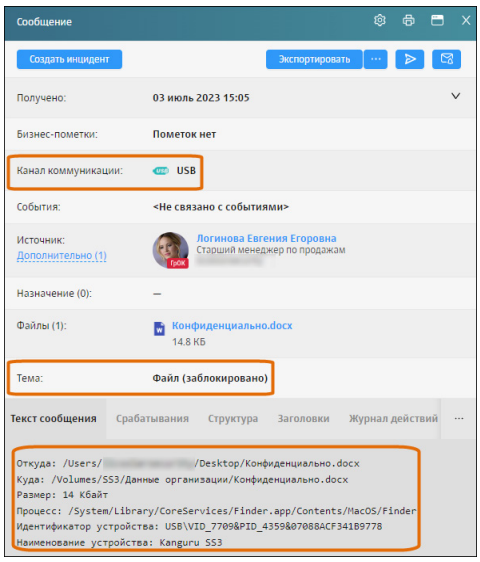


Рисунок 9. Интерфейс Solar Dozor: сведения о заблокированной попытке копирования файла на USB

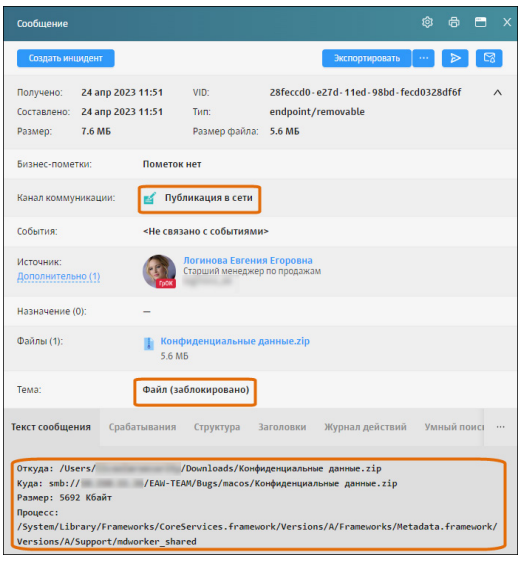


Рисунок 10. Интерфейс Solar Dozor: сведения о заблокированной попытке копирования архива на сетевой ресурс

Контроль канала AirDrop: перехват файлов и блокировка их передачи

С помощью Dozor Endpoint Agent для macOS и настроенных в Solar Dozor правил политики безопасности можно автоматически отслеживать и при необходимости блокировать AirDrop-передачу данных, выполняемую из файлового менеджера Finder, рабочего стола операционной системы или напрямую из приложений.

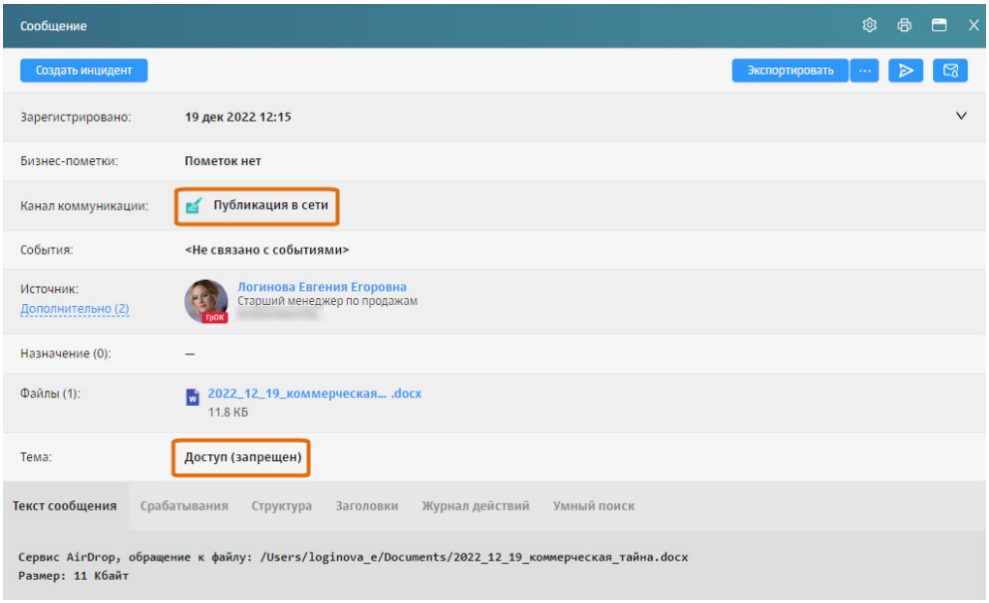


Рисунок 11. Интерфейс Solar Dozor, карточка сообщения: сведения о заблокированной попытке AirDrop-передачи файла

Контроль данных, отправляемых на печать: перехват и блокировка по контенту

Функция контроля печати, реализованная в Dozor Endpoint Agent для macOS, позволяет:

- перехватить данные, отправляемые сотрудниками на локальные, сетевые или виртуальные принтеры для последующей печати (независимо от приложения, из которого пользователь запускает печать);
- зафиксировать в системе факт печати документа любого типа;
- проверить содержимое документа, отправленного на печать, на соответствие правилам политики безопасности (в случае многостраничного документа будет проверен текст только печатаемых страниц);
- заблокировать операцию печати, если по результатам проверки документа в нем была найдена критичная информация.

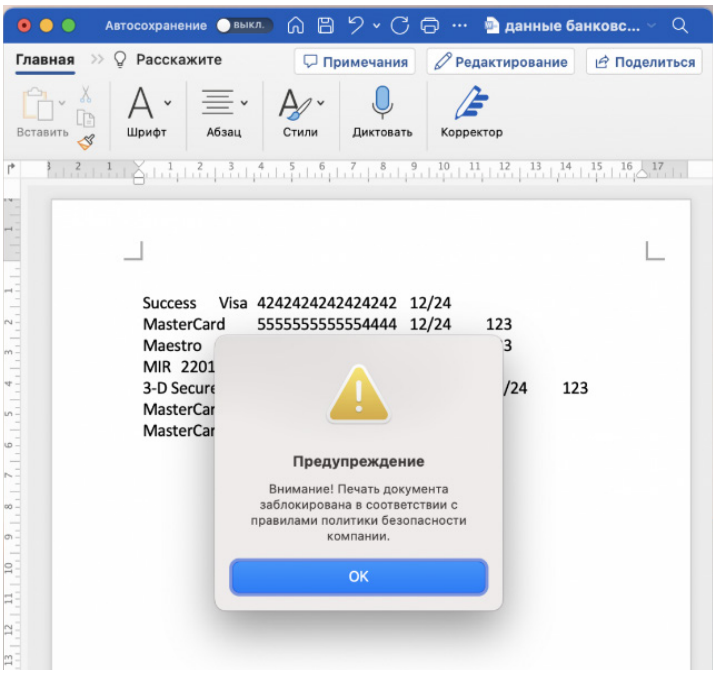


Рисунок 12. Экран рабочей станции сотрудника компании при заблокированной попытке печати файла с конфиденциальными данными

Выводы

Несмотря на тенденцию импортозамещения в сфере программного обеспечения и оборудования, компьютеры, работающие на macOS, продолжают активно использоваться в российском корпоративном сегменте. Как уже было сказано выше, ключевыми пользователями macOS-устройств являются топ-менеджмент компаний, а также представители творческих профессий — дизайнеры, разработчики, маркетологи.

Среди пользователей Dozor Endpoint Agent для macOS — крупнейшие компании финансового и строительного секторов, ИТ-индустрии, сферы розничной и оптовой торговли, а также рекламы (медиаиндустрия).

Они ценят возможности ненавязчивого мониторинга, когда дело касается привилегированных пользователей, и преимущества активного противодействия угрозам, когда речь заходит о попытках вывода защищаемой информации за периметр корпоративной сети.

Одним из важнейших векторов дальнейшего развития модуля Dozor Endpoint Agent для macOS является стремление к паритетности его функций с модулем Dozor Endpoint Agent для Windows, исторически наиболее функционально развитым агентским модулем DLP-системы Solar Dozor.

Яна Менжевицкая
Аналитик группы бизнес-аналитики
Центр технологий кибербезопасности
ГК «Солар»

ИНТЕГРАЦИЯ DLP-СИСТЕМ С ВНЕШНИМИ ИСТОЧНИКАМИ: «ТАНЦЫ С БУБНОМ» ИЛИ «КАК ПО МАСЛУ»?

Проблематика

О том, что информация стоит денег, люди знают давно. А вот понимание того, что потеря информации тоже имеет свою цену, стало приходить только в последние несколько лет. И с приходом этого понимания вопросы обеспечения ИБ начали наконец выходить на первый план, и компании все чаще стали вкладываться в средства защиты информации от несанкционированного доступа (СЗИ от НСД). В том числе — и в DLP-системы.

Раньше DLP-системы были простые. Потому что требования к ним предъявлялись тоже простые: перехват корпоративной почты, печати. Может, запись на внешние носители. Остальная корпоративная среда в зону охвата DLP не попадала. Да и не то чтобы была она слишком развита: хранилища — папки с общим доступом на локальном сервере, мессенджер — ICQ, а под облаками понимались исключительно атмосферные образования в небе.

С развитием корпоративной ИТ-инфраструктуры, соответственно, стали расти и запросы к DLP-системам: заказчикам уже мало было контролировать только почту и печать. Потребовался контроль мессенджеров, комнат данных, различных ИС, например, SharePoint или Confluence, систем электронного документооборота и пр.

Теперь перед DLP-системами ставится задача «перехватывать все» — данные со всех корпоративных ИС, находящиеся как в покое, так и в движении. Данная интеграция просто необходима для обеспечения надлежащего уровня ИБ, особенно в наши непростые времена.

К сожалению, в настоящий момент это трудновыполнимая задача — в техническом плане такое просто не всегда возможно: где-то можно перехватить трафик, например, с использованием реверсивного прокси-сервера, где-то нет. У одной программы есть прямой внешний коннектор, а у другой он отсутствует. Но даже если удастся направить трафик с ИС в DLP, все равно требуется проведение НИРов, чтобы информация в DLP-системе отображалась корректно. Но на все это необходимы дополнительные инвестиции и время. В итоге что-то получается интегрировать, что-то — нет. А может сложиться ситуация, когда интеграция вроде бы реализована, но не полностью: например, перехваты идут, но не в полном объеме или без блокировок. Получается, что результат попытки интеграции не гарантирован.

Технические аспекты интеграции

В целом при интеграции ИС с DLP всегда встают две проблемы: первая связана с получением и обработкой трафика, приходящего от ИС в DLP-систему, а вторая — с передачей ответов DLP-системы в ИС.

Разберем их подробнее.

1. Получение информации DLP-системой от ИС.

Проблема получения DLP-системой данных от ИС состоит в следующем:

a. Отсутствие единого формата.

Разные ИС передают информацию во внешние системы в разных форматах представления: например, в формате json, или xml, а то и просто как текст. Метаданные могут передаваться как в заголовках, так и в теле сообщения.

b. Состав сообщения.

Тут основная проблема: недостаток передаваемых атрибутов, например отсутствие адресной информации (для мессенджеров — это данные об отправителе и получателе). Для антивирусов может быть этого и достаточно, но не для DLP-системы, которая должна осуществлять привязку зарегистрированной информации к ее владельцам.

c. Контекст.

Один объект, например сообщение, может из ИС передаваться в DLP раздельными фрагментами, например — отдельно текст, отдельно файл. Как следствие, теряется целостность объекта, для представления его в DLP требуется создавать механизм его предварительной сборки вручную.

2. Обработка ИС ответов от DLP для активного противодействия (блокировки передачи запрещенного контента).

DLP-система по своему назначению в первую очередь должна обеспечивать предотвращение утечки информации, а значит, обрабатывать данные, поступившие от ИС, в активном режиме, например, при выявлении нарушения правил хранения информации осуществлять блокировку доступа к данным. Протоколы HTTP и ICAP, которые для этого обычно используются, в принципе позволяют настроить интерактивное взаимодействие ИС с DLP. Но далеко не во всех ИС предусмотрен механизм приема и обработки ответов от DLP. Например, многие мессенджеры не понимают информацию, полученную по протоколу ICAP от DLP-системы, и просто не знают, что надо делать.

При обработке ответного трафика от DLP к ИС следует обратить внимание еще и на время ожидания отклика: этот параметр должен быть управляемым, в зависимости от сложности применяемых в DLP политик.

Резюмируя, можно сказать, что многие ИС, если и имеют возможность передавать в DLP свой трафик, то в виде, далеком от желаемого (так как специфика взаимодействия ИС с DLP не учитывалась). А с обработкой ответов от DLP у ИС дела обстоят еще хуже. В итоге получается, что каждая интеграция превращается для компании в отдельный трудозатратный проект, требующий участия обеих сторон (разработчиков ИС и DLP), и при этом с негарантированным результатом.

Мы подходим к пониманию того, что для обеспечения нормальной интеграции ИС с DLP — для 100-процентной передачи информации в DLP в соответствии с требованиями DLP, а также обеспечения работы связки ИС-DLP-ИС в активном режиме, — необходимо провести унификацию протоколов взаимодействия (форматов запроса и форматов ответа) в единый стандарт.

Свет надежды

Сейчас у нас уникальное время. Многие иностранные ИС заменяются отечественными аналогами. Задачи перед нашими производителями стоят колоссальные: в короткий срок заместить огромный срез зарубежных ИС, при этом сделать хорошо, и даже лучше, чем было (в итоге многие отечественные ИС, в т.ч. вновь созданные, действительно оказались не хуже, и даже лучше западных систем). Но бросив все ресурсы на функциональность, разработчики порой забывают про возможности интеграции своих продуктов со смежными системами.

И это понятно: программисты на вес золота, да тут еще и цейтнот. А заказчик, у которого главная задача — срочно импортозаместить, к примеру, SharePoint (лицензия на который уже просрочена) и надо как можно быстрее выбрать и заново внедрить отечественный аналог, тоже вспоминает про интеграцию с СЗИ уже после сдачи ИС в эксплуатацию. И начинаются те самые танцы с бубном: трудозатраты, время — дополнительный расход ресурсов, о котором писалось выше.

Что же делать?

На первый взгляд, кажется, все просто: при разработке ИС, еще на этапе ее проектирования, предусматривать создание универсального коннектора с внешним ПО в таком объеме, чтобы он подходил и для СЗИ (в т.ч. DLP-систем). Но, повторюсь, отечественным производителям ПО в условиях жесткого дефицита ресурсов просто некогда этим заниматься.

Заказчики требуют просто работающий продукт (у них тоже голова другим занята, помните?), и на продажи отсутствие коннектора не влияет. А проблемы интеграции можно решить и потом, по мере поступления. Да и вообще, пусть производители DLP разбираются. Это уже их боль.

Действительно, главный вопрос: зачем это разработчикам ИС. Ведь проблема интеграции стоит перед DLP. Я бы ответил так: проблема это не у DLP, а у бизнеса. А мы все зависим от бизнеса. И устойчивое экономическое состояние бизнеса во многом зависит от состояния ИБ: собственно говоря — способности корпоративных СЗИ своевременно выявлять проблемы безопасности и оперативно их решать.

Именно поэтому в наших общих интересах обеспечить бесшовную интеграцию ИС (как бизнесовых, так и ИБ-шных) в корпоративную ИТ-инфраструктуру. В данном случае это обеспечение взаимодействия между собой ИС с СЗИ. Это как повысит привлекательность таких продуктов на рынке, так и обеспечит общий высокий уровень ИБ в отечественном ИТ-сегменте.

Выводы

Для того чтобы обеспечить интеграцию ИС с DLP, конечно, потребуется не просто предусматривать в ИС какой-то механизм взаимодействия. Этого мало. Он должен быть унифицированным, и унификация эта должна быть описана в нормативной документации как стандарт. Например, на уровне ГОСТа, в котором будет закреплена необходимость наличия универсальных коннекторов для СЗИ в ИС. Внедрение такого ГОСТа приведет к тому, что крупный отечественный бизнес сможет рассматривать на конкурсах только такие перспективные ИС, в которых будет реализован коннектор с СЗИ. А за крупными компаниями подтянутся и остальные. В итоге у нас будет решена еще одна немаловажная проблема ИБ.

Дмитрий Мешавкин
Руководитель группы продуктовой аналитики
Центр технологий кибербезопасности
ГК «Солар»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — ЭТО ВСЕГДА СТРЕМЛЕНИЕ БЫТЬ НА ШАГ ВПЕРЕДИ ЗЛОУМЫШЛЕННИКОВ

Современные цифровые предприятия активно внедряют в свою работу платформы и решения, управляющие всем спектром корпоративных коммуникаций. О том, как защитить компанию от утечек конфиденциальной информации по каналам коммуникаций, в интервью TAdviser рассказал Руслан Добрынин, эксперт Центра технологий кибербезопасности компании ГК «Солар».

Руслан, насколько активно, по вашим оценкам, российские компании используют мессенджеры, как публичные, так и корпоративные, для рабочих взаимодействий?

Вопрос о мессенджерах сегодня весьма актуален — это очень важный канал коммуникаций, который не уступает корпоративной почте, а может быть, даже превосходит ее по интенсивности общения. Зачастую сотрудники пользуются не только корпоративными мессенджерами, но и публичными, в частности, для связи с коллегами и партнерами из внешнего контура. Очевидно, что риски утечек конфиденциальных сведений существуют во всех этих случаях и коммуникации нужно контролировать. Причем если внешние атаки и угрозы очевидны всем, то внутренние утечки — это гораздо более скрытая угроза. Руководство может не подозревать о глубинных процессах внутри организации, а затем как гром среди ясного неба происходит утечка — она может быть как ненамеренной, так и вызванной желанием подзаработать, но в обоих случаях одинаково болезненной. Поэтому внутренний периметр компании нужно защищать не менее тщательно, чем внешний. Сегодня, когда, по сути, идет полноценная кибервойна, DLP-система — базовая необходимость для бизнеса, как и средства коммуникаций, инструменты защиты периметра и прочие сервисы, без которых немыслимо бесперебойное существование современной компании.

Обычно считается, что главная опасность, исходящая от мессенджеров, связана с использованием одного мобильного устройства как для рабочей, так и личной переписки. Это так?

Такой риск, конечно, есть. Но сегодня развитые корпоративные мессенджеры, как, например, eXpress, хорошо приспособлены к этой ситуации: контакты делятся на внутренний и внешний контур, поэтому в целом их контролировать проще, чем публичные мессенджеры. К тому же, как правило, вендоры, которые производят мессенджер и DLP-систему, находятся в тесном контакте друг с другом и синхронизируют модернизацию ПО, например развитие протокола передачи данных и т. д. Мы сотрудничаем с eXpress именно так.

Для конфиденциальных сведений важно не столько выявить факт утечки и установить виновных, сколько не допустить самой утечки. Это возможно?

Есть различные сценарии защиты данных от утечек. Например, можно осуществлять пассивный мониторинг и контроль, а можно обеспечивать блокирование утечки. Уместность этих подходов определяется ИБ-службой компании: в некоторых случаях необходимо заблокировать передачу чувствительной информации, в других ситуациях есть смысл разрешить отправку нелегитимного сообщения и понаблюдать за дальнейшей судьбой такой переписки. Это может быть полезным для сбора доказательной базы или, например, для раскрытия деталей схемы, реализуемой злоумышленниками. Отследить факт попытки передачи сообщения с конфиденциальной информацией можно, например, по атрибутам: в ходе коммуникаций появляются некоторые речевые обороты, которые описаны в DLP-системе как подозрительные, и это знак того, что происходит некоторое событие в области ИБ (передача письма или сообщения), которое можно либо немедленно заблокировать, либо просто обратить на него внимание офицера безопасности. На техническом уровне необходимо контролировать все возможные каналы коммуникаций, используемые в компании. При этом на организационном уровне обязательны корпоративные политики безопасности. Именно они дают ответы на вопросы: какие именно каналы связи разрешены в компании, каков регламент реагирования на подозрительную активность или очевидную утечку.

Современные мессенджеры поддерживают широкий спектр пользовательских устройств, как стационарных, так и мобильных, на базе различных ОС. Одна DLP-система способна контролировать утечки на всем многообразии конечных устройств сотрудников?

В целом достичь этого возможно. Другое дело, что в нашей системе ценностей, связанной с DLP-системой Solar Dozor, контролировать личные устройства пользователей считается неэтичным и неправильным. Мы всегда рекомендуем организации выстраивать понятные и логичные политики безопасности, которые определяют, каким образом ограничивается использование личных средств связи в рабочих целях. В зрелых организациях всегда в актуальном состоянии поддерживается перечень документов, содержащих КТ (коммерческую тайну) и с грифом ДСП (для служебного пользования), списки доступа и маршруты (это фактически является политикой DLP). Если сотруднику разрешено использование личного устройства, то это всегда регламентировано.

Зачастую внедренные средства ИБ снижают производительность защищаемой ИТ-инфраструктуры, что для системы коммуникаций может оказаться критичным. Каким образом удается добиться несниженной производительности системы коммуникаций, где передается трафик, чувствительный к задержкам?

Здесь тоже есть свои нюансы. Работа DLP-системы никак не сказывается на производительности компьютеров пользователей, с вероятностью 99% пользователь не заметит ее наличия. Но если контроль почты или мессенджеров установлен «в разрыв» (контролирующая система находится между отправителем и получателем, а значит, способна заблокировать сообщение в процессе передачи) — это может увеличить время доставки письма. Если принято решение об установке перехватчика в разрыв, то это значит, что заказчик осознает важность предотвращения утечки, и важность эта существенно превосходит возможную секундную задержку.

Компания ГК «Солар» поддерживает в своей DLP-системе Solar Dozor разные корпоративные мессенджеры. По какому принципу отбираются коммуникационные системы?

Мы стремимся контролировать все инструменты коммуникаций, которые есть на рынке, но их очень много. Поэтому мы концентрируем внимание в первую очередь на тех мессенджерах, которые пользуются популярностью в корпоративном секторе. К их числу относятся как публичные мессенджеры (WhatsApp, Telegram, Skype и другие), так и корпоративные, прежде всего те, которые активно внедряются в российских компаниях. Конечно, eXpress — в числе наших приоритетов по причине взрывного роста его востребованности. Мы настоятельно рекомендуем нашим заказчикам использовать в служебных целях только корпоративные мессенджеры — они надежнее публичных с точки зрения сохранения конфиденциальности (вся переписка хранится на серверах компании), они значительно проще в настройке и гарантированно поддерживаются внедренной в компании системой DLP.

У платформы eXpress есть уникальные свойства — например, так называемые круги доверия, которые позволяют надежно разграничивать на одном устройстве коммуникации с различными группами лиц. Сложно ли учесть эти особенности при интеграции DLP-системы с мессенджером?

Наша DLP-система изначально создана с учетом уровней доверия. Более того, благодаря наличию кругов доверия и в eXpress, и в Solar Dozor, применительно к этому мессенджеру достаточно легко реализуется наша технология, не имеющая аналогов на российском рынке защиты от утечек, — анализ поведения пользователей (User Behavior Analytics, UBA). Например, сотрудник по роду своей рабочей деятельности чаще всего взаимодействует с коллегами внутри своей компании, но в один из дней вдруг непрерывно общается с внешними адресатами — это очевидная поведенческая аномалия, на которую службе ИБ стоит безотлагательно обратить внимание. Поведенческая аномалия — это не плохо и не хорошо, причины ее возникновения могут быть абсолютно разными. Но это безусловный повод для офицеров безопасности рассмотреть такой эпизод подробнее. В целом же полноценная совместная работа двух продуктов — Solar Dozor и eXpress — подтверждается двусторонним сертификатом совместимости. Кроме того, оба решения входят в Единый реестр отечественного ПО и сертифицированы ФСТЭК России. Все вместе это говорит о том, что Solar Dozor и eXpress не просто достигли интеграции, а совместно образуют защищенную инфраструктуру корпоративных коммуникаций.

Что еще умеет контролировать DLP-система в корпоративных коммуникациях, помимо переписки и поведения сотрудников?

Мы стремимся к возможности всестороннего контроля движения информации внутри компании — ее использования, перемещения, доступа к ней и так далее. Solar Dozor выявляет нарушителей корпоративных политик хранения конфиденциальных данных, полностью контролирует процесс печати, так как в слабозащищенных организациях часты случаи утечки информации путем ее банального распечатывания на принтере. Система может разрешать или блокировать подключение USB-устройств к корпоративным ПК или ноутбукам и, например, контролировать запись файлов на флешки, отслеживает использование облачных сервисов — всего не перечислишь. Solar Dozor — всеобъемлющее и зрелое средство защиты от утечек изнутри.

Иногда DLP-систему называют системой слежки за сотрудниками...

Хотел бы особо подчеркнуть: Solar Dozor — это не система слежки за сотрудниками. Это не карательный инструмент, а решение, препятствующее совершению противоправных действий, которые могут навредить организации. Наша система в том числе является страховкой сотрудников от непреднамеренных нарушений. Разница очевидна. Мы не стремимся никого ущемлять или наказывать, наша цель — обеспечить безопасность. DLP-система — это одна из многих возможных мер по информационной защите. И чем больше таких мер будет принято, тем спокойнее будет себя чувствовать владелец бизнеса, да и сам сотрудник, застрахованный от ошибки. При этом в основе нашей DLP-системы лежит концепция People-Centric Securty. Это означает, что в фокусе нашего внимания не технические средства, а человек и его действия. Solar Dozor умеет создавать профили сотрудников, анализировать их поведение, строить графы связей — это помогает подходить к защите от утечек комплексно и, конечно, облегчает процесс расследования инцидентов ИБ, если они происходят. Концепция People-Centric Security позволяет также расширить использование DLP-системы для расследования инцидентов или событий, произошедших в прошлом. Например, в ситуациях, когда информация ранее не являлась коммерческой тайной, а потом оказалась под таким грифом и требуется узнать, кто и куда ее пересылал до перехода в разряд КТ. Несмотря на все преимущества, которые DLP дает в части расследования инцидентов, всегда необходимо помнить, что информационная безопасность — это не борьба с последствиями, а всегда комплексная работа на упреждение, способность быть на шаг впереди злоумышленников, независимо от того, где они находятся: снаружи или внутри компании. Для защиты чувствительной для организации информации следует принимать все возможные меры, использовать все доступные ИБ-средства, включая технологии NGFW (Next Generation Firewall), XDR (Extended Detection and Response), DLP, IdM, PAM и остальные необходимые системы. И, конечно, очень важно найти баланс между безопасностью и бизнес-ценностью, поскольку победа безопасности над здравым смыслом ничем не лучше пренебрежения мерами защиты.

Означает ли это, что компании нужно искать такую DLP-систему, где реализован максимальный набор функций анализа поведения сотрудника, вплоть до, например, автоматического выявления факта появления в руках у сотрудника телефона — вдруг он пытается сфотографировать экран с секретной информацией?

Действительно, сегодня в системах DLP появляется такой функционал. Реализован он довольно просто: видеокамера следит за человеком, и если он достает телефон и наводит его на экран, то камера реагирует на это действие. Однако здесь не все так радужно. Постоянное слежение за происходящим возле ПК ощутимо нагружает систему. И при этом эффективность технологии анти-фото вызывает вопросы. Если телефон находится под небольшим углом по отношению к камере, система уже не распознает, что в кадре появился именно телефон, и никак на него не реагирует. Не стоит забывать, что в ряде случаев веб-камера вообще отсутствует на АРМ сотрудника, а когда она все же есть, ее всегда можно прикрыть, заклеить и тому подобное. Поэтому в случаях, когда сотрудник имеет возможность фотографировать сведения, составляющие коммерческую тайну, целесообразным решением будет ограничение для этого сотрудника использования личного телефона на работе. Делать ставку только на технические средства, пусть и очень умные, неразумно, ведь любую техническую защиту можно обойти.

И нельзя быть уверенным в том, что тебя не взломают только потому, что в компании внедрены современные ИБ-решения. Панацеи не существует и здесь, безопасность — это процесс, и главный секрет его успеха — комплексный подход.

Иными словами, не обязательно вносить в поведенческий анализ факт съемки экрана камерой телефона? Организационные меры здесь работают лучше?

Организационные меры должны дополнять специализированные технические меры защиты. Вместе они составляют комплекс, единую сложную систему, которая не ограничивается тем или иным прикладным решением. По большому счету безопасность — это некая философия компании. Поэтому в одних компаниях сотрудникам разрешается все, а руководители надеются, что проблемы с защитой данных их просто не коснутся. Другие, наоборот, запрещают все, и сотрудники ощущают себя как в тюрьме. Любые крайности опасны, поэтому в идеале необходим баланс между ограничениями и свободой. И в этот баланс должны быть органично вплетены все необходимые технические средства, существующие на рынке, а также организационные моменты, определяющие то, как устроены бизнес-процессы.

Руслан Добрынин
Менеджер по развитию бизнеса Solar Dozor
Центр технологий кибербезопасности
ГК «Солар»

SOLAR

W: RT-SOLAR.RU
W: RT.RU

T +7 (499) 755-07-70
E solar@rt-solar.ru

Центральный офис, 125009, Москва
Никитский переулок, 7с1