

Под надзором DLP

13 экспертных статей о предотвращении утечек информации,
анализе поведения пользователей и проведении расследований

Solar Dozor. Сборник публикаций 2022 года



Содержание

Экосистема корпоративной безопасности. На Форуме DLP+ представили портрет нарушителя ИБ.....	2
Практические советы по применению DLP-систем.....	8
Как защититься от утечек при масштабировании бизнеса.....	13
Территориально распределенная безопасность: как сделать, чтобы реально работало.....	19
Может ли endpoint-агент работать стабильно на 300 000 + рабочих станций?.....	28
Почему DCAP не DLP? И хорошо это или плохо?.....	35
Модуль Dozor Endpoint Agent for Linux для DLP Solar Dozor 7. Обзор возможностей.....	40
Какой DLP-агент под macOS может предложить российский рынок.....	59
Как мы разрабатывали функционал записи звука с микрофона для проведения расследований ИБ-инцидентов.....	64
Данные нуждаются в прикрытии: чем опасны неконтролируемые файловые хранилища.....	74
Анализ поведения пользователей во благо экономической безопасности.....	85
«С этим сотрудником что-то не так». Как анализ поведения пользователей предотвращает инциденты в фармкомпаниях.....	90
Новости из будущего: прогнозируем поведение пользователя.....	98

Экосистема корпоративной безопасности.

На Форуме DLP+ представили портрет нарушителя ИБ

В июне 2022 года в Москве прошел Форум DLP+, организованный компанией «Ростелеком-Солар», на котором эксперты в сфере информационной безопасности и представители бизнеса обсуждали вопросы противодействия внутренним угрозам корпоративной безопасности. В условиях кардинально изменившейся за последнее время реальности угрозы продолжают эволюционировать.

Перед специалистами стоит проблема выбора эффективных средств защиты в зависимости от ситуации. Решению этой задачи поможет создание экосистемы ИБ-инструментов, полагают эксперты.

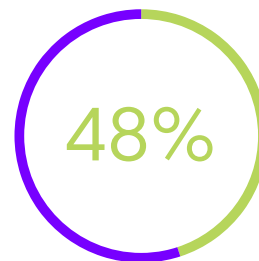


Штрихи к портрету

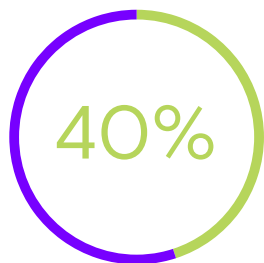


Компания «Ростелеком-Солар» представила на Форуме DLP+ портрет типичного нарушителя ИБ и служебной дисциплины в российской организации. Специалисты проанализировали обезличенные данные отчетов о пилотировании DLP-системы Solar Dozor компании «Ростелеком-Солар» более чем в 100 российских компаниях на предмет признаков нарушений информационной безопасности и служебной дисциплины в минувшем году.

Согласно выводам экспертов, стаж работы типичного нарушителя служебной дисциплины составляет в среднем шесть с половиной лет. Нарушитель трудится преимущественно в кадровой службе организации (около 20% случаев), в юридической, инженерной и ИТ-службе, а также в сфере делопроизводства в статусе помощника руководителя (13%). Чаще всего в категорию нарушителей попадают квалифицированные специалисты (48%).



случаев нарушений служебной дисциплины происходит по вине квалифицированных специалистов



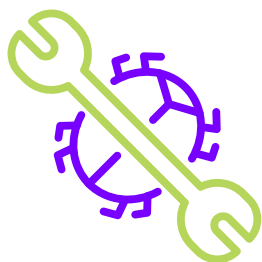
нарушений в течение
рабочего дня – отправка
на личные почтовые ящики
документов с пометкой ДСП

На протяжении рабочего дня нарушитель в лучшем случае занят просмотром развлекательного контента (13% нарушений), а в худшем – отправляет на личные почтовые ящики за пределами организации-работодателя документы с пометкой «Для служебного пользования» (40%) или копирует информацию ограниченного доступа на личные съемные устройства (13%).

По мере адаптации инструментов и подходов, используемых службой ИБ, под новые профили нарушителей все отчетливее становится понимание того, что для управления сопутствующими рисками важно развивать экосистему внутренней безопасности.

Инструменты защиты и мера ответственности

Участники форума обсудили важность внедрения инструментов для защиты данных от угроз и комплексного повышения уровня защищенности российских организаций. В ходе беседы представители государства и бизнеса выразили различные мнения в отношении ответственности компаний за утечки конфиденциальной информации и дали ряд рекомендаций по применению DLP-систем.



«Проблему низкого уровня
защищенности данных
невозможно решить только
путем увеличения штрафов»



В частности, CSO и GR-директор HeadHunter Виталий Терентьев полагает, что проблему низкого уровня защищенности данных невозможно решить только путем увеличения для компаний штрафов за утечку данных. Государство предъявляет все более высокие требования к безопасности информации, следовательно, бизнесу должны быть предложены эффективные инструменты защиты.



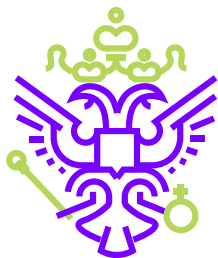
«Нельзя недооценивать
персональную ответственность
человека, допустившего утечку
данных»

Аналогичной точки зрения придерживается руководитель направления защиты информации госкорпорации «Ростех» Игорь Каландадзе, считающий, что нельзя недооценивать персональную ответственность человека, допустившего утечку данных. Если возложить всю ответственность на предприятие, то она будет размываться. При этом компания несет репутационные и финансовые потери.



«Для обеспечения защиты
предлагается немало
разноплановых инструментов
и средств»

Заместитель директора департамента обеспечения кибербезопасности Минцифры России Евгений Хасин напомнил, что для обеспечения защиты предлагается немало разноплановых инструментов и средств. Главное – применять их комплексно, что позволит снизить уровень рисков. Он также отметил, что основная идея недавнего Указа Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» – мотивировать необходимость руководителей предприятий, которые раньше находились в серой зоне и уделяли мало внимания ИБ, заняться вопросами информационной безопасности, внедрения средств защиты.

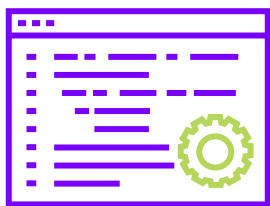


«Под действие Указа подпадает
более 100 тыс. систем
в российских организациях»

Под действие Указа подпадает более 100 тыс. систем в российских организациях. В сфере информационной безопасности достаточно высокая готовность к импортозамещению, немало отечественных средств защиты. Конечно, есть проблемы с оборудованием, их государство планирует решать. Выполнение требований Указа повысит интерес к инвестированию в новые ИБ-решения, в развитие кадрового потенциала отрасли кибербезопасности.

При обсуждении реальных кейсов использования DLP на практике участники конференции сформулировали ряд рекомендаций. Эксперты советуют повседневную рутину доверять настроенным политикам DLP. Также важно организовать совместный доступ к DLP-системе, построив ролевую модель, которая подходит специалистам не только отделов ИБ, но и других подразделений для решения актуальных задач. Очевидно также, что предстоит найти баланс между завышенными ожиданиями и скептицизмом по отношению к DLP: нет повода отказываться от использования этой системы, если с ее помощью можно контролировать 80% каналов.

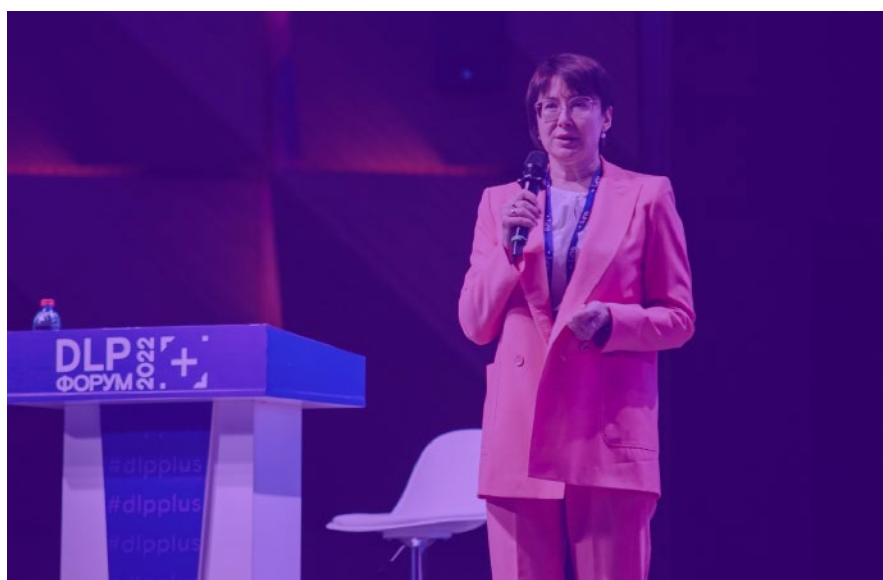
DLP в контуре безопасности



«Классическая история
автоматизации процессов
с точки зрения интегратора
представляет собой
архитектурный «сэндвич»»

Место DLP в системе безопасности предметно анализировалось на одной из тематических сессий. Эксперты считают, что DLP надо интегрировать со смежными системами, обогащать досье данными для проведения расследований, последовательно наращивая возможности экосистемы в сфере защиты от всевозможных угроз.

Классическая история автоматизации процессов с точки зрения интегратора представляет собой архитектурный «сэндвич». На верхнем слое находятся непрерывные процессы, которые отображаются на уровне задач и функций, ниже – область приложений: программных продуктов и ИТ-инфраструктура.



Ожидания заказчиков в сфере защиты от внутренних угроз сводятся к наличию набора программно-аппаратных средств, которые представляют собой единое целое. Однако, по словам директора центра продуктов Solar Dozor компании «Ростелеком-Солар» Галины Рябовой, реальность такова, что вендоры предлагают отдельные решения. При этом немало времени компании тратят на «фичеризацию», чтобы удивить заказчика, придумать внутри предлагаемого продукта нечто такое, что позволит им выделиться среди конкурентов.

Многие компании проделали сложный путь, чтобы вписать продукт DLP в систему безопасности. В «Ростелеком-Солар» шли к этому несколькими маршрутами. Системно анализировали все запросы на интеграцию, пытаясь понять тренды и угадать задачи.

Как показывает практика, вендору немного известно о самом верхнем слое упомянутого «сэндвича» – бизнес-процессах заказчика (закрытая область), чуть больше – о задачах и функциях. «Анализируя запросы на интеграцию к DLP-системе, я пыталась понять, в какую среду вписывается DLP. Очевидных трендов не видела», – говорит Галина Рябова. Предпринимались попытки с помощью участников клуба Dozor очертить область задач.

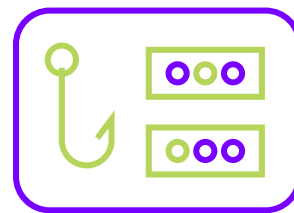
Лед тронулся, когда в 2020 г. компания приступила к реализации крупного проекта внедрения DLP в зрелую экосистему безопасности. В «Ростелеком-Солар» начали поступать обоснованные и внятные запросы на интеграцию. Представителя вендора вовлекли в составление сценариев использования продукта за рамками самого продукта. Не менее важное обстоятельство заключалось в том, что соседним подразделением, которое занимается внешними угрозами, была выстроена экосистема безопасности.

К настоящему времени существенно изменились внешние обстоятельства. Еще полгода назад внутренние утечки воспринимались недостаточно серьезно («да, репутация, безусловно, пострадает, но финансовые риски трудно подсчитать»). Ставки выросли, как только выяснилось, что и секреты нужны, и сотрудники могут быть чересчур политизированы, чтобы умышленно или неумышленно делиться секретами с заинтересованными лицами. Иными словами, на рынке сформировался запрос на создание экосистемы защиты, ландшафт которой постепенно выстраивается.

В последнее время заказчики интересуются файловым аудитором в качестве модуля DLP-системы. Функцию контроля данных «в движении», «на отдыхе» хочется расширить за счет аудита файлов в хранилищах. На этапе инспекции выгружаемых пользователем данных появляется еще одна связанная задача – контроля посещаемых ресурсов. Возникает новый класс продуктов. Сегодня у DLP- и SWG-системы – общее досье.



«Многие компании проделали сложный путь, чтобы вписать продукт DLP в систему безопасности»



«Внутренние утечки воспринимались недостаточно серьезно»



Галина Рябова, директор
Центра продуктов Дозор
компании «Ростелеком-Солар»

Есть запрос на то, чтобы данные DCAP тоже были в общем хранилище, их можно было бы совместно анализировать и т. д. По словам эксперта, агенты DCAP и EDR – технологически очень близкие. Понятно, что удобно пользоваться одним ПО, позволяющим решать широкий круг задач, и при этом избежать установки на станцию двух–пяти инструментов, да еще и разных производителей. DLP как самостоятельная система может служить источником данных для XDR.

Компания близка к выстраиванию непрерывной экосистемы безопасности, причем не только в контуре внутренних угроз. Решение можно увязать с готовой экосистемой в сегменте внешних угроз. Для вендоров это перспективное направление дальнейшего развития. Ресурсы на создание дополнительного функционала (не всегда востребованного) можно переориентировать на то, чтобы обеспечить взаимосвязь систем ради решения общей задачи безопасности.

«Обеспечивая свою кибербезопасность, компании выбирают разные средства защиты, причем они могут быть как от одного, так и от разных вендоров. И крайне важно, чтобы у штатных ИБ- и ИТ-специалистов было понимание того, как все решения можно удобно связать между собой. И тогда в зависимости от того, какая именно угроза актуальна в данный момент, компания сможет взять каждый «кубик» этой экосистемы и выстроить прозрачную и понятную для себя киберзащиту», – пояснила Галина Рябова.

Практические советы по применению DLP-систем

«Когда команда внедрения установила в организации DLP и настроила первоначальные политики, когда подписан акт сдачи системы в эксплуатацию, офицер безопасности остается наедине с этой сложной системой. Руководство компании, которое заплатило большие деньги за внедрение DLP и покупку лицензий, сразу же ожидает получить от нее видимый результат – и начинает нагружать безопасника заданиями, запросами на выгрузку переписки, на проведение расследования или мониторинг определенного сотрудника. Наши практические кейсы предназначены для того, чтобы помочь специалисту по безопасности окупить внедрение DLP, не допустить утечек и по максимуму использовать систему, сэкономив свое рабочее время и время своих коллег», – пояснила Софья Худякова.

Первый совет: использовать политики DLP, чтобы сократить ручной труд

Политики являются основными механизмами выявления инцидентов в DLP-системе. Они строятся на перечнях конфиденциальной информации, которая не должна выходить за периметр организации.

Офицер безопасности, не имеющий достаточного опыта общения с DLP и настройкой политик, для решения поставленных руководством задач зачастую предпочитает поиск: вводит в систему простые поисковые запросы. Система эти поисковые запросы обрабатывает и выдает некий перечень информации, который, на первый взгляд, отражает текущую ситуацию. Однако при ручной обработке большого объема данных нетрудно упустить важную информацию, особенно если она намеренно скрыта злоумышленником.

Поиск хорошо подходит для решения определенного класса задач, но в повседневной рутинной работе с DLP стоит доверять именно политике. DLP-система не устает и видит гораздо больше и лучше человека: она может автоматически найти и классифицировать даже скрытую информацию, создать инцидент, указав место срабатывания, и отправить уведомление офицеру безопасности.



Политика безопасности vs Поиск



Поиск

- Простой и понятный механизм
- Создает иллюзию контроля
- Не исключает человеческий фактор
- Обработка результатов отнимает много времени



Политика безопасности

- Избавит от человеческой ошибки
- Найдёт скрытую утечку
- Автоматически создаст инцидент
- Отправит уведомление офицеру ИБ

Второй совет: организовать совместный доступ к DLP (ролевую модель)



«DLP-система имеет функционал проведения расследований в собственном интерфейсе»

Служба безопасности крупных компаний – это, как правило, разветвленная структура, которая включает в себя не только информационную безопасность, но и экономическую безопасность, отдел внутренних расследований и т. д.

У всех этих подразделений разные задачи, зачастую их расследования не пересекаются между собой. Соответственно, офицеру информационной безопасности могут приходить запросы от смежных подразделений на предоставление данных из DLP-системы, причем эти запросы формируются максимально абстрактно, например – «выгрузить переписку за определенный период». Система тратит большое количество ресурсов на то, чтобы сформировать необходимый пул данных, перенести его на внешний носитель. Таким образом, автор запроса в этом потоке данных долго выявляет факты, которые его действительно интересуют.

В таких ситуациях стоит помнить о том, что DLP-система имеет функционал проведения расследований в собственном интерфейсе, то есть для проведения расследования не нужно выгружать данные. Кроме того, современная DLP-система позволяет гибко настроить права доступа. Если сотрудники разных подразделений безопасности организуют совместный доступ к системе на основе гибкой ролевой модели, обучатся ей пользоваться, это сэкономит время и повысит уровень безопасности организации в целом.

Третий совет: удалять ненужные правила политики

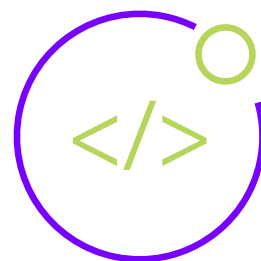
При внедрении системы DLP на нее ставится стандартная политика безопасности вендора, построенная по принципу максимальной возможной полезности для максимального количества заказчиков. Эта политика содержит много правил, которые могут быть не актуальны для текущих задач конкретной компании: например, если компания не производит программное обеспечение, то ей не нужно регистрировать передачу файлов-исходников программ.

Ненужные правила политики могут сильно мешать системе, засорять ее, вызывать технические проблемы и задерживать обработку событий. Кроме того, офицер безопасности, заходя в систему, может столкнуться с массой лишних уведомлений и предостережений.

Хорошей практикой станет ревизия политики безопасности организации, удаление оттуда ненужных правил.

Четвертый совет: сделать доработку политик непрерывным процессом

Любая политика безопасности, даже безупречно настроенная, не может не устаревать со временем. Это происходит из-за того, что мир меняется, компании подстраиваются под новые условия: реагируют на рыночные и масштабные геополитические изменения, начинают использовать в работе новые формы документов, внедряют новые системы и перестраивают многочисленные бизнес-процессы. Если не реагировать на это и не проводить донастройку системы DLP, политика будет не только не отрабатывать важные инциденты, но и генерировать ложноположительные срабатывания в больших количествах. Обработка и фиксация ЛПС может занять продолжительное время.



«Любая политика безопасности, даже безупречно настроенная, не может не устаревать со временем»

Высокое качество политики определяется двумя следующими факторами: достаточной шириной выявления действительных нарушений и минимальным количеством ложноположительных срабатываний. Таким образом, настройка политики включает в себя два основных последовательных шага. Сначала – исключение ложноотрицательных срабатываний: каждая утечка – это огромный риск для организации и триггер к немедленному пересмотру всей политики. Затем – тюнинг, тонкие настройки. В этом процессе исключаются ложноположительные срабатывания.

Тюнинг DLP-политик

Шаг 1 – Исключаем утечки

- Утечка — реальный риск для организации
- Утечка требует немедленного пересмотра

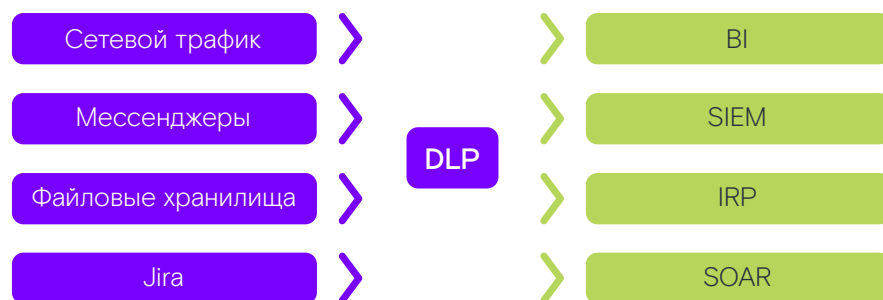
Шаг 2 – Минимизируем ложноположительные срабатывания

- Засоряют пул событий
- Затрудняют поиск реальных инцидентов
- Требуют настройки исключений

Зачастую функциональность DLP устанавливается в компании в стандартном формате, продиктованном требованиями руководства компании или регулятора: например, только мониторинг почтового трафика и мониторинг трафика от endpoint-агентов. Но современные мощные DLP умеют гораздо больше, чем просто обрабатывать трафик от почты и агентов. В них имеются модули анализа сетевого трафика, сканеры файловых хранилищ. DLP может эффективно обрабатывать и данные корпоративных мессенджеров.

Что касается интеграции – от самой системы DLP другие информационные системы организации также могут получать ценную информацию: например, системы обработки событий класса IRP, SOAR или SIEM, BI-системы.

Интеграция DLP-систем со стеком ИТ/ИБ- и бизнес-решений



Выводы

Хорошая практика – это расширение возможностей DLP-систем. Если у вас в руках оказался такой дорогой, мощный, многофункциональный механизм, то следует использовать его возможности по максимуму.



Автор: Софья Худякова,
руководитель отдела
продуктовой аналитики
Центра продуктов Дозор
компании «Ростелеком-Солар»

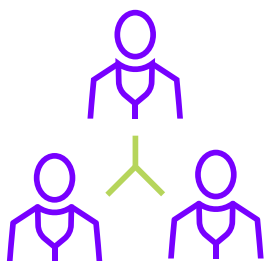
Как защититься от утечек информации при масштабировании бизнеса

Слияния и поглощения компаний происходят на рынке постоянно. Одни компании вливаются в другие и перестают существовать, превращаясь в региональные филиалы, другие становятся дочерними компаниями крупных корпораций. В любом случае более крупной компании, поглотившей или присоединившей другую, достаются ее ИТ-инфраструктура и штат сотрудников. А это в свою очередь означает появление новых рисков с точки зрения информационной безопасности, в том числе утечек конфиденциальной информации. В этой статье расскажем, как в DLP-системе Solar Dozor эта проблема легко решается благодаря модулю MultiDozor для территориально распределенных организаций.

Почему контролировать территориально распределенную компанию сложно

DLP-система предназначена для блокирования утечек информации, контроля коммуникаций сотрудников и выявления признаков корпоративного мошенничества. Даже когда мы говорим об организации, у которой нет филиальной сети или дочерних компаний, внедрение подобной высокопроизводительной системы – масштабный трудоемкий процесс. В случае же с территориально распределенной компанией все еще сложнее. Ведь важно обеспечить не только контроль внутри каждого филиала, но и иметь возможность следить за ситуацией из головного офиса, так как руководитель ИБ-службы несет ответственность за всю компанию с сетью ее филиалов или «дочек».

До появления у вендоров DLP-систем модулей для территориально распределенных организаций решить проблему контроля сотрудников можно было двумя способами.



«Важно обеспечить не только контроль внутри каждого филиала, но и иметь возможность следить за ситуацией из головного офиса»

Первый вариант – отдельные инсталляции DLP в головном офисе и в каждом филиале или дочерней компании. Оперативный централизованный мониторинг в таком случае практически невозможен. Реальное положение дел в каждом филиале известно только работающим там офицерам безопасности. Руководителю ИБ-службы остается полагаться на отчеты, которые он периодически получает от них. При этом проверить их достоверность очень сложно.

Второй вариант – единая инсталляция DLP. Несмотря на то, что звучит это многообещающе, получаем много проблем. Среди них необходимость централизовать весь трафик, создать единое хранилище, куда будут стекаться данные из всех филиалов или дочерних компаний.

В отсутствие готового решения «из коробки» понадобятся высококвалифицированные инженеры, которые смогут развернуть единую инсталляцию во всех филиалах или «дочках» компании и заставят ее правильно работать. Добавим сюда проблему ширины каналов связи в регионах, и станет ясно, что решение может оказаться слишком дорогим и не совсем рабочим.

Как решает проблему специализированный модуль

Модуль для территориально распределенных организаций объединяет отдельные инсталляции DLP в головной компании и филиалах или «дочках» в единую систему. Получается, что контроль есть не только на местах, но и в центре: безопасники в головном офисе видят, что происходит в филиалах, и могут этим управлять. В случае с модулем MultiDozor нашей DLP-системы это реализовано через возможность представить филиалы как подкластеры, которые сами по себе являются отдельными инсталляциями Solar Dozor.

А инсталляция системы с модулем MultiDozor разворачивается в головной компании. Используется единая точка входа в интерфейс, а все территориально распределенные пользователи MultiDozor обращаются к системе через веб-сервис по внутрикорпоративной сети.

Для ИБ-службы это означает возможность централизованно настраивать и применять единые для всей компании политики. Кроме того, можно кастомизировать их под конкретные филиалы. Офицеры безопасности могут в реальном времени получать полную картину по всем филиалам и дочерним компаниям, проводить сквозные расследования, автоматически, а не вручную формировать единые отчеты по всей большой организации. При этом права доступа для безопасников на местах настроены так, что они могут работать с данными только по своему филиалу.

Как это работает в Solar Dozor

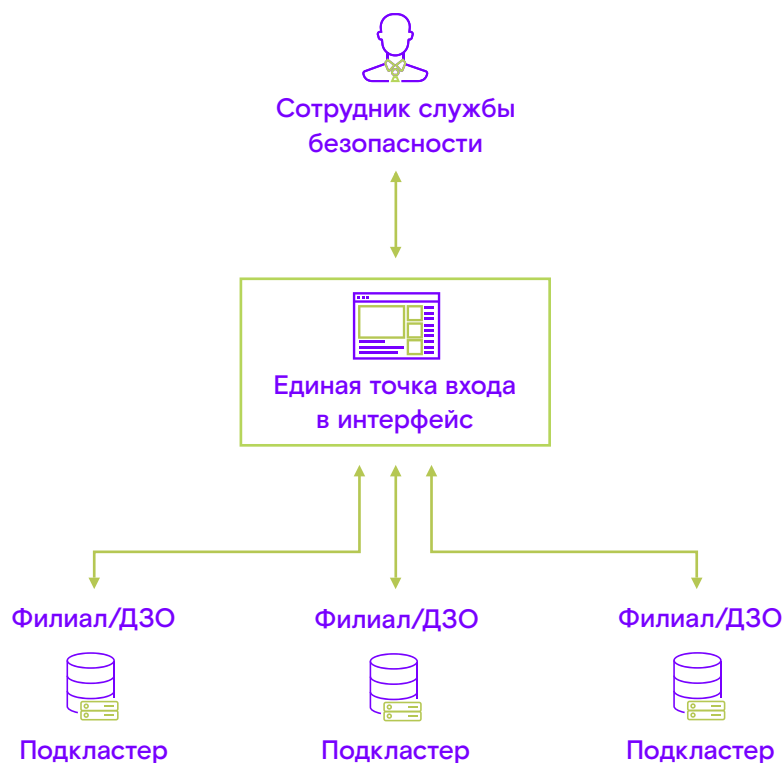
В Solar Dozor благодаря модулю MultiDozor можно реализовать целых три архитектурные схемы работы DLP-системы в территориально распределенной организации. Выбор конкретной схемы зависит от особенностей ИТ-инфраструктуры заказчика.

Первая схема подразумевает, что данные хранятся и обрабатываются в филиалах без передачи в центральный архив. При этом офицер безопасности в филиале видит и работает только с данными своего филиала, а офицер безопасности в центральном офисе работает со своими данными и с данными филиала как с единым целым.



«Благодаря модулю MultiDozor можно реализовать три схемы работы DLP-системы в территориально распределенной организации»

Такой вариант хорошо применим, когда происходит **поглощение компаний**. В этом случае вся ИТ-инфраструктура присоединяемой компании (домен, почта, рабочие станции сотрудников) остается как есть, без объединения с головной компанией.



При второй схеме все данные хранятся и обрабатываются в центре. Например, в том случае, когда произошло **слияние компаний** и все сотрудники пользуются общей почтой, корпоративными ресурсами и т. д. Модуль MultiDozor позволяет разделить пользователей по подкластерам, чтобы офицеры безопасности в филиалах могли работать только с теми данными, которые касаются их подразделения. При этом остается необходимость постоянно пересылать все данные из филиалов в центральный офис, что требует надежных каналов связи.

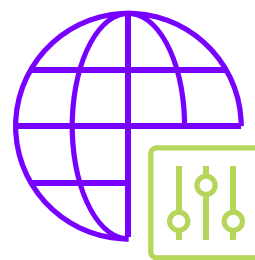
Третья схема представляет собой **гибридный вариант**, когда часть данных хранится и обрабатывается в центральном офисе, часть – в филиалах. Из всех представленных на российском рынке DLP-систем такая схема может быть реализована только в Solar Dozor. Например, модуль MultiDozor поддерживает работу при архитектуре с общей почтой и распределенными endpoint-агентами, которые ставятся на рабочие станции и контролируют действия пользователей на них. Некоторые данные могут быть общими для компании (почта), другая же их часть может обрабатываться в филиалах или «дочках», а затем передаваться в единый центральный архив или же храниться на местах.

Ряд вендоров предлагают в своих продуктах аналогичную функциональность, которая позволяет обеспечить централизованное управление DLP-системой в территориально распределенной организации. Однако в имеющихся на рынке решениях реализована только та схема, при которой все данные филиалов отправляются для обработки в центральный офис. И одной из главных проблем здесь может стать упомянутая выше пропускная способность канала связи.

Не секрет, что у территориально распределенных организаций филиалы часто находятся в местах, где широкие интернет-каналы попросту недоступны. В таком случае передача больших объемов трафика, которым оперирует DLP-система, становится практически невозможной и неизбежно будет мешать бизнес-процессам. При этом, если из какого-то филиала данные доставляются нестабильно, это может повлиять на работу всей системы. Некоторые вендоры предлагают решить эту проблему, установив расписание, когда данные перекачиваются в центр, например вечером или ночью, когда канал не перегружен. Но такой вариант обязательно скажется на оперативности реагирования на инциденты и их расследования.

Кроме того, некоторые рыночные решения, помимо развертывания отдельных инсталляций DLP в филиалах и в головном офисе, также требуют установки в центре дополнительного сервера, который будет агрегировать и обрабатывать полученные данные. То есть заказчику придется нести дополнительные расходы на оборудование.

Модуль MultiDozor не требует дополнительных аппаратных мощностей кроме тех, которые в принципе необходимы для развертывания DLP-системы в инфраструктуре заказчика. А три архитектурные схемы, которые можно реализовать при использовании MultiDozor, позволяют внедрить DLP-систему в любой ИТ-инфраструктуре территориально распределенной организации.



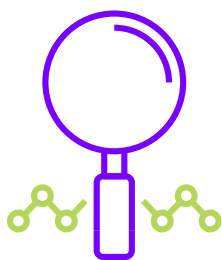
«Модуль MultiDozor не требует дополнительных аппаратных мощностей кроме тех, которые необходимы для развертывания DLP-системы в инфраструктуре заказчика»

Кейсы использования MultiDozor из практики

Мы принимали решение о создании модуля, анализируя запросы заказчиков. Многие корпорации в России и некоторых странах СНГ имеют в своей структуре множество филиалов или дочерних компаний. И часто их разделяют сотни километров. Поэтому проблема сквозного мониторинга для них очень актуальна.

Один из наших заказчиков – нефтяная компания из ближнего зарубежья. У нее достаточно много дочерних организаций, которые расположены в труднодоступных местах.

Собственных ИБ-служб в них вообще нет, а каналы связи в регионах, как известно, порой оставляют желать лучшего.



«MultiDozor также востребован, когда возникает необходимость контролировать новую дочернюю организацию»



С помощью гибридного варианта использования MultiDozor компания наладила централизованный контроль отдаленных филиалов из головного офиса. Лайфхак, который использовали в компании: чтобы находчивые сотрудники не искали способов обхода DLP-системы, ее можно устанавливать под видом каких-либо технических работ.

MultiDozor также востребован, когда возникает необходимость контролировать новую дочернюю организацию. Так, к нам обращался один российский банк, который приобрел страховую компанию, чтобы самостоятельно оказывать соответствующие услуги своим клиентам. В уже сложившейся не очень большой компании важную роль часто играют личные связи и сопряженные с этим злоупотребления. Поэтому даже при наличии в «дочке» внедренной ранее DLP-системы и собственной службы безопасности уровень доверия к последней со стороны головного офиса был невысок. Поступающие отчеты были неполными или недостоверными. При этом доказать факт каких-либо нарушений без централизованного мониторинга дочерней организации невозможно. MultiDozor позволил среди прочего контролировать действия ее офицера безопасности, например, если тот удалял какие-то сообщения в системе.

Выводы

Первый вывод, который напрашивается из всего сказанного выше, очевидный: полноценная работа службы информационной безопасности в корпорации, в которой появляются новые филиалы или дочерние компании, без DLP-системы крайне затруднительна. Появление новых сотрудников, которые сидят где-то вдалеке от головного офиса, подключение ИТ-инфраструктуры присоединяемых компаний – все это повышает риск утечек информации, усложняет мониторинг непрерывности бизнес-процессов, а также контроль рабочих коммуникаций. DLP-система, которая имеет широкие возможности реализации мониторинга территориально распределенных предприятий, все эти риски значительно уменьшает.

Второй вывод: DLP-система должна работать так, чтобы не мешать бизнес-процессам, учитывать особенности ИТ-инфраструктуры, ширину интернет-канала, нюансы организационно-штатной структуры, а также легко и удобно масштабироваться в случае изменений, например при появлении новых филиалов или дочерних компаний. Модуль MultiDozor решает все эти задачи наименее трудозатратным для заказчика способом.



Автор: Андрей Воробьев,
технический партнер Центра
продуктов Дозор компании
«Ростелеком-Солар»

Территориально распределенная безопасность: как сделать, чтобы реально работало

В 2020 году компания "Ростелеком-Солар" в рамках DLP- системы разработала модуль управления безопасностью многофилиальных компаний – MultiDozor. Ниже рассказываем об этом модуле, благодаря которому защита от утечек, профилактика инцидентов выходят на новый уровень.

Кратко о MultiDozor



«MultiDozor позволяет использовать DLP-систему Solar Dozor в территориально распределенных компаниях»

MultiDozor позволяет использовать DLP-систему Solar Dozor в территориально распределенных компаниях, которые заинтересованы в контроле конфиденциальных данных во всех своих коммуникациях. Раньше компаниям для решения подобного рода задач приходилось устанавливать отдельные экземпляры DLP-системы в своих территориальных подразделениях и потом пытаться различными инженерными способами агрегировать данные коммуникаций, если такое вообще было возможно.

Архитектура MultiDozor была создана таким образом, чтобы территориально распределенную конструкцию системы можно было настроить под запросы больших компаний с самыми различными вариантами организации ИТ-инфраструктуры. Какие это могут быть варианты?

Вариант развертывания в подкластерах¹

Этот вариант предназначен для крупных компаний, у которых структурные подразделения четко обособлены и самостоятельно поддерживают свои информационные ресурсы на своих технических мощностях.

Если говорить в терминах MultiDozor, то в подобном случае данные коммуникаций каждой **организационной единицы**² аккумулируются внутри ее подкластера. То есть, к примеру, весь трафик сообщений экземпляра Solar Dozor, установленного в филиале, обрабатывается и накапливается на серверах этого филиала.

Подкластер¹ – совокупность локальных информационных ресурсов, узлов системы в подразделении компании. Узлы подкластера могут обращаться как к хранящимся локально данным Solar Dozor, так и к общим ресурсам.

Организационные единицы (ОЕ)² – термин в MultiDozor, описывающий подразделения в составе территориально распределенных компаний. ОЕ могут быть описаны через соответствующие им подкластеры.

Технически в данном случае организационные единицы соотносятся с подкластерами. Гибкая настройка прав в модуле MultiDozor дает возможность организовать доступ сотрудников безопасности в зависимости от их категории (квалификации, уровня доступа к информации и т.п.): к данным только своего подразделения, к данным нескольких подразделений или к данным всей компании в целом. Доступ офицеров безопасности, работающих с данными только своих филиалов, к данным персон из других филиалов организации ограничивается общими сведениями.

Вариант развертывания в компании с централизованной ИТ-инфраструктурой

Данные всех коммуникаций компании находятся в одном месте, но офицеры безопасности хотят видеть логическое разделение данных по территориальным подразделениям и настраивать права доступа к ним.

Говоря языком бизнеса, в компании используется и контролируется единая корпоративная почта, весь почтовый трафик аккумулируется в одном месте, но при этом требуется понимать, какому подразделению какая часть данных принадлежит, и, соответственно, по-разному организовывать доступ к этим данным.

Такую модель в MultiDozor можно реализовать посредством соотнесения организационных единиц с ветками организационно-штатной структуры, по принадлежности к которым система будет маркировать данные.

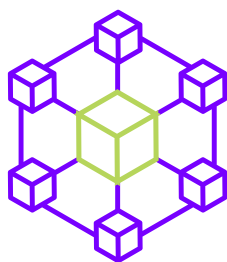


«Говоря языком бизнеса, в компании используется и контролируется единая корпоративная почта»

Комбинированный вариант развертывания с частичной централизацией и использованием подкластеров

Комбинированный вариант развертывания MultiDozor предназначен для крупных компаний, данные коммуникаций сотрудников которых частично находятся в одном месте и частично накапливаются и располагаются в территориально распределенных подразделениях. В качестве примеров можно привести случаи, когда компании используют единую корпоративную почту, а трафик, поступающий в DLP-систему с endpoint-агентов, которые развернуты на рабочих станциях сотрудников, обрабатывается и хранится на ресурсах территориально распределенных подразделений.

Либо часть сообщений может быть общими для организации, другая же их часть может обрабатываться в филиалах и затем передаваться в общий центр обработки данных. При таком варианте организационные единицы соотносятся и с подкластерами, и с ветками организационно-штатной структуры компании.



«MultiDozor является единственным решением на рынке, поддерживающим все известные варианты реализации ИТ-инфраструктуры крупных компаний»

Следует заметить, что MultiDozor является единственным решением на рынке, поддерживающим все известные варианты реализации ИТ-инфраструктуры крупных компаний.

Вариант развертывания в подкластерах в настоящее время наиболее востребован. В использовании такой конструкции оказались заинтересованы крупные компании таких отраслей, как транспорт, топливно-энергетический комплекс, промышленность, а также холдинги, объединяющие предприятия разного рода деятельности. Это объясняется тем, что у данных компаний подразделения обладают высокой степенью самостоятельности, а также тем, что компании указанных сфер зачастую являются объединениями разных дочерних обществ, которые до включения в общую структуру уже обладали собственными ИТ-ресурсами.

Вариант развертывания системы в компании с централизованной ИТ-инфраструктурой заинтересовал организации финансовой сферы. Централизация данных в таких компаниях связана с тем, что они стремятся собрать свою чувствительную информацию в одном месте, а не «распыляться» ею, то есть обеспечить максимально возможный контроль. Это объяснимо, так как именно банки представляют особый интерес для злоумышленников с точки зрения близости к деньгам.

Напротив, многие компании нефинансовой сферы не стремятся разворачивать и поддерживать единые центры обработки данных, да и подобных объемов информации у них, как правило, нет. Поэтому они обычно используют вариант развертывания в подкластерах или комбинированный.

Комбинированный вариант в целом встречается нередко. Ряд компаний практикует развертывание именно такой конструкции с общей почтой и endpoint-агентами на местах. В комбинированном варианте оказались заинтересованы компании сферы энергетики и отдельные организации топливно-энергетического комплекса. С точки зрения бизнеса в такой конструкции нагрузка на территориально распределенную DLP-систему снижается, хотя и сохраняется необходимость выделять производительные мощности под общие ресурсы.

Варианты развертывания в подкластерах либо одновременно в подкластерах и в центре могут быть интересны для государственных организаций, поскольку территориально они распределены по всей стране (в России 85 регионов), а каналы передачи данных у некоторых подразделений могут иметь невысокую пропускную способность.

Использование MultiDozor: практика и нюансы

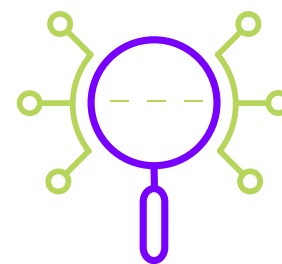
Как показала практика использования модуля, новые возможности оказались очень полезными особенно для сотрудников службы безопасности, контролирующих ситуацию по всей многофилиальной компании.

MultiDozor позволяет выбрать конкретный филиал и исследовать ситуацию исключительно в нем: активность филиальных сотрудников безопасности, коммуникации и данные изучаемого филиала, правила политики безопасности и инциденты филиала. По выбранному филиалу можно построить отчетность. Также можно исследовать коммуникации на предмет межфилиального взаимодействия; тут могут обнаружиться инциденты, плохо заметные в разрозненных DLP-системах, связанные с межфилиальными конфликтами или, и того хуже, – с межфилиальным сговором.

По результатам анализа ситуации в филиалах офицер безопасности из центра с помощью MultiDozor может корректировать политики безопасности в отношении филиалов, а также устанавливать и настраивать endpoint-агенты применительно к каждому филиалу в зависимости от уровня риска.

Учитывая наличие вариантов развертывания в подкластерах и комбинированного, стоит отметить особенности организации хранения данных и доступа к ним. После обработки данные могут храниться как локально на ресурсах филиалов (предпочтительный вариант), так и передаваться на общие ресурсы, если это необходимо.

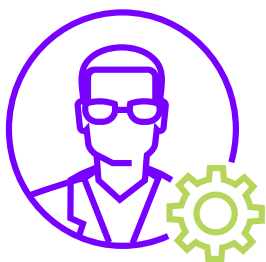
Прежде чем приступить к разработке модуля MultiDozor, был проведен опрос среди потенциальных заказчиков на тему предпочтений в отношении схем доступа к данным. Выяснилось, что большинство высказалось за централизованный подход с возможностью разграничения прав при работе с DLP-системой. Соответственно, архитектура MultiDozor была спроектирована таким образом, чтобы данные могли обрабатываться и храниться локально, но доступ к ним при этом был организован через единый интерфейс – точку входа, к которой могли бы подключаться различные сотрудники службы безопасности.



«MultiDozor позволяет выбрать конкретный филиал и исследовать ситуацию исключительно в нем»

Расширение возможностей

За 2 года жизни MultiDozor получил большое развитие в результате множества пилотов и внедрений в самых разных организациях. Чем же прирос модуль за это время?



«В процессе использования MultiDozor мы выяснили, что у многих клиентов значительно выросло число сотрудников службы безопасности»

В процессе использования MultiDozor мы выяснили, что у многих клиентов значительно выросло число сотрудников службы безопасности, активно работающих на местах с данными только своих филиалов.

Так, сотрудники филиалов одной крупной компании-холдинга сферы ТЭК пользовались широким набором функций Solar Dozor при работе с данными. Поскольку каналы связи в ряде регионов, в которых находились филиалы, оставляли желать лучшего, то процесс просмотра, скачивания скриншотов, файлов, а также прослушивания аудиозаписей осложнялся или становился невозможным. С такой же проблемой к нам обратилась другая крупная компания-заказчик из отрасли перевозок.

Так у нас появилась задача локализовать интерфейс системы в филиалах, то есть сделать локальные точки входа в MultiDozor. При этом потребность в доступе к данным всей компании или части филиалов через единую точку входа никуда не делась.

В результате в модуле появился локальный интерфейс, и при использовании MultiDozor только в подкластерах либо при комбинированном варианте пользователю, который работает с данными своего филиала и не нуждается в доступе к другим коммуникациям компании, теперь нет необходимости обращаться за данными через общий интерфейс. Доступ к сообщениям, файлам, скриншотам, аудиозаписям, а также использование быстрого и расширенного поиска пользователя получают на местах. При этом, если используются общие для MultiDozor функции, локальный модуль обращается к общему интерфейсному модулю и работает с ним совместно (рис. 1).



MultiDozor

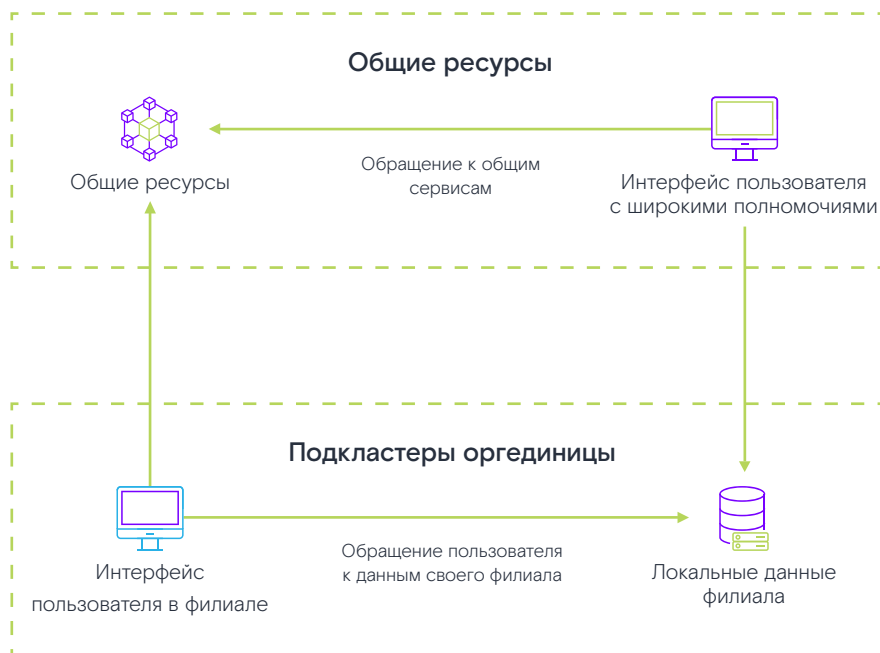


Рисунок 1. Схема реализации MultiDozor с общим и локальным интерфейсом

Такая доработка не только значительно повысила гибкость архитектурной конструкции модуля, но и позволила снизить нагрузку на корпоративную сеть заказчиков, а также ускорить работу системы для пользователей в филиалах.

MultiCrawler

В рамках усовершенствования MultiDozor в территориально распределенный режим работы был также переведен discovery-модуль DLP-системы Solar Dozor – Dozor File Crawler.

Модуль Dozor File Crawler позволяет сканировать файловые и облачные хранилища, а также исторически накопленные почтовые сообщения. Кроме того, модуль позволяет строить карту сети и делает это в инкрементальном режиме, то есть пользователь может видеть изменения, произошедшие с данными с момента их прошлого сканирования.

При помощи Dozor File Crawler офицеры безопасности некоторых компаний-заказчиков получали представление обо всей инфраструктуре корпоративной сети, находили неизвестные ранее места хранения данных, выявляли представляющие угрозу для безопасности места в сети, обнаруживали факты нерегламентированного хранения конфиденциальной информации, перемещали защищаемую информацию в карантин для дальнейших разбирательств.



«Модуль Dozor File Crawler позволяет сканировать файловые и облачные хранилища, а также исторически накопленные почтовые сообщения»



«В Dozor File Crawler появилась возможность настраивать задачи по сканированию файловых ресурсов, сети, архива корпоративной почты, облачных хранилищ в разрезах выбираемых организационных единиц»

Чего не хватало Dozor File Crawler, по мнению заказчиков? Во-первых, настройки задач под различные филиалы, – так как угрозы безопасности и, соответственно, потребности в инвентаризации данных для разных подразделений различны. Во-вторых, представления карты сети в разрезе филиалов, – так как в крупных территориально-распределенных компаниях возникают сложности при анализе всего массива данных, поступающего от Dozor File Crawler.

В итоге в Dozor File Crawler появилась возможность настраивать задачи по сканированию файловых ресурсов, сети, архива корпоративной почты, облачных хранилищ в разрезах выбираемых организационных единиц, то есть физических ресурсов. Кроме того, теперь модуль умеет работать с построенной картой корпоративной сети компании в разрезах организационных единиц.

Технически это было реализовано так, что управляющий модуль Master Dozor File Crawler размещается на общих ресурсах, а задачи по сканированию передает как на общие ресурсы (если это необходимо), так и на служебные модули в подкластерах организационных единиц (рис. 2).

MultiDozor Multi File Crawler

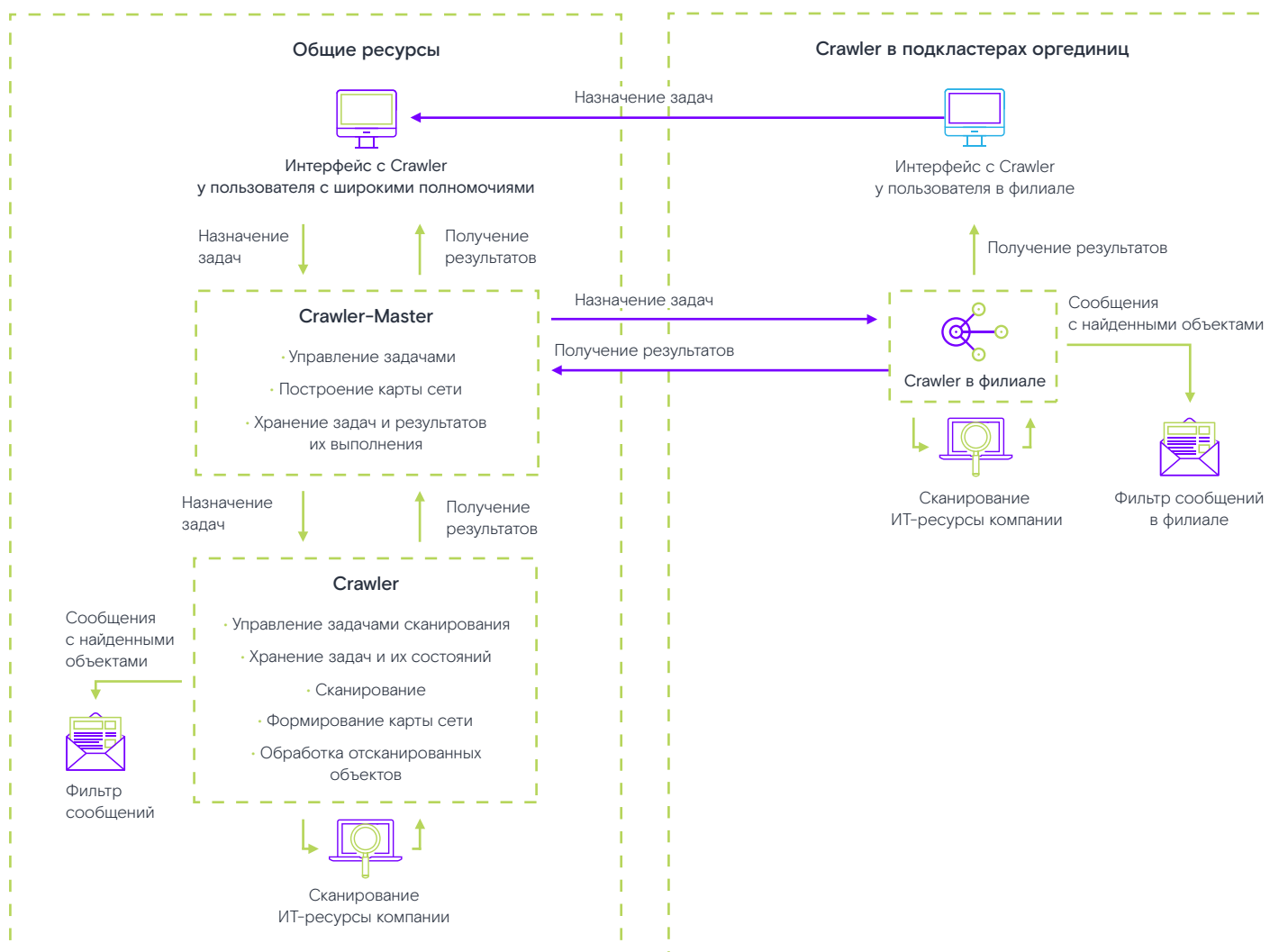


Рисунок 2. Схема реализации Multi File Crawler

Dozor User Behavior Analytics (UBA) – модуль в составе DLP Solar Dozor, который по сути является самообучаемой системой анализа поведения сотрудников. Dozor UBA используется многими клиентами для мониторинга и выявления поведенческих отклонений, детектирования аномалий, предотвращения и расследования нарушений, обнаружения рисков, в том числе ранее неизвестных.

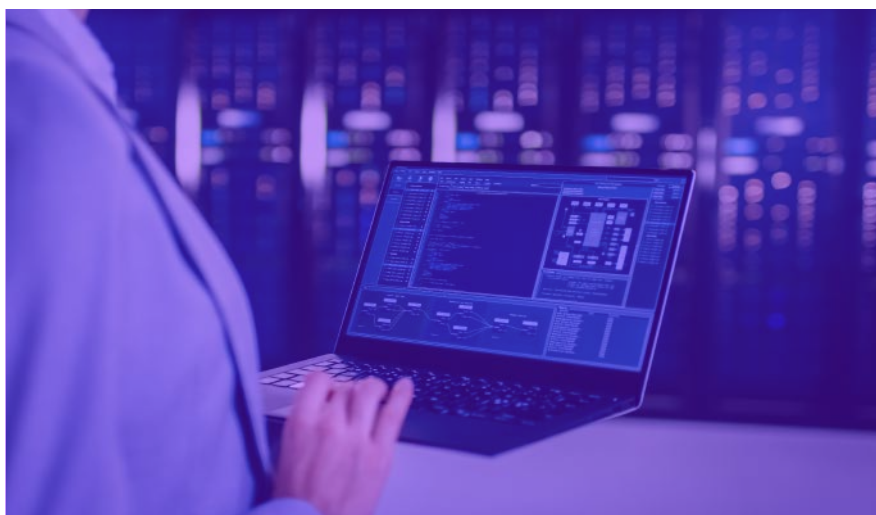
Один из заказчиков в банковской сфере тестировал модуль Dozor UBA в территориально распределенном режиме. В процессе пилотирования выяснилось, что у заказчика есть отдельное территориальное подразделение, которое занимается только техническими вопросами, и есть операционное подразделение, которое активно взаимодействует с внешним миром. У обоих – принципиально разный характер коммуникаций, и сравнивать поведение их сотрудников некорректно. Также по итогам пилота стало очевидным, что необходимо соотносить результаты анализа поведения сотрудников по времени суток (утро, день, вечер, ночь) в филиалах в Москве и, скажем, в Петропавловске-Камчатском.

Именно благодаря этому заказчику в модуле MultiDozor появился механизм расчета показателей поведения, нормы поведения и аномальных отклонений по каждому филиалу (организационной единице). При работе с данными теперь можно фильтровать их в разрезах интересующего филиала. А анализ сообщений по времени суток для каждого филиала осуществляется с учетом его местного времени (часовых поясов).

Технически это было реализовано так, что информация о сообщениях обрабатывается в каждом подкластере организационной единицы, после чего передается модулю Dozor UBA на общих ресурсах, где производятся расчеты поведенческих показателей с учетом принадлежности сотрудников к тому или иному филиалу (рис. 3).



«Dozor User Behavior Analytics (UBA) – модуль в составе DLP Solar Dozor, который по сути является самообучаемой системой анализа поведения сотрудников»



MultiDozor
MultiUBA

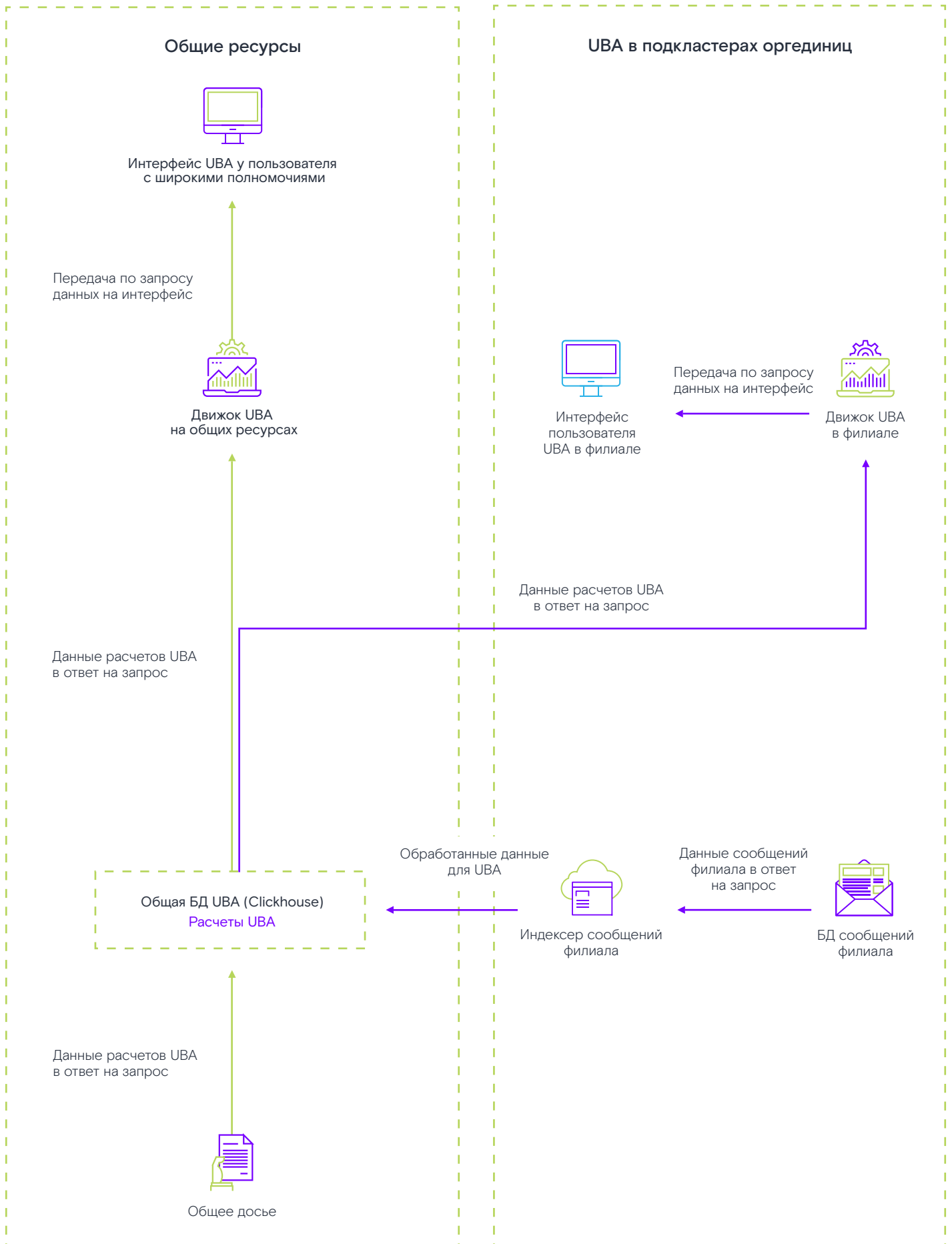


Рисунок 3. Схема реализации MultiUBA

Выводы

На сегодняшний день работа DLP-системы Solar Dozor в территориально распределенном режиме предоставляет службам безопасности компаний беспрецедентно широкий набор возможностей комплексного управления безопасностью как по всей компании, так и по любому отдельному филиалу. Все ИБ-процессы являются сквозными и позволяют в режиме онлайн понимать, что происходит в любой точке любого филиала. С данными можно работать быстро, как централизованно, так и локально, снижая нагрузку на каналы. Можно сканировать сеть на предмет нарушений хранения конфиденциальной информации именно в том филиале, в котором это нужно. Можно из центра выявлять аномалии в поведении сотрудников любого филиала с учетом локального времени суток, предотвращая таким образом будущие инциденты. Только с таким глубоким и одновременно комплексным видением можно обеспечить действительно высокий уровень защиты от внутренних угроз безопасности всей компании в целом и каждого ее подразделения в отдельности.



Автор: Михаил Остапчук,
ведущий аналитик Центра
продуктов Дозор компании
«Ростелеком-Солар»

Может ли endpoint-агент работать стабильно на 300 000+ рабочих станций?



«Защитить бизнес от утечек конфиденциальной информации стремятся как небольшие компании, так и крупные предприятия, независимо от рода их деятельности»

DLP – зрелый и востребованный класс систем. Защитить бизнес от утечек конфиденциальной информации стремятся как небольшие компании, так и крупные предприятия, независимо от рода их деятельности. Но если в первом случае DLP-система ведет себя в инфраструктуре компании вполне предсказуемо, то интеграция в организациях-гигантах может вызвать массу сложностей. Основная причина – огромное количество подконтрольных рабочих станций и, как следствие, критические нагрузки на систему. Как успешно интегрироваться в инфраструктуру корпорации, развернув агенты на трехсоттысячный компьютерный парк, и с какими сюрпризами при этом можно столкнуться, расскажем на своем опыте.

Для защиты конфиденциальных данных компании от утечек с компьютеров сотрудников применяются агенты мониторинга рабочих станций – endpoint-агенты. Руководствуясь настройками и правилами (политиками), полученными от сервера, endpoint-агент успешно позволяет фиксировать, а в решениях некоторых вендоров и блокировать потенциально нежелательную активность, не нарушая при этом общий рабочий процесс пользователя. Перехваченная информация отправляется на сервер endpoint-агента для обработки и анализа специалистом по безопасности. Уже начиная с этого этапа можно встретить ряд сложностей при интеграции на больших предприятиях. И дело далеко не в компетенции специалиста по безопасности.

Сетевая нагрузка

Информация с каждой машины передается постоянно, генерируя огромный информационный поток. При обработке потока с 300 000+ агентов неизбежно возникает высокая нагрузка на сеть. Если оставить этот вопрос без внимания, очень скоро можно столкнуться с увлекательной задачей решения вала возникших проблем. Это может быть потеря перехваченной информации, ошибки получения и обработки перехватов со стороны узла DLP-системы, некорректная работа сетевой коммуникации в целом. Неизбежно будет накапливаться высокая нагрузка, приводящая к нестабильной работе сервисов системы.

Для решения задачи по распределению трафика успешно применяются серверы балансировки. Ограничений выбора такого сервиса у заказчика нет. Это может быть как система, находящаяся в инфраструктуре предприятия, так и реализованная средствами DLP-решения, например, на базе программного обеспечения HAProxy.

Такой сервер способен получать трафик на указанный порт и распределять полученный от агентов поток по различным узлам. Их количество зависит от общего числа автоматизированных рабочих мест (АРМ), контролируемых в компании, и рассчитывается еще до внедрения. Теперь все endpoint-агенты обращаются к балансировщику, который распределяет трафик между узлами. Казалось бы, проблема решена... Но не все так просто!

Разгружаем сервер

Несмотря на разделение информационного потока, на конечные узлы все еще продолжает приходить достаточный объем информации, способный вызвать «волнение» при обработке. И причина здесь даже не в вычислительной мощности оборудования заказчика, хотя и она играет не последнюю роль в этом процессе.

Большинство java-веб-серверов – синхронные. Особенность их работы заключается в резервировании отдельного потока (thread) на каждый http-запрос. В случаях медленного или нестабильного сетевого взаимодействия между агентом и сервером, а также при большом объеме перехваченных данных передача не может осуществляться мгновенно. Обработка будет происходить частями. Значит, на каждый запрос будет открыт новый thread, который не освободится до тех пор, пока запрос полностью не будет обработан. Лишь после этого он вернется обратно в пул, откуда может быть использован повторно.

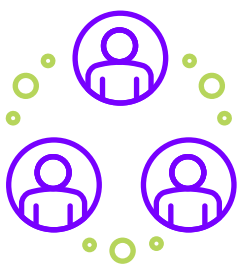
Легко можно рассчитать, что на 1000 запросов с таймингом обработки каждого в 1 секунду сервер израсходует 1000 потоков. Это не слишком критично, когда агентов несколько сотен, но при большем количестве заметно уменьшается производительность.

Потоки в системе являются ограниченным ресурсом. Более того, существуют лимиты по числу одновременно открытых thread на 1 процесс. Все это в комплексе способствует помещению новых запросов в очередь для ожидания освободившегося потока и последующей его обработки. Запросы в очереди не обрабатываются.

Для устранения этой проблемы можно использовать метод асинхронной обработки, например, на базе платформы Netty. Такой подход позволяет освобождать потоки, даже если запрос передан не полностью, и возвращать их обратно в пул. Теперь в запасе всегда есть лишний thread для обработки очередного запроса. Проблема с очередью успешно устранена.



«Несмотря на разделение информационного потока, на конечные узлы все еще продолжает приходить достаточный объем информации, способный вызвать «волнение» при обработке»



«После массового перевода сотрудников на удаленку в 2020 году технология виртуализации рабочих мест стала еще более востребованной»

После массового перевода сотрудников на удаленку в 2020 году технология виртуализации рабочих мест стала еще более востребованной. Многие компании используют виртуализацию посредством технологии «золотого образа». Если не углубляться в подробности, технология позволяет централизованно хранить рабочие данные сотрудника, а при его удаленном подключении к рабочему месту в компании автоматически создавать персональную виртуальную машину с развернутым на ней необходимым программным обеспечением для выполнения сотрудником рабочих задач. Перечень программ определяется при настройке «золотого образа» системы, из которого и происходит клонирование пользовательских виртуальных станций. Такие машины используются однократно, а «золотой образ» служит эталонным шаблоном при создании клонов. После использования виртуальные машины автоматически удаляются.

Однажды один из заказчиков обратился к нам с предложением рассмотреть возможность взять под контроль и такие рабочие места. Главной проблемой здесь стала невозможность отслеживать временные виртуальные АРМ и своевременно удалять более не используемые. В небольших организациях можно попытаться реализовать такой контроль в ручном режиме, однако в масштабах заказчика (более 300 тыс. динамических АРМ) это становилось непосильной задачей. Кроме этого, агент на клонированной машине должен быть уникальным с собственным персональным ID. Очевидно, требовалась автоматизация процесса.

Мы проанализировали ситуацию и сформулировали 3 основные задачи, которые требовалось решить.

1. Автоматическое распределение клонированной АРМ в группу с соответствующими настройками перехватов на сервере DLP-системы.
2. Своевременное удаление неиспользуемых АРМ из списка.
3. Триггеры для генерации уникального идентификационного номера каждого агента.

Для решения этих задач endpoint-агент получил в свое распоряжение два дополнительных параметра – метку и флаг. Они позволили немного скорректировать запрос от клонированных машин. Теперь при их наличии агент передает произвольную метку (заказчик может сгенерировать ее самостоятельно). При указании такой же метки в настройках группы на сервере, куда предполагается распределить АРМ, система получает возможность выполнять автоматическое добавление станций в группу.



Рисунок 1. Настройка автодобавления станций в группу

Флаг позволяет идентифицировать вновь созданную машину как временную и сгенерировать ряд параметров для помещения ее в категорию временных APM (рис. 2), а также определить таймаут удаления из списка агентов на сервере (рис. 3). Для более комфортного управления была добавлена настройка, позволяющая задавать период таймаута. Кроме этого, флагом диктуется необходимость присвоения уникального ID.

	Имя хоста (IP-адрес)/ID	Статус	Подстатус	Подкластер	Пользователи	Версия/OS
	gold 192.168.11.19 c539e561-b952-23fc-3430-bbc74fb147d2	Работает				4.1.1.363 Win 10 Pro ...
Временные станции						
	machine-001.horizon.local 192.168.11... 743a44e9-ba73-34da-7c6e-eab134d3e1dd	Работает			ha	4.1.1.363 Win 10 Pro ...

Рисунок 2. Категория временных станций

Таймаут удаления временных станций (мин)	short-lived timeout	480
Максимальное время недоступности агента (мин)	station-silent timeout	14

Рисунок 3. Настройки по выставлению таймаутов

Теперь пользовательские машины в автоматическом режиме распределяются в группы и удаляются по истечении таймаута недоступности, а каждый агент вновь созданного клона получает уникальный идентификатор.

Победа любит подготовку

Для любой компании-заказчика важна надежность: безопасность системы и устойчивость бизнес-процессов при ее внедрении. Однако невозможно предугадать все проблемы, которые могут проявиться при интеграции системы в масштабах сотен тысяч рабочих станций. Для этого нужно использовать комплексный подход при тестировании продукта, прежде чем он будет внедрен в инфраструктуру заказчика.

Частой проблемой является различное поведение одной и той же функции при разного рода нагрузках. Функциональность, стабильно работающая на малом числе агентов, может отрицательно показать себя на большом объеме. Залогом успеха является своевременное детектирование таких проблем.

Для того чтобы прогнозировать поведение продукта в масштабах предприятий с более чем 300 тыс. агентов, нужно проводить ряд операций по функциональному и нагрузочному тестированию. Для этих целей разрабатываются уникальные скрипты, позволяющие имитировать нагрузку реальной структуры заказчика путем генерирования сложных запросов с их изменяемым количеством в дельту времени. Такой подход позволяет более качественно выявлять нестабильное поведение и предпринимать действия по его исправлению.

Так, в нашей практике была детектирована и успешно исправлена одна из проблем, оказывающая влияние на доступность функциональности по управлению агентами. С точки зрения пользовательского интерфейса она проявляла себя как невозможность загрузки списка установленных агентов и выполнения команд по управлению ими.

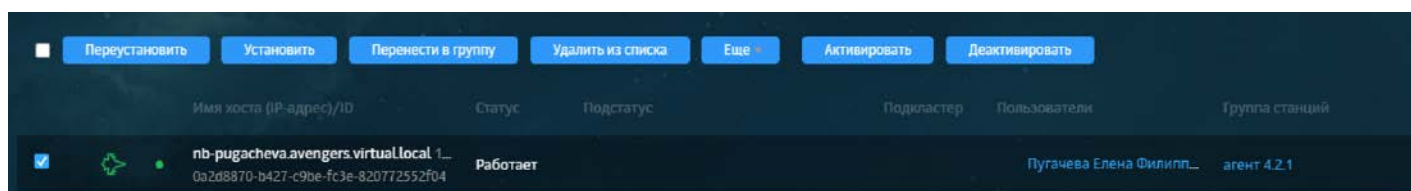


Рисунок 4. Элементы управления Endpoint Agent с сервера

Дело в том, что агенты постоянно присылают свой ping на сервер, в котором содержится служебная информация, необходимая для их контроля. Данные попадают в специально выделенную таблицу базы данных, чем провоцируют ее регулярное обновление. Однако каждая последующая строка данных, как правило, оказывается физически больше, чем предыдущая. В результате каждая новая строка не умещается в освободившееся от старой место, и для нее выделяется новый блок.

В данном случае размер такой таблицы увеличивался в прямой прогрессии и мог вырасти с 1 ГБ до 300 ГБ всего за несколько дней. Это, в свою очередь, сказывалось и на ее производительности. Ведь при последовательной обработке приходилось считывать большее количество частично заполненных блоков. При малом количестве агентов подобная проблема не критична и практически не оказывает влияния на работу, однако в описываемом кейсе масштабной интеграции она становилась заметнее и приводила к ошибкам. После оптимизации таблицы проблема была успешно устранена.

Но даже такой подход не всегда позволяет обратить внимание на те функции, которые, казалось бы, и так работают стабильно. При этом со стороны заказчика могут возникать пожелания, анализируя которые, можно найти способ для еще большей оптимизации алгоритмов. На помощь приходит обратная связь и стремление к совершенству.

Выводы

Успешное функционирование агента в масштабах организаций с более 300 тыс. агентов не миф, а реальная практика. Несмотря на разное поведение одной и той же функциональности при различных нагрузках, ее всегда можно оптимизировать. А регулярные проверки работоспособности в собственной инфраструктуре позволяют гарантировать стабильное поведение продукта даже на больших предприятиях и, как следствие, получать благодарного заказчика.

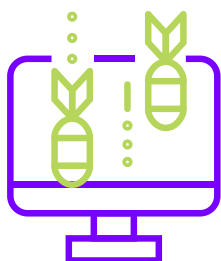


Автор: Евгений Гришкин,
инженер 3-й линии поддержки
Центра продуктов Дозор
компании «Ростелеком-Солар»

Почему DCAP не DLP? И хорошо это или плохо?

Сейчас все чаще говорят о DCAP как об элементе DLP. Некоторые производители DLP-систем представляют DCAP-модули собственной либо сторонней разработки, с большей либо меньшей глубиной интеграции в свои продукты. Создатели независимых DCAP-решений, наоборот, отгораживаются от DLP и утверждают, что это непересекающиеся продукты с совершенно разным функционалом. Насколько DCAP – часть DLP, мы постараемся разобраться в этой статье.

Для чего нужна DLP-система

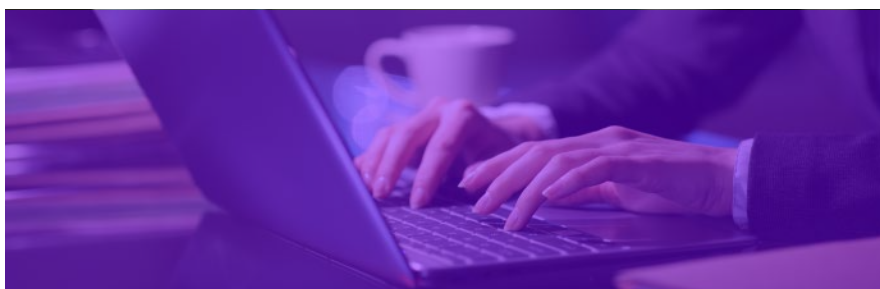


«Задача DLP – предотвращение утечек информации»

Задача DLP – предотвращение утечек информации. По сути, это активное реагирование на действия пользователей, которыми в самом упрощенном понимании являются передача конфиденциальной информации за контролируемый периметр организации: например, отправка по электронной почте или запись на внешний носитель.

Аналитические механизмы DLP также используются для выявления сотрудников, несущих потенциальные риски для организации: лиц, по каким-либо причинам планирующих сменить работу, ищущих параллельные источники дохода, увлекающихся наркотиками, религиозными культами и прочей деструктивной деятельностью, да и просто бездельников. Востребованность этого функционала даже привела к появлению в составе DLP-систем отдельных модулей: контроля рабочего времени, поведенческого анализа и профилирования персонала.

Кроме того, входящие в состав DLP сканеры (так называемые краулеры) позволяют успешно категоризовать информацию, хранящуюся как на пользовательских АРМ, так и на петабайтных СХД, выявлять факты хранения конфиденциальной информации в неположенных для этого местах. А некоторые даже умеют переносить такую выявленную информацию в специальные защищенные хранилища. И тем не менее основной задачей DLP-системы остается функция, зашифрованная в ее аббревиатуре.

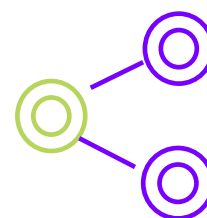


Для чего нужен DCAP

Назначение системы DCAP иное: категорирование информационных массивов организации – файловых хранилищ, аудит прав доступа к файлам, а также регистрация обращений к ним пользователей. То есть DCAP ничего не предотвращает, зато выявляет потенциальные угрозы утечек иным, в отличие от DLP, способом: определяя избыточные права доступа к информации, регистрируя аномальную активность пользователей при обращении к ней, а также выявляя нарушения правил хранения конфиденциальной информации.

Похожие, но разные

Как мы видим, в некоторых местах функционал DLP и DCAP пересекается: обе системы способны сканировать файловые хранилища, обе системы используют аналитические механизмы и OCR для категорирования информации и выявления конфиденциальных данных. Но функционал DCAP сфокусирован на сервисной поддержке ИТ-инфраструктуры и выявлении потенциальных уязвимостей, связанных с ошибками распределения AP-полномочий пользователей и прав доступа к файлам в файловых хранилищах. DLP-система же нацелена непосредственно на предотвращение утечек конфиденциальной информации, а функции сервисного аудита не являются ее целевой задачей.



«В некоторых местах
функционал DLP и DCAP
пересекается»

Например, рассмотрим одинаковый, казалось бы, для DLP и DCAP функционал сканирования файловых ресурсов и категорирования информации, которая на них хранится. Решая эту задачу, DCAP построит карту файловых хранилищ, классифицирует информацию и выявит нарушения прав доступа к ней. А краулеру – компоненту DLP-системы, предназначенному для выявления хранения конфиденциальной информации в неразрешенных для этого местах, глубоко безразлично, какие у этих выявленных файлов права. Его задача – как можно быстрее обнаружить такие файлы, убрать их из общедоступных мест и перенести конфиденциальную информацию в предназначенное для этого защищенное хранилище, с соответствующим ограниченным доступом.

Проще говоря, DLP сфокусирована на контентном анализе информации, классификации конфиденциальных данных и ограничении их передачи, а DCAP – на общей классификации информации, хранящейся на корпоративных СХД, и аудите доступа к ней.

Еще большая разница наблюдается в потребителях информации об инцидентах, генерируемых DLP- и DCAP-системами.



«Расследованием инцидентов, выявленных DLP-системой, занимаются подразделения внутренней и экономической безопасности»

DLP ориентирована на подразделения безопасности. ИТ-специалисты в части взаимодействия с DLP только настраивают систему, разворачивают на рабочих станциях агентов, а также решают технические вопросы при их возникновении. Иногда – пишут политики безопасности, что, собственно, неправильно: для настройки в DLP качественной политики требуется анализ реальных образцов документов, имеющих ограничительные грифы организации («конфиденциально», «коммерческая тайна» и т. п.). А сисадмин не может и не должен иметь доступ к такой информации, разве что к конфиденциальным данным, относящимся к сведениям об ИТ-инфраструктуре.

Поэтому расследованием инцидентов, выявленных DLP-системой, занимаются подразделения внутренней и экономической безопасности, которые отсекают ложноположительные срабатывания (ЛПС), идентифицируют участников инцидента и проводят соответствующие мероприятия. ИТ-специалисты же к непосредственной обработке DLP-инцидентов привлекаются время от времени, по мере необходимости, например, для проведения гарантированного удаления конфиденциальной информации из почтовой системы после выявления попытки утечки.

У DCAP-систем все наоборот, целевые потребители зарегистрированных инцидентов – ИТ-подразделения. Это системные администраторы средств ИБ, которые сами обрабатывают эти инциденты и генерируют на доменных администраторов ИТ-департамента обращения по исправлению проблем информационной безопасности, связанные как с нарушением прав доступа к данным, так и с хранением конфиденциальной информации в ненадлежащих местах на корпоративных файловых хранилищах. Для отсека ЛПС и подтверждения идентификации конфиденциальных данных, обнаруженных DCAP-системой, привлекаются сотрудники службы ИБ из подразделения защиты конфиденциальной информации. Именно они определяют, действительно ли данная информация должна быть ограничена в доступе, и, если это так, проводят собственное расследование и определяют место, куда эта информация должна быть перенесена. При этом системные администраторы, как было сказано выше, не должны иметь самостоятельного доступа к конфиденциальным файлам и оперируют лишь кратким резюме на срабатывание.

Не интеграция, а взаимодействие

Сложности в организации применения одной системы в интересах двух разных групп пользователей привели к тому, что DCAP-системы стали развиваться в отдельное самостоятельное направление ИБ. И развитие это, как мы наблюдаем, – вполне успешное.

Конечно, и DLP, и DCAP внедряются в корпоративные SIEM- и IRP-системы, передают в них свои инциденты, не дублируя их и не конкурируя друг с другом, а, скорее, наоборот, дополняя. Так, наличие в организации системы DCAP позволяет не только выявлять потенциально слабые места в ИТ-инфраструктуре (нарушения прав доступа к информации), но и обогащает сгенерированные DLP-системой инциденты дополнительной информацией для проведения успешного расследования (например, за счет предоставления статистической информации о доступе нарушителя к тому либо иному документу).

Что же до непосредственной интеграции DCAP в продукт DLP, то, несмотря на идентичность ряда компонентов этих систем, надо вспомнить, что пути их уже один раз разошлись по вполне обоснованным причинам. И здесь уместно упомянуть русскую басню про последствия впряжения в одну телегу трех разных животных. А схожесть функционала описывается русской же пословицей «кто в лес, кто по дрова»: вроде бы ходят иногда в одни и те же места, но с разными целями.



«Именно сложности в организации применения одной системы в интересах двух разных групп пользователей привели к тому, что DCAP-системы стали развиваться в отдельное самостоятельное направление ИБ»

В поиске выбора

Но не дорого и не избыточно ли иметь сразу две системы? Может быть, стоит ограничиться чем-то одним?

Смогла бы серьезная организация обходиться без функционала DLP? Конечно, нет. Ее присутствие, во-первых, останавливает потенциальных нарушителей от непоправимых поступков, а во-вторых – действительно предотвращает реальные утечки. И заменить такую систему нечем. Более того, практика показывает, что большинство утечек чувствительной информации осуществляют люди, получившие к ней доступ вполне себе легитимно, а утечка такая произошла даже не по злому умыслу, а по банальному разгильдяйству, и только правильно настроенная, работающая в активном режиме DLP-система сможет такую утечку предотвратить.

С другой стороны, DCAP автоматизирует процесс контроля организации доступа к файловым ресурсам и распределения прав, что существенно облегчает работу системного администратора и снижает потенциальные риски в любой крупной организации. А для сегмента крупных компаний решениям DCAP просто нет альтернативы.



Автор: Дмитрий Мешавкин,
старший аналитик Центра
продуктов Дозор компании
«Ростелеком-Солар»

Выводы

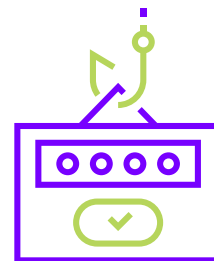
Как известно, самые страшные секреты можно найти в какой-нибудь синей папке, забытой на автобусной остановке – и ни DLP, ни тем более DCAP не сможет гарантированно оградить от такой ситуации. Но такие случаи единичны на фоне количества инцидентов, связанных с нарушением правил хранения и передачи конфиденциальной информации. Поэтому и DLP, и DCAP должны являться неотъемлемой частью корпоративной инфраструктуры ИБ.

Модуль Dozor Endpoint Agent for Linux для DLP

Solar Dozor 7. Обзор возможностей

Говорит статистика по утечкам данных

В 2021 г. количество утечек информации достигло очередного максимума. Согласно данным, собранным командой Atlas VPN, в течение 2021 года от утечек данных **пострадало 5,9 млрд учетных записей**. Исследовательский центр по краже личных данных (ITRC) косвенно подтверждает эту статистику: в 2021 г. по сравнению с 2020 годом количество зарегистрированных утечек данных увеличилось на **17%**, а ущерб от утечек – минимум на **10%**.



«В 2021 г. количество утечек информации достигло очередного максимума»

Основные цифры по утечкам информации в 2020–2021 гг.:



\$4,24 млн

за инцидент – средний ущерб от утечек во всех сферах



\$9,23 млн

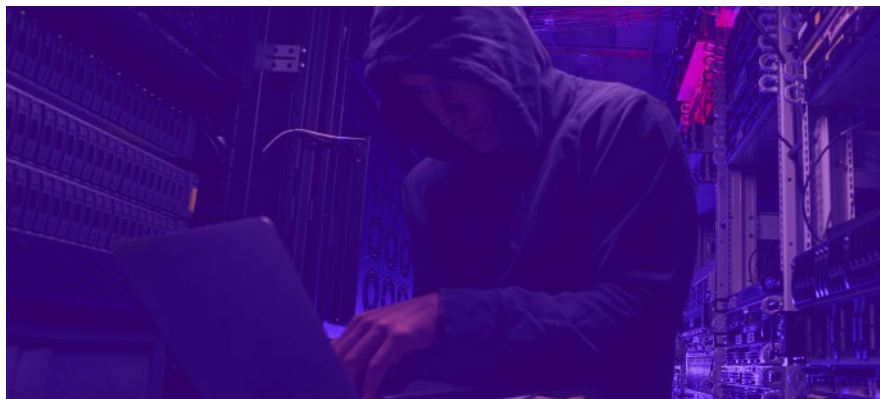
ущерб от утечек данных в сфере здравоохранения

5,9 млрд

пострадало учетных записей (по данным Atlas VPN)

40%

более чем в 40% случаев к утечкам причастны сотрудники компаний (по данным «Ростелеком–Солар»).





«Своевременное выявление утечек и защита от них обеспечивается в том числе с помощью комплекса мер мониторинга и контроля действий пользователей рабочих станций»

Учитывая текущую обстановку в России, были все основания предполагать, что 2022 г. мог в худшем смысле побить эти рекорды, то есть подобные инциденты могли происходить чаще и в более крупных масштабах. В первой половине 2022 года зарегистрировано несколько крупнейших утечек данных. Так, например, по данным сервиса разведки утечек информации и мониторинга даркнета DLBI, с конца февраля 2022 года в Сеть утекли данные более 8 млн российских пользователей различных сервисов доставки еды.

А по словам заместителя председателя правления Сбербанка С. Кузнецова, с того же времени были украдены данные 65 млн россиян, скомпрометированы не менее 13 млн банковских карт, ущерб из-за перевыпуска которых составил не менее 4,5 млрд рублей.

Своевременное выявление утечек и защита от них обеспечиваются в том числе с помощью комплекса мер мониторинга и контроля действий пользователей рабочих станций (персональных компьютеров, ноутбуков, терминалов и т. п. устройств).

Для этого на рабочие станции устанавливается специальный программный модуль DLP-систем – агент. Этот модуль собирает информацию о действиях пользователей рабочей станции и передает ее DLP-системе.

В обзоре мы рассмотрим возможности модуля DLP-системы Solar Dozor версии 7 – Dozor Endpoint Agent for Linux, который собирает информацию с рабочих станций под управлением операционных систем (ОС) семейства GNU/Linux. Модуль устанавливается и работает незаметно для пользователя рабочей станции.

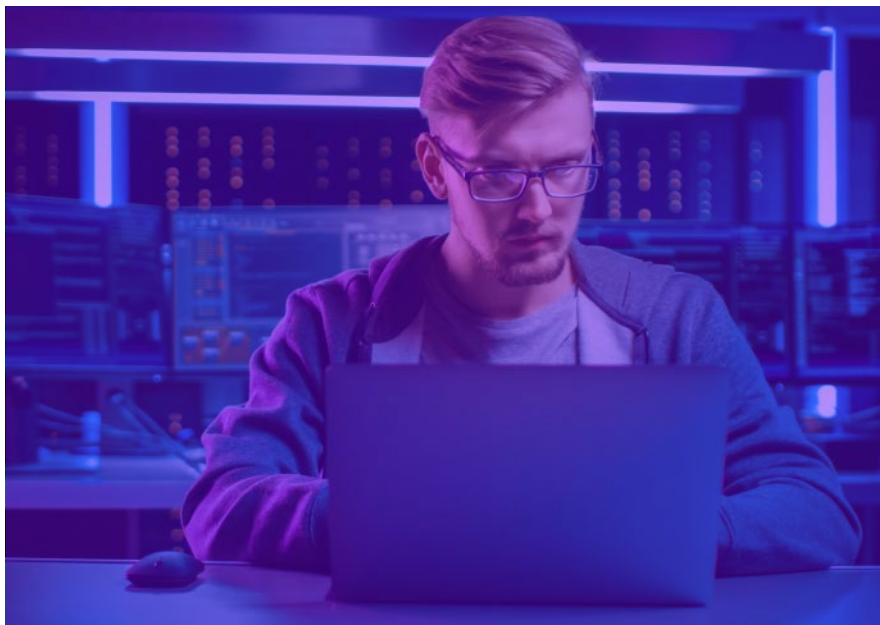
Dozor Endpoint Agent for Linux в свете импортозамещения



«DLP-система Solar Dozor и ее модуль Dozor Endpoint Agent for Linux являются комплексным решением, соответствующим стандартам защиты персональных данных и коммерческой тайны»

DLP-система Solar Dozor и ее модуль Dozor Endpoint Agent for Linux являются комплексным решением, соответствующим стандартам защиты персональных данных и коммерческой тайны, которое может использоваться для импортозамещения:

- оба продукта включены в Единый реестр отечественного программного обеспечения (№ 7441 / №7447),
- имеется сертификат соответствия ФСТЭК России № 3706 по 4-му уровню контроля отсутствия недеklarированных возможностей и техническим условиям,
- подтверждена совместимость Dozor Endpoint Agent for Linux с российскими ОС Astra Linux «Орел», Astra Linux «Смоленск» и РедОС «Муром».



Согласно реализуемой в России программе импортозамещения, к 2025 г. все государственные организации должны перейти на отечественное программное обеспечение (ПО), работающее на ОС, в том числе отличной от распространенной Windows. Вариант замены Windows на Linux – один из самых очевидных.

Уже сейчас во многих компаниях рабочие станции сотрудников постепенно массово переводятся на Linux. Например, известно, что российская корпорация «Росатом» планирует полностью перейти на отечественную операционную систему Astra Linux до конца 2024 г. и в целом импортозамещены будут **до 130 тыс.** рабочих мест по всей стране.



Наличие полнофункционального Linux-агента способствует тому, что уровень защиты от утечек информации при этом не снижается.

Модуль Dozor Endpoint Agent for Linux работает на многих ОС семейства Linux, среди которых:

• **Отечественные ОС:**

- Astra Linux Special Edition версий 1.6 («Смоленск») и 1.7 («Орел», «Смоленск», «Воронеж»);
- Astra Linux Common Edition 2.12 («Орел»);
- Альт 8 СП;
- Альт Рабочая станция 9;
- Гослинукс ИК6;
- РЕД ОС 7.2/7.3 («Муром»).



«Наличие полнофункционального Linux-агента способствует тому, что уровень защиты от утечек информации при этом не снижается»

• Свободно распространяемые ОС:

- CentOS 7/8;
- Debian 10/11;
- Linux Mint 20.3;
- Ubuntu 18.04/20.04 LTS.

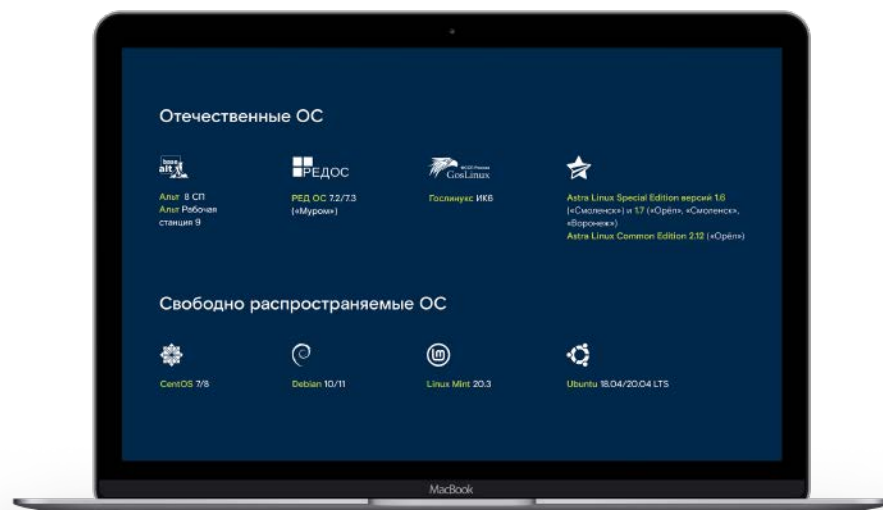
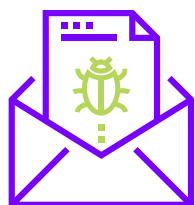


Рисунок 1. Операционные системы, на которых работает Dozor Endpoint Agent for Linux

О назначении и функциях Dozor Endpoint Agent for Linux: краткий ликбез



«Наличие подробных сведений о действиях сотрудников предприятия на рабочих станциях, включая их переписку, позволяет на ранней стадии выявить потенциальных нарушителей»

Наличие подробных сведений о действиях сотрудников предприятия на рабочих станциях, включая их переписку, позволяет на ранней стадии выявить потенциальных нарушителей, вовремя начать расследование и таким образом предотвратить утечку важной информации. Также необходимы меры противодействия, включая контроль и запрет определенных операций.

С помощью модуля Dozor Endpoint Agent for Linux и автоматизированного процесса ИБ-службы могут контролировать:

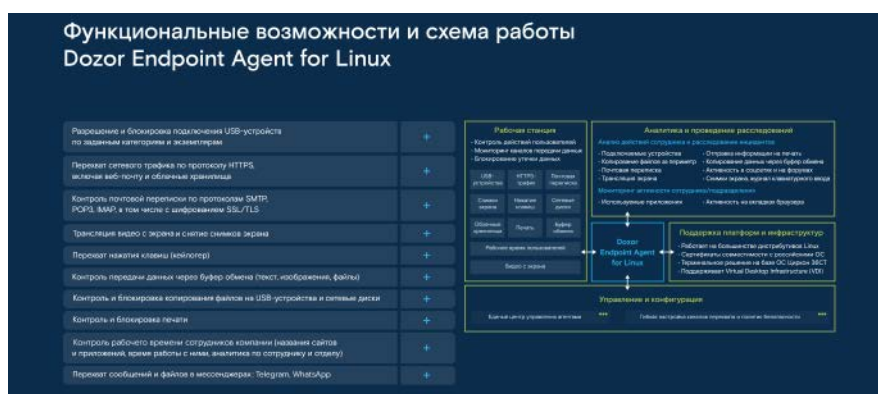
- переписку в веб-почте, общение в соцсетях;
- публикацию данных в облачных хранилищах Yandex.Disk и Mail.Cloud через веб-браузер;
- переписку в мессенджерах Telegram (через веб-версию и десктопное приложение) и WhatsApp (через веб-версию);
- операции с внешними устройствами (флеш-накопителями, картами памяти, внешними жесткими дисками и т. п.), подключенными через USB-порт к рабочим станциям сотрудников;
- операции с буфером обмена;
- операции с файлами (в том числе с архивами), включая:
 - копирование/перемещение на съемные носители и сетевые диски,
 - печать на принтере.



Иными словами, некорректные с точки зрения политики безопасности действия пользователей рабочих станций могут быть автоматически заблокированы:

- Печать документа блокируется путем удаления (отмены) сформированного системой задания на печать.
- Передача файлов на внешние носители и сетевые диски блокируется путем запрета записи файла на соответствующий внешний ресурс.
- Подключение USB-устройств блокируется специальным программным компонентом, который получает и анализирует информацию об устройстве до того, как оно будет отображено в системе, и при наличии блокирующей политики отключает устройство.

Кроме того, агент собирает сведения о действиях пользователей рабочих станций в приложениях и интернете. Помимо контроля в сфере безопасности, включая выявление различных схем мошенничества и предотвращение утечек данных, это позволяет руководству компании увидеть, как и на что сотрудник тратит свое рабочее время.



44

Работа Dozor Endpoint Agent for Linux гибко настраивается – в веб-интерфейсе Solar Dozor офицер безопасности может указать, кого, что, как и по какому каналу надо контролировать.

Общий процесс настройки включает следующие шаги:

1. Объединение рабочих станций с установленным модулем Dozor Endpoint Agent for Linux в конкретную группу, например группу станций, физически расположенных в Санкт-Петербурге.

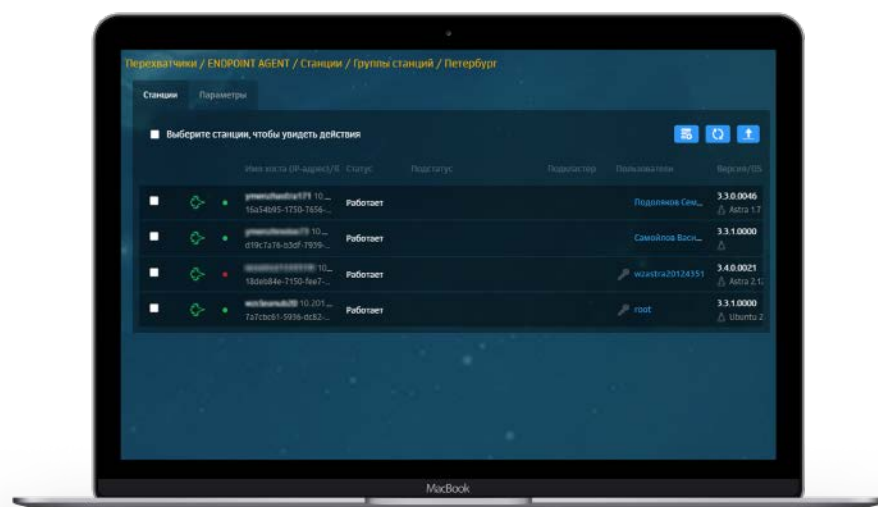


Рисунок 3. Пример объединения рабочих станций с установленным агентом в группу

2. Создание профиля (набора) настроек, которые планируется применять для группы станций. Используя шаблон со стандартными настройками перехвата, можно создать новый профиль настроек, в котором задать, что и как перехватывать: установить нужные флажки и при необходимости изменить списки ресурсов, приложений и т. п. (списки составлены экспертами «РТК-Солар» и поставляются вместе с системой).

Так, например, при установке флажков на «Каналы перехвата» и «HTTP/HTTPS» агент будет перехватывать сообщения и файлы, переданные

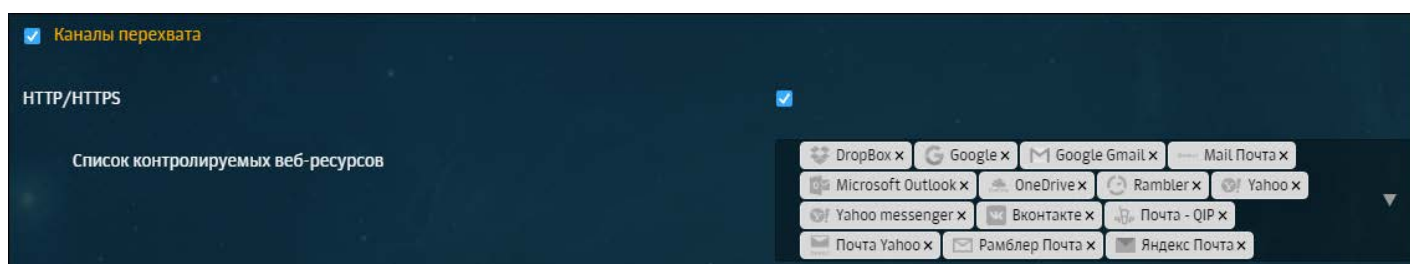


Рисунок 4. Пример настроек для группы рабочих станций.

3. Создание набора правил агентской политики безопасности.

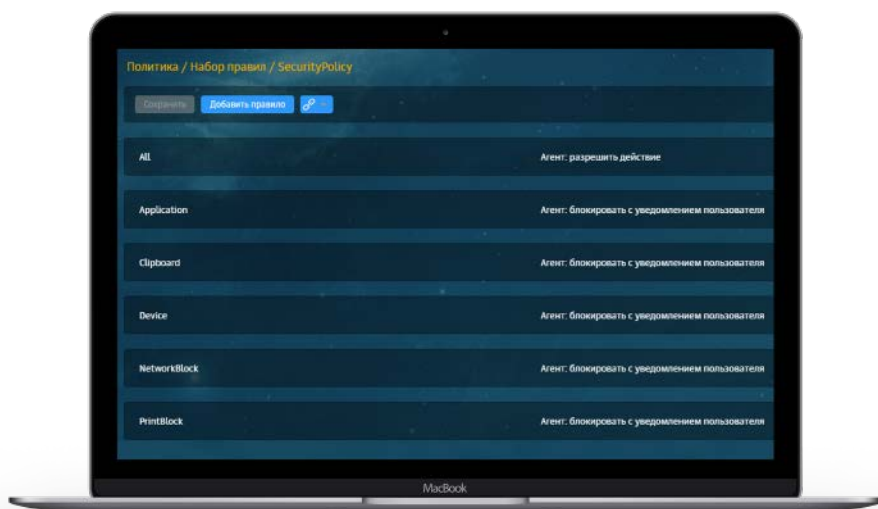


Рисунок 5. Пример набора правил политики безопасности
(эти правила можно применить к группе рабочих станций)

4. Задание ранее созданного набора правил политики безопасности и профиля настроек для группы станций.

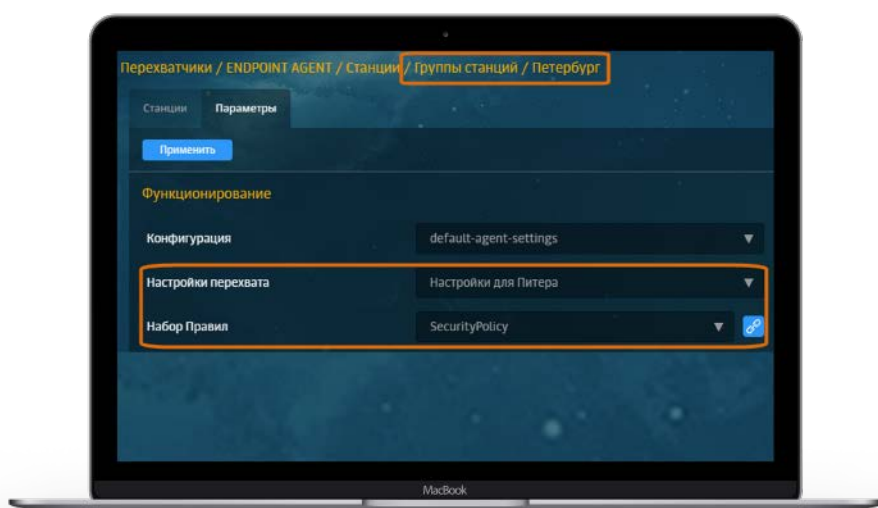
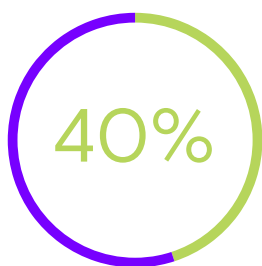


Рисунок 6. Настройки перехвата и набор правил политики безопасности
для группы рабочих станций

Такая организация настройки работы Dozor Endpoint Agent for Linux позволяет, например, задавать отдельные наборы параметров для каждого филиала или подразделения компании.

Примеры использования:

- Запретить сотрудникам отдела бухгалтерии копировать на USB файлы формата ODT, в которых содержатся личные данные сотрудников.
- Разрешить доступ к веб-ресурсу [Консультант](#) + только для сотрудников из юридического отдела [компании](#).
- Запретить отправку сообщения, в котором содержатся персональные данные, с корпоративного ящика на внешний.



всех нарушений политики ИБ
в компаниях происходит
из-за неосмотрительного
использования электронной
почты

40% всех нарушений политики ИБ в компаниях происходит из-за неосмотрительного использования электронной почты (как личной, так и рабочей), по которой пересылается самая разная информация: от рабочих данных до файлов с пометкой «Для служебного пользования» – к такому печальному выводу пришли аналитики «Ростелеком-Солар».

Dozor Endpoint Agent for Linux позволяет специалистам службы безопасности компаний отслеживать и контролировать передаваемые сотрудниками:

- сообщения электронной почты;
- посты, комментарии, личные сообщения в социальных сетях;
- поисковые запросы.

Кроме того, контролируется обмен файлами на веб-ресурсах, включая облачные хранилища Яндекс.Диск и Облако Mail.ru. Например, можно настроить систему так, что при попытке публикации файла, содержащего определенные конфиденциальные данные, операция будет заблокирована, а пользователь рабочей станции получит предупреждение о нарушении политики безопасности компании.

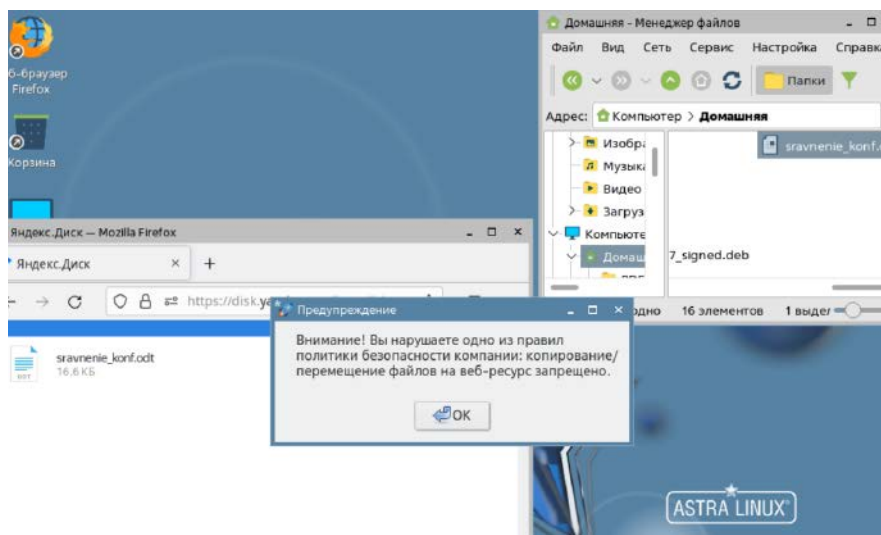


Рисунок 7. Экран рабочей станции сотрудника компании при попытке загрузить файл с конфиденциальными данными на Яндекс.Диск: предупреждение о нарушении правил политики безопасности

Перехваченные агентом данные можно посмотреть в интерфейсе Solar Dozor, в частности, в карточках соответствующих сообщений – там будет информация о канале передачи исходных данных, например, Веб-почта (входящая, исходящая, внутренняя), Веб-запрос, Публикация в интернете.

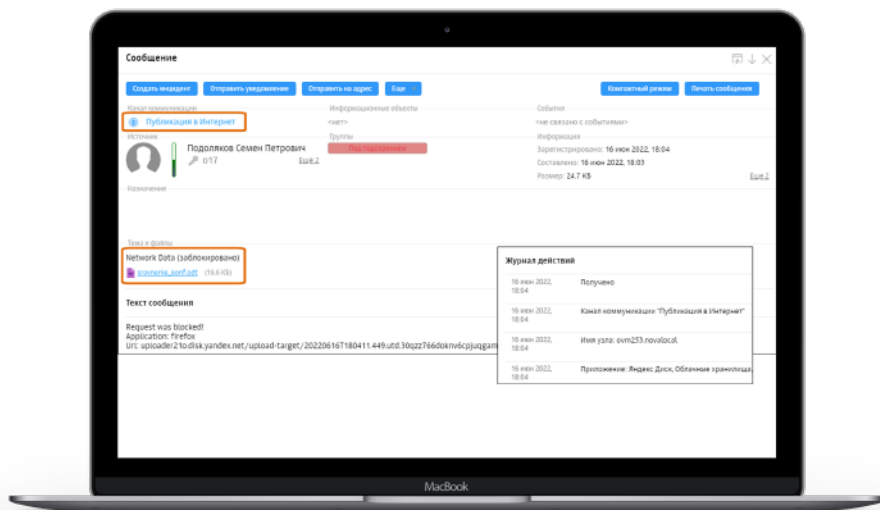


Рисунок 8. Попытка публикации файла с конфиденциальными данными на Яндекс.Диск

Контроль переписки в мессенджерах: перехват сообщений в Telegram и WhatsApp

По данным исследования, проведенного сервисом по поиску работы Superjob, **93% из 1000** опрошенных российских компаний используют мессенджеры для решения рабочих вопросов. При этом используются как общие, так и корпоративные мессенджеры. Общение в мессенджерах вообще стало настолько обыденным, что многие сотрудники с легкостью пересылают информацию, совершенно не задумываясь о том, насколько это корректно и безопасно.



Компания «АльфаСтрахование» в июле 2021 г. проводила опрос, результаты которого показали, что более **60%** россиян отправляют скриншоты с рабочей перепиской в мессенджеры и соцсети.



Информация от экспертов в сфере ИБ также настораживает: минимум **12%** утечек происходит именно через мессенджеры.



Поэтому контроль переписки в мессенджерах – одна из важнейших задач службы безопасности компании. Кроме того, анализируя переписку, можно выявлять задумывающихся об увольнении, нелояльных и/или конфликтных сотрудников.

Dozor Endpoint Agent for Linux перехватывает и передает Solar Dozor сообщения и файлы, которыми обмениваются сотрудники в популярных мессенджерах Telegram и WhatsApp (в случае с Telegram контролируется десктопная и веб-версия, в случае WhatsApp – веб-версия). Офицер безопасности может просматривать переданные агентом данные в интерфейсе Solar Dozor и настраивать политику безопасности с учетом этих данных.

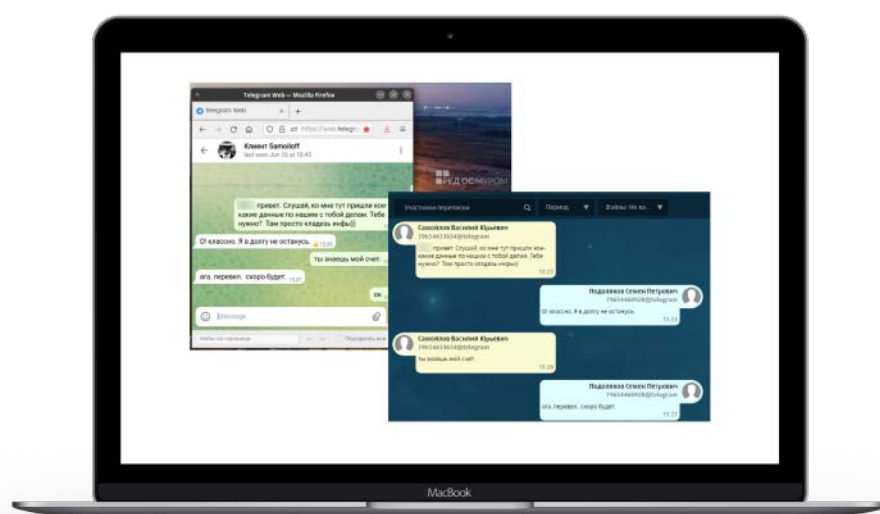
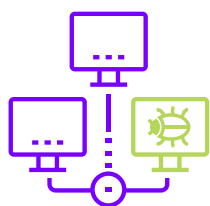


Рисунок 9. Перехват переписки в Telegram: слева экран рабочей станции, где открыта веб-версия мессенджера, справа – та же переписка в интерфейсе Solar Dozor

Контроль съемных устройств



«Агент собирает подробную информацию об устройствах, которые сотрудники пытались подключить»

С модулем Dozor Endpoint Agent for Linux у служб безопасности компаний есть возможность контролировать как подключение различных устройств к рабочим станциям сотрудников, так и операции с подключенными устройствами.

Агент собирает подробную информацию об устройствах, которые сотрудники пытались подключить, в их числе следующие данные:

- Дата и время подключения к рабочей станции.
- Имя узла или IP-адрес рабочей станции, к которой пользователь выполнил подключение устройства.
- Имя пользователя, пытавшегося подключить устройство к рабочей станции.
- Статус – результат попытки подключения устройства.
Возможные значения: Подключено/Заблокировано.

В настройках работы агента можно задать, например, какие экземпляры и/или категории USB-устройств разрешено/запрещено подключать к рабочим станциям, входящим в конкретную группу. Возможна работа с «черным» и «белым» списками устройств, блокировка по типу устройств и/или их идентификаторам.

Кроме того, офицер безопасности может задавать (в том числе по модели или производителю), какие экземпляры и/или категории USB-устройств разрешено/запрещено подключать конкретному сотруднику / группе персон, либо к определенным рабочим станциям, входящим в конкретную группу. Например, так можно запретить подключать к корпоративным компьютерам внешние жесткие диски, оптические приводы, токены и т. п.

Таким образом, можно пресечь утечку информации через флешки и переносные диски, в том числе по протоколу MTP (Media Transfer Protocol).



Рисунок 10. Настройки работы агента, параметры подключения USB-устройств: заданы устройства, которые разрешено/запрещено подключать к рабочим станциям

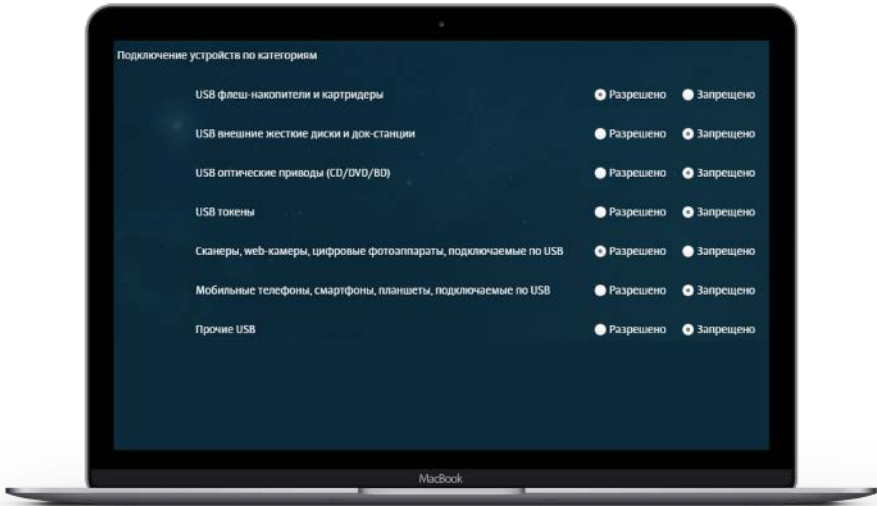


Рисунок 11. Настройки работы агента, параметры подключения устройств по категориям

DLP-система Solar Dozor может заблокировать попытку подключения сотрудником USB-устройства из списка запрещенных .

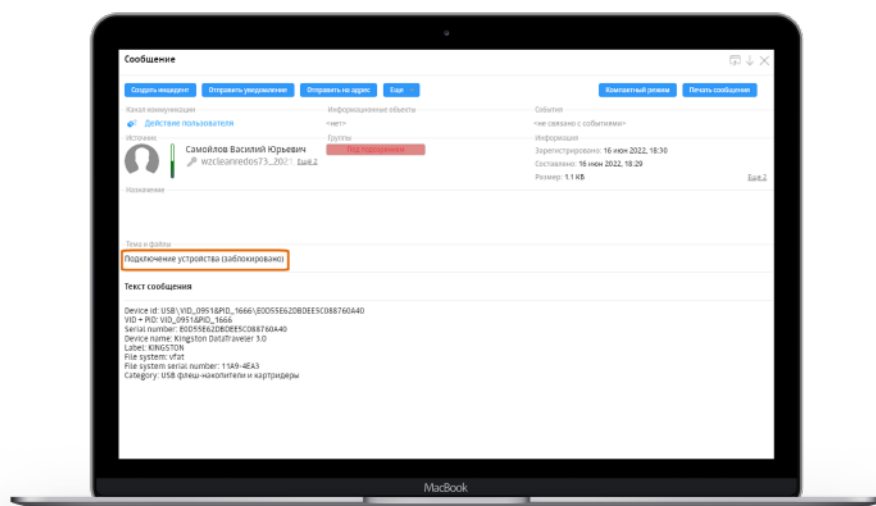


Рисунок 12. Карточка сообщения в Solar Dozor: информация о блокировке устройства

Также можно узнать, какие USB-устройства пытался подключить конкретный сотрудник – эта информация доступна в его карточке в разделе [Устройства](#).

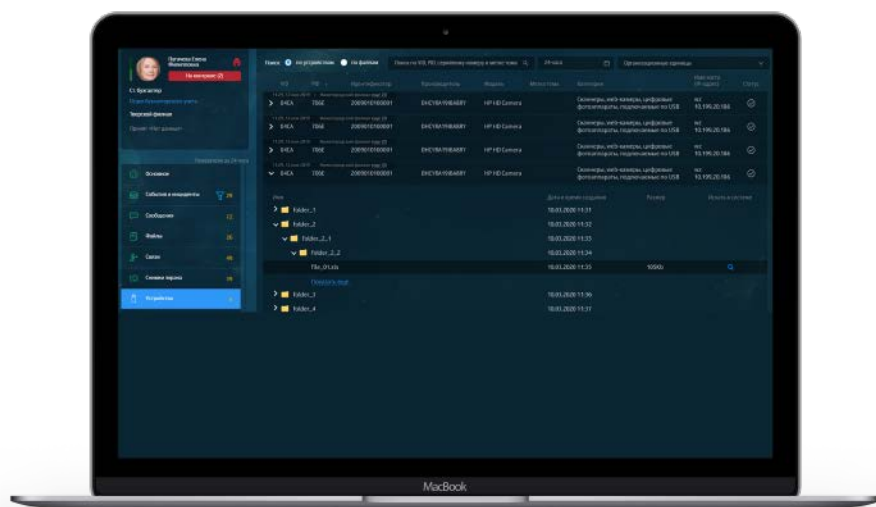


Рисунок 13. Интерфейс Solar Dozor, карточка сотрудника: сведения об устройствах, которые сотрудник пытался подключить к рабочей станции

Кроме того, в интерфейсе Solar Dozor доступно ведение базы экземпляров USB-устройств, которая может быть дополнена как в ручном режиме, так и в автоматическом – с использованием перехваченных агентом данных об устройствах.

При этом USB-устройства автоматически группируются по определенным категориям, которые также могут быть использованы для настройки запрета подключения конкретных устройств.

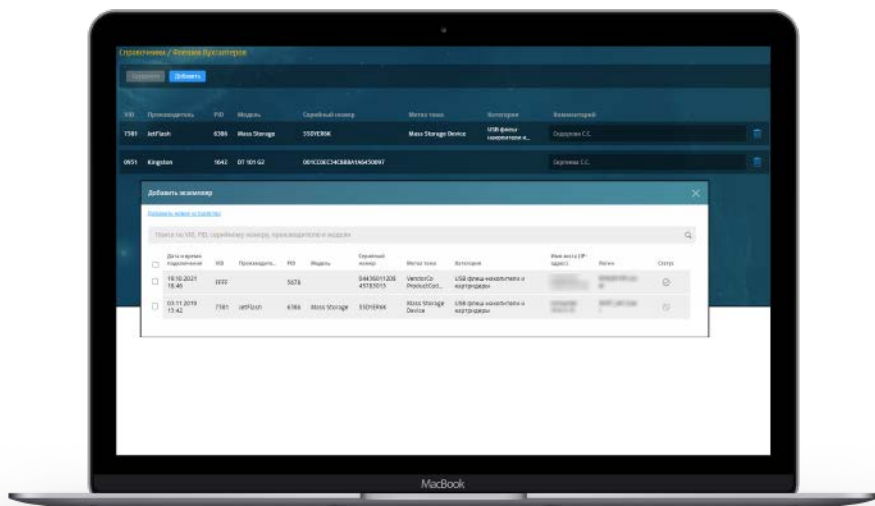


Рисунок 14. Интерфейс Solar Dozor, раздел «Списки устройств»: сведения об устройствах, подключаемых к рабочим станциям в корпоративной сети

Контроль операций с файлами: копирование, перемещение, печать

Давайте представим ситуацию: увольняющийся сотрудник копирует целый архив конфиденциальных документов и/или распечатывает файлы с персональными данными... Увы, такое вполне возможно. Как говорят эксперты ИБ, практически в половине случаев утечек данных виноваты сотрудники компаний.

С помощью Dozor Endpoint Agent for Linux и настроенных правил политики безопасности можно контролировать выполняемые сотрудниками операции с файлами:

- копирование/перемещение файлов, к примеру, на съемные носители. При этом на соответствие политике безопасности проверяется содержимое как самих файлов, так и архивов (TAR, GZIP, ZIP, RAR, 7ZIP, BZIP, TARGZ). Обработываются и самораспаковывающиеся архивы – извлеченные файлы также проверяются;
- печать документов – агент перехватывает и анализирует данные, отправляемые на локальные, сетевые или виртуальные принтеры.

Соответственно, можно запретить группе сотрудников выполнять вышеуказанные операции с файлами, содержащими какие-либо конфиденциальные данные.

Лайфхак: с помощью имеющегося в Solar Dozor версии 7 модуля анализа поведения сотрудников Dozor UBA, данные которому предоставляет в том числе и агент, можно на ранней стадии выявлять сотрудников, еще только думающих об увольнении. Рабочие станции таких сотрудников рекомендуется сразу добавлять в группу, к которой применимы более жесткие, чем для других групп, правила политики безопасности. Таким образом, повышается уровень защиты конфиденциальных данных.



«С помощью Dozor Endpoint Agent for Linux и настроенных правил политики безопасности можно контролировать выполняемые сотрудниками операции с файлами»

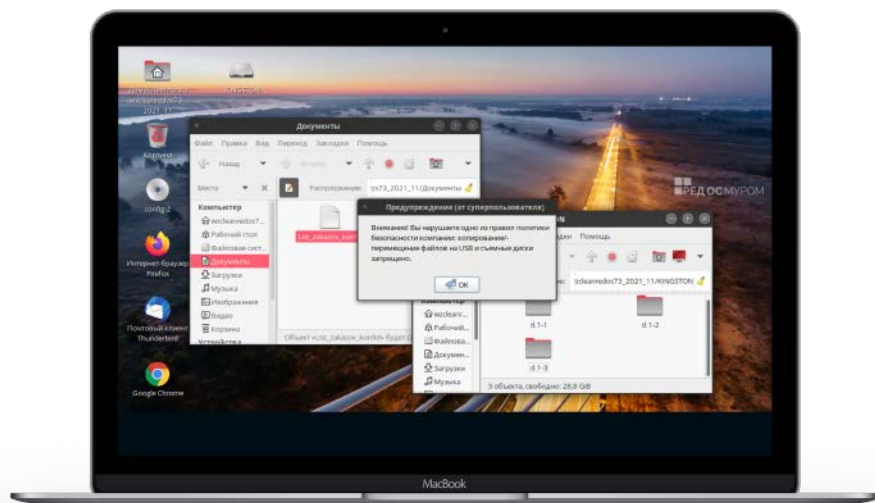


Рисунок 15. Окно оповещения сотрудника о нарушении политики безопасности



«С помощью модуля Dozor UBA можно на ранней стадии выявлять сотрудников, еще только думающих об увольнении»

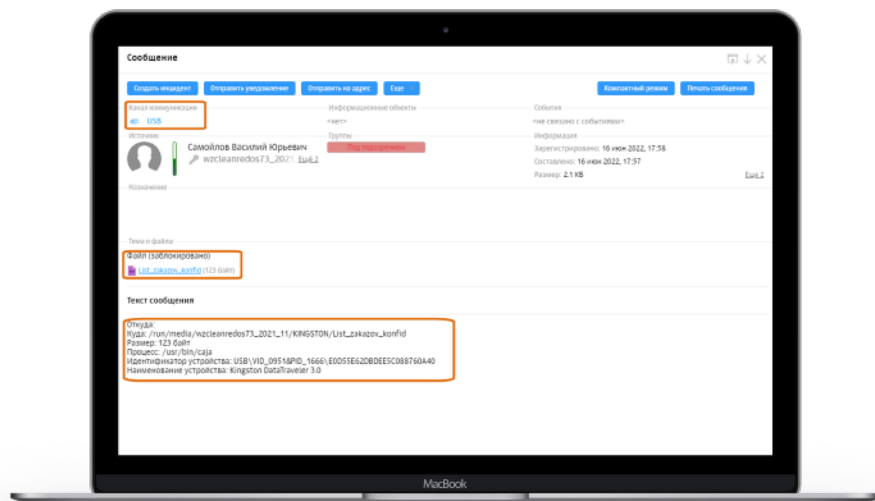


Рисунок 16. Интерфейс Solar Dozor, карточка сообщения: сведения о заблокированной попытке копирования файла с конфиденциальными данными

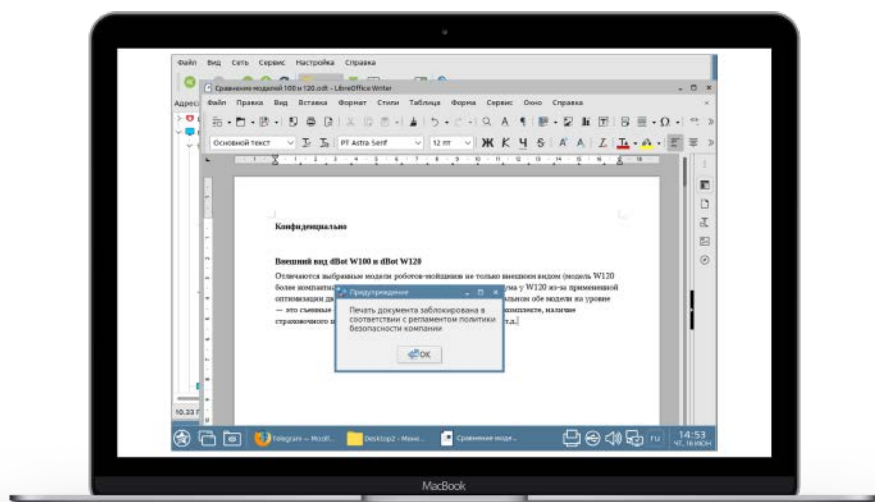


Рисунок 17. Экран рабочей станции сотрудника компании при заблокированной попытке печати файла с конфиденциальными данными: предупреждение о нарушении правил политики безопасности

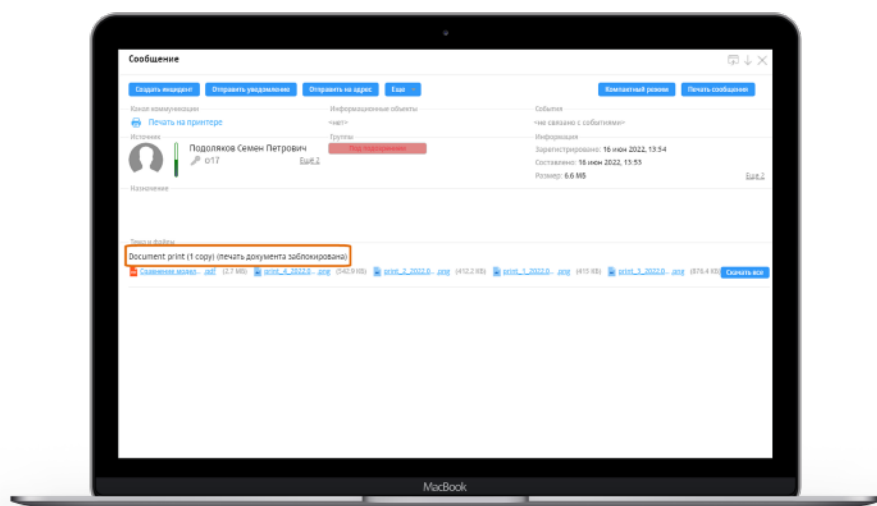
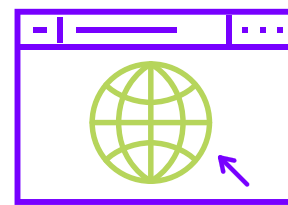


Рисунок 18. Интерфейс Solar Dozor, карточка сообщения: сведения о заблокированной попытке печати файла с конфиденциальными данными

Мониторинг экрана рабочей станции: снятие снимков и видеотрансляция

Один из инструментов мониторинга действий сотрудников на рабочих станциях – снимки экрана рабочей станции. Формирование снимков выполняется [Dozor Endpoint Agent for Linux](#) по заданному событию (по активации окна приложения, по нажатию пользователем клавиши Enter) или через заданный интервал времени.

В Solar Dozor снимки экрана рабочей станции отображаются в карточке сотрудника. В ней также отображается список всех приложений, запущенных в момент формирования снимка. Есть возможность поиска снимков по названию активного приложения.



«Один из инструментов мониторинга действий сотрудников на рабочих станциях – снимки экрана рабочей станции»

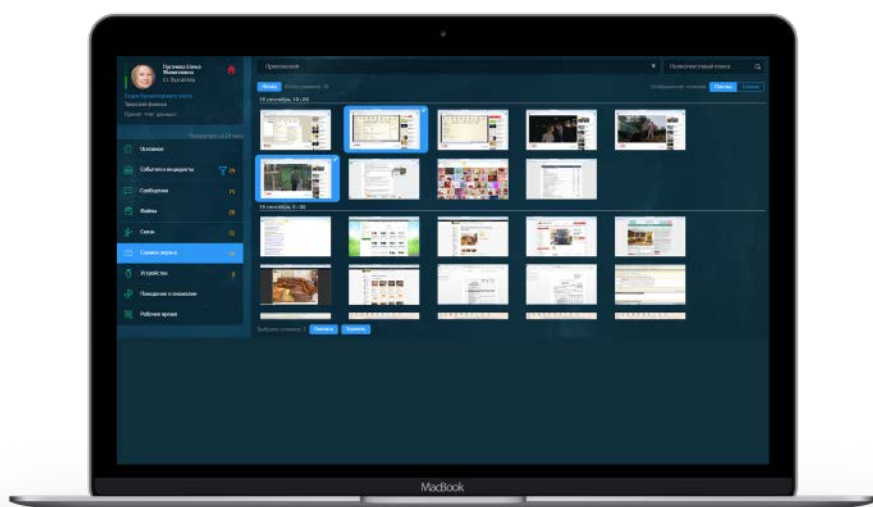


Рисунок 19. Интерфейс Solar Dozor, карточка сотрудника: снимки экрана рабочего компьютера сотрудника

Кроме снимков экрана, в интерфейсе Solar Dozor можно посмотреть видеотрансляцию рабочего стола интересующего сотрудника.

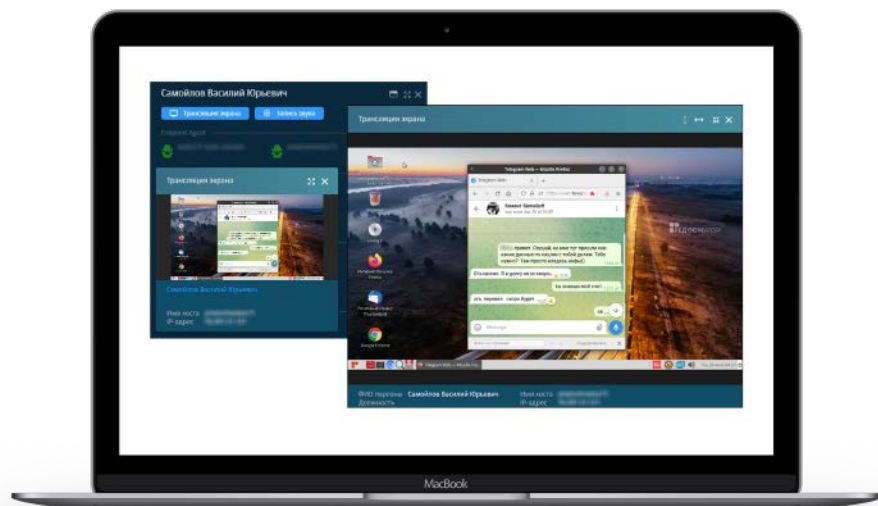


Рисунок 20. Интерфейс Solar Dozor: трансляция видео с экрана рабочего компьютера сотрудника

Если сотрудник использует несколько рабочих станций, можно попеременно просматривать видео с каждой из них. При наличии у сотрудника нескольких мониторов видео отображается со всех. Таким образом, офицер безопасности может в режиме реального времени прицельно контролировать действия сотрудников, а значит – оперативно предотвращать возможные нарушения.

Контроль рабочего времени сотрудника: что, где, когда



«Функция контроля рабочего времени сотрудников позволяет руководству и службе безопасности получать подробные сведения о том, чем занимается сотрудник на рабочем месте»

Функция контроля рабочего времени сотрудников позволяет руководству и службе безопасности оперативно оценить эффективность работы компании в целом по тому, как работники распоряжаются рабочим временем: сколько и на какую деятельность они его тратят и какие веб-ресурсы и приложения используют. Например, можно отследить использование рабочего времени или оборудования в личных целях.

В карточке сотрудника офицер безопасности может просматривать, например:

- суммарные за конкретный день или период сведения о том, сколько времени сотрудник тратит на работу;
- топ-5 категорий приложений, которые использовались сотрудником больше всего (за день или период);
- детальную статистику по использованию персоной рабочего времени – подробные данные о времени, проведенном сотрудником как в приложениях, так и в интернете (за день или за период).

Данные отображаются как в текстовом виде, так и в виде диаграмм, где периоды работы персоны в конкретном приложении представлены как временные отрезки, выделенные определенным цветом.

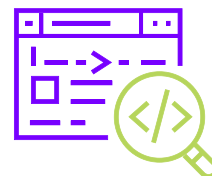


Рисунок 21. Интерфейс Solar Dozor, карточка сотрудника: данные о том, сколько времени и на какую деятельность тратит сотрудник, какие веб-ресурсы и приложения использует на рабочем месте

Функция ориентирована в первую очередь на решение задач безопасности. Например, с ее помощью можно выявлять использование сотрудником нежелательных приложений, оценивать риск утечки информации по активности сотрудника в интернете и т. п.

Dozor Endpoint Agent for Linux в VDI: усиленная защита от утечек данных

VDI (Virtual Desktop Infrastructure) — инфраструктура управления виртуальными рабочими столами пользователей. Эта инфраструктура предполагает, что каждому сотруднику выделяется виртуальная рабочая станция (виртуальная машина, VM) с определенным набором программ, документов и других данных, хранящихся на сервере.



Dozor Endpoint Agent for Linux можно включить в «золотой образ» VDI – корпоративный стандарт рабочей станции пользователя. В этом случае при создании виртуальной машины из образа агент определит, что это новая рабочая станция, которая должна быть зарегистрирована в Solar Dozor в качестве нового объекта (аналогично обычной рабочей станции). После регистрации виртуальной рабочей станции агент выполняет на ней свои функции в полном объеме в течение всего времени жизни виртуальной машины.

«VDI (Virtual Desktop Infrastructure) — инфраструктура управления виртуальными рабочими столами пользователей»

Поскольку в случае организации в компании инфраструктуры управления виртуальными рабочими станциями данные хранятся не на жестком диске компьютера сотрудника, а в дата-центре, который, как правило, защищен лучше, чем персональные рабочие станции, применение VDI уже само по себе препятствует утечке конфиденциальных данных. А с использованием VDI совместно с Dozor Endpoint Agent for Linux уровень защиты данных повышается как минимум в 1,5-2 раза.



«Dozor Endpoint Agent for Linux
поддерживает работу на всех
ведущих отечественных
дистрибутивах ОС Linux»

В настоящее время Dozor Endpoint Agent for Linux уже достиг определенной зрелости и как средство защиты от утечек информации на рабочих станциях является одним из наиболее развитых решений для семейства Linux на отечественном рынке DLP-систем.

Еще раз хотим отметить, что Dozor Endpoint Agent for Linux поддерживает работу на всех ведущих отечественных дистрибутивах ОС Linux, что позволяет российским компаниям успешно контролировать рабочие станции при переводе инфраструктуры на отечественное ПО в рамках импортозамещения.

Несмотря на достаточно зрелый уровень, продукт продолжает активно развиваться и улучшаться. По словам руководителя продукта Юрия Деревнина, в современных условиях качественная DLP-система должна обеспечивать защиту от утечек критичной информации на рабочих станциях сотрудников с учетом максимального контроля всех каналов обмена информацией.

Выводы

Особое внимание мы уделяем обеспечению предотвращения утечек информации на рабочих станциях, функционирующих на отечественных ОС семейства Linux.

В ближайших планах у команды продукта:

- Развертывание Dozor Endpoint Agent for Linux непосредственно из графического интерфейса Solar Dozor. Таким образом, процесс установки, обновления и удаления агентов Windows и Linux будет унифицирован. Это, как минимум, обеспечит удобство при переводе рабочих станций с Windows на Linux.
- Запись звука с микрофона рабочей станции – еще один способ получения данных для доказательной базы при проведении расследований инцидентов ИБ.

Кроме того, будет продолжено расширение блокирующих функций агента при передаче данных по различным каналам. В частности, в скором времени планируется добавить возможность блокирования передачи сообщений и файлов при обмене ими в популярных мессенджерах по результатам анализа данных в соответствии с предварительно заданными правилами политики безопасности.



Автор: Яна Менжевицкая,
аналитик Центра продуктов
Дозор компании
«Ростелеком-Солар»

Какой DLP-агент под macOS может предложить российский рынок

Сегодня в любой достаточно крупной компании или государственном учреждении вряд ли найдется скептик из сотрудников ИБ, который спросит: «А зачем нужен DLP-агент под Mac?» Однако еще несколько лет назад ответ был не столь очевиден. У нас как вендора DLP-системы Solar Dozor также не было однозначного ответа, нужна ли нашим заказчикам эта функциональность, поэтому мы решили провести исследование такой потребности.

Анализ рынка. Кому нужен DLP-агент под macOS?

Сначала мы проанализировали в целом динамику продаж компьютеров Apple в России. Выяснилось, что продажи ноутбуков от Apple в 2015–2020 гг. неуклонно росли, и к середине 2021 года по количеству проданных в РФ моделей MacBook Air и MacBook Pro Apple заняли 5-е место с долей 6%. Также важной вехой в продвижении устройств Apple стали договоренности американского производителя с Минцифры о поддержке российского ПО. В поставляемой в РФ технике вендор предусмотрел возможность развертывания отечественных сервисов Яндекса, Mail.ru, антивируса «Лаборатории Касперского», социального сервиса «Госуслуги» и платежной системы «Мир». Стало понятно, устройства Apple, в частности MacBook, востребованы на российском рынке.

Отдельно отметим, что в марте 2022 года власти США ввели санкции против России, запретив продажи американского ПО и оборудования в страну. Однако уже в апреле США частично сняли ограничения, разрешив поставлять американский софт и технику для коммуникаций граждан в РФ. По мнению экспертов российского ИТ-рынка, послаблением в первую очередь воспользуются Apple, Microsoft и Samsung. Так что задача мониторинга Mac-устройств в российских организациях продолжает оставаться актуальной.

Следующим шагом стало изучение потребностей наших текущих и потенциальных заказчиков в агенте под macOS. Проведенный нами опрос показал, что наибольший интерес к мониторингу действий пользователей на Mac-устройствах проявил финансовый сектор, крупные промышленные компании, предприятия топливной и энергетической промышленности, ИТ и телекоммуникационные компании, крупные ретейлеры, федеральные государственные структуры. Количество пользователей устройств Apple в этих компаниях составляло от 5 до 60%.

Затем мы проанализировали целевые группы сотрудников, использующих в работе устройства Apple. Выяснилось, что чаще всего такими ноутбуками пользуются:

- VIP-сотрудники: руководство компаний, топ-менеджмент;
- ведущие сотрудники ИТ-сектора: разработчики, архитекторы, дизайнеры UI/UX;
- руководители и ведущие сотрудники других направлений: менеджеры среднего звена, эксперты, дизайнеры и т. п.

Очевидно, что все эти группы персон владеют важной, а зачастую критичной для развития бизнеса или контроля государственных интересов информацией. Без включения этих групп в сферу контроля служб информационной и экономической безопасности контроль утечек информации в организации нельзя считать полноценным.



«Чтобы максимально быстро обеспечить заказчиков полнофункциональным macOS-агентом, мы поставили перед собой самые амбициозные цели»

Определяем цели, планируем задачи

Чтобы максимально быстро обеспечить заказчиков полнофункциональным macOS-агентом, мы поставили перед собой самые амбициозные цели. **За первый год** – реализовать DLP-агент, обеспечивающий базовый контроль основных каналов утечки данных, закрывающий первоочередные потребности ключевых заказчиков.

За второй – довести агент до полной функциональности, сопоставимой с флагманом линейки – агентом под Windows. Конечной целью стало создание лучшего на российском рынке агента DLP под macOS.

Решение задачи начали с составления и приоритизации списка функций и формирования дорожной карты развития продукта.

Так сформировался список базового функционала нашего macOS-агента:

- Контроль интернет-трафика (веб-почта, поисковые запросы, облачные сервисы и т. п.).
- Перехват локальной почты (почтовые протоколы SMTP, POP3, IMAP).
- Контроль мессенджеров.
- Контроль печати.
- Контроль подключения USB-устройств.
- Создание снимков экрана.
- Запись ввода с клавиатуры (кейлоггер).
- Контроль данных, передаваемых через буфер обмена.
- Контроль операций копирования файлов на съемные носители и корпоративные сетевые ресурсы.



«Мы заложили в план
дополнительное время
на проработки – проведения
исследований (НИР)
по каждой из ключевых
функций»

Не секрет, что Apple во главу угла ставит безопасность своих ОС и каждый новый релиз приносит новые ограничения, касающиеся безопасности функционирования компонентов операционной системы и работы приложений в ней. Учитывая эти риски, мы заложили в план дополнительное время на проработки – проведения исследований (НИР) по каждой из ключевых функций.

Примеры проведенных нами исследований:

- Доступные решения для контроля трафика на уровне сетевого перехвата (MitM).
- Возможность контроля подключения USB-устройств.
- Способы контроля копирования файлов на съемные носители и сетевые ресурсы (корпоративные файловые каталоги).

В целом следует отметить, что существующие решения задач для Windows и Linux не подходят для macOS-агента, поэтому по результатам НИР потребовалась либо серьезная доработка (в случае с MitM), либо собственное решение задачи с учетом специфики macOS (в случае контроля USB-устройств и контроля копирования файлов).

Разработка первой версии

Начало создания нашего агента совпало с выходом macOS версии 11 (Big Sur), в которой появились существенные ограничения на разработку компонентов ядра. Но при этом Apple сохранил возможность разработки системных расширений (System Extensions), что позволяет создавать приложения для контроля сети, файловых операций, контроля действий с устройствами и т. п.

Благодаря проведенным исследованиям, разработка функционала не выбилась из графика реализации дорожной карты. Первый релиз macOS-агента состоялся в сентябре 2021 года. В него вошел контроль интернет-трафика по всем запланированным для базовой реализации каналам, перехват локальной почты по всем запланированным протоколам и контроль мессенджеров WhatsApp и Skype.

После этого провели демонстрации нового модуля нескольким потенциальным заказчикам. Так мы подтвердили большой интерес рынка к нашей новой разработке.

Настоящим прорывом оказалась возможность контроля интернет-трафика на Mac-устройствах, включая облачные ресурсы, а также контроля мессенджеров: на данный момент ни одно из конкурирующих решений, которых на рынке буквально единицы, такого функционала не предоставляет.

На момент выхода первого релиза macOS-агента уже активно продавались устройства на базе новой архитектуры Apple M1. Первый релиз тестировали еще на старой архитектуре – x64-86, но за время разработки первой версии мы уже подготовили инфраструктуру для поддержки новой платформы.

В последующие два релиза вошли две ключевые функции любого DLP-агента: контроль печати и контроль подключения USB-устройств, и, конечно, мы сделали агент работоспособным на платформе M1.

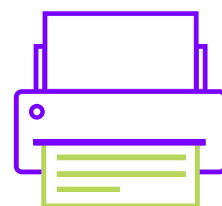
Функция контроля печати позволяет перехватывать факт вывода на печать документа независимо от приложения, из которого пользователь запускает печать. При этом macOS-агент Solar Dozor сохраняет копию содержимого документа и позволяет приобщить ее к отчету о расследовании инцидента.

Но главное, чего нет ни в одном macOS-агенте на российском рынке, – это блокировка печати в случае нарушений правил политики.

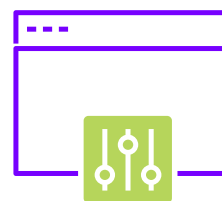
Контроль подключения съемных носителей позволяет собирать данные о подключенных USB-устройствах и гибко управлять доступом к ним: разрешать или блокировать подключение с использованием белых и черных списков устройств по отдельным экземплярам, моделям и производителям. Благодаря этой функции, macOS-агент Solar Dozor стал отличной заменой зарубежным продуктам, стремительно уходящим с нашего рынка.

На этом этапе активно стартовали пилотные проекты, по которым мы получили положительные отзывы, в том числе в сравнении с другими системами. Один из пилотов прошел настолько успешно, что превратился в коммерческое внедрение. Наличие развитого агента для macOS стало для заказчика из банковского сектора одним из ключевых факторов при выборе DLP-системы, поскольку в компании около 60% сотрудников работают на Mac-устройствах. Заказчика впечатлил как уже имеющийся функционал, так и планы по его развитию.

Так Dozor Endpoint Agent для macOS стал флагманом движения российского рынка защиты от утечек к полнофункциональному агенту для мониторинга рабочих мест на базе устройств Apple. В начале 2022 года в нашем агенте была реализована поддержка вышедшей в конце 2021 г. новой, 12-й версии macOS (Monterey). А уже в марте Dozor Endpoint Agent для macOS был зарегистрирован в Реестре отечественного ПО.



«Функция контроля печати позволяет перехватывать факт вывода на печать документа независимо от приложения, из которого пользователь запускает печать»



«Dozor Endpoint Agent для macOS стал флагманом движения российского рынка защиты от утечек к полнофункциональному агенту для мониторинга рабочих мест на базе устройств Apple»



Автор: Юрий Деревнин,
руководитель продукта
Центра продуктов Дозор
компании «Ростелеком-Солар»

Выводы

Как мы отмечали выше, анализ рисков, связанных с возможными проблемами пользователей устройств Apple из-за санкций со стороны правительства США, не привел нас к каким-либо трагическим выводам, а скорее дал возможность сделать взвешенно-оптимистичные прогнозы. Отечественные компании в ближайшей перспективе вряд ли откажутся от использования устройств Apple, и снижения интереса к нашему macOS-агенту не ожидается.

Поэтому в самое ближайшее время в Dozor Endpoint Agent для macOS появятся новые возможности, на которые нам уже поступили многочисленные запросы от заказчиков. Во-первых, это снятие снимков с экрана макбуков сотрудников, которое позволит контролировать действия пользователей на устройстве с сохранением истории для формирования доказательной базы. Во-вторых, это перехват нажатий клавиш на клавиатуре (кейлогер) для контроля вводимой пользователем информации даже в тех приложениях, которые недоступны для мониторинга другими способами.

Как мы разрабатывали функционал записи звука с микрофона для проведения расследований ИБ-инцидентов

Бывают случаи, когда функциональность записи звука с микрофона в DLP-системе становится очень весомым подспорьем для специалиста по безопасности при расследовании различных инцидентов. В этой статье мы собрали яркие примеры успешного использования в расследованиях возможности записи звука с микрофона рабочей станции, а также расскажем, как реализовали эту функциональность в своей DLP-системе, чтобы она приносила максимальную пользу.

Зачем нужна запись звука с микрофона рабочей станции

Прежде чем приступить к разработке новой функции, мы собрали и проанализировали пару десятков сценариев, при которых запись звука с микрофона могла бы помочь в проведении расследований или получении другой важной для компании информации. Расскажу о некоторых из них.

Выявляем нарушителей среди сотрудников, взятых на карандаш либо в случае обнаружения подозрительных действий этих сотрудников в DLP-системе, либо в случае обращения других сотрудников компании в службу безопасности. Рассмотрим на конкретном примере.

В отдел ИБ обратился руководитель одного из подразделений компании. Он сообщил, что его подчиненный начал регулярно уходить из кабинета с ноутбуком в переговорные или на улицу для проведения телефонных разговоров. При этом, если руководитель заходил в помещение, в котором находился сотрудник, тот резко прерывал разговор. Если сотруднику задавались какие-либо вопросы, он начинал нервничать.

Специалист отдела ИБ решил поставить этого работника на особый контроль в DLP-систему. Сотрудника добавили в группу «Под подозрением» и в качестве дополнительной меры контроля настроили запись звука с микрофона рабочей станции через endpoint-агент. Также специалист отдела ИБ попросил руководителя сообщать обо всех случаях подозрительной активности со стороны контролируемого работника.

Однажды руководитель вновь обнаружил, что сотрудник ведет подозрительный разговор по телефону, при этом старается говорить крайне тихо, подбирая очень странные слова, словно «шифруется».



«Сотрудник передавал
на сторону по телефону
конфиденциальную
информацию из базы клиентов»

Руководитель сообщил о произошедшем в отдел ИБ. Безопасник оперативно подключился к прослушиванию записи с микрофона рабочей станции сотрудника и обнаружил, что тот во время разговора продиктовал целый набор имен и цифр. Также безопасник обратил внимание, что, говоря по телефону, сотрудник делал снимки с экрана рабочей станции. Просмотр снимков выявил, что сотрудник снимал скриншоты с базы данных VIP-клиентов компании.

Стало понятно, что сотрудник передавал на сторону по телефону конфиденциальную информацию из базы клиентов. Служба ИБ потребовала от него объяснений. В итоге сотрудник признался в содеянном: слив информации был заказан конкурентами.

В нашей практике было много подобных случаев, когда запись звука с микрофона помогала выявлять нарушителей. Так, по похожему сценарию один из заказчиков выявил сговор сотрудников складских помещений, выносивших продукцию за периметр незаметно для охранных систем. После зафиксированных фактов недостачи на рабочих станциях в помещении стали вести запись звука с микрофонов, которая и помогла выявить нарушителей.

Контролируем сотрудников отдела продаж

Представим компанию, которая разрабатывает ИТ-продукты. В ней есть свой отдел продаж. При выезде к заказчикам сотрудники отдела занимаются демонстрацией продуктов. Руководителю отдела важно понимать, о чем и как говорят сотрудники с потенциальными заказчиками. Например, не предлагают ли приобрести продукт по какой-нибудь «серой» схеме или купить продукт конкурентов, не ругают ли продукт и т. д. Такой контроль будет полезен и для понимания, что и как можно улучшить в плане навыков общения сотрудников с заказчиками, нужно ли подтянуть знания о продаваемом продукте.

«Черный ящик»

Классическая история из телеком-сферы. В техническом блоке есть дежурные смены, которые в случае возникновения аварийной ситуации на оборудовании обязаны по нормативам отреагировать в течение нескольких минут и устранить аварию в строго определенный срок. Но есть сотрудники, которые выдергивают кабель из системы аварийного оповещения и отдыхают. А при разборе полетов инцидент подается как отказ оборудования и оператор предъявляет претензии к производителю.

Для беспристрастного расследования такой ситуации хорошо иметь данные из нескольких объективных источников – с камер видеонаблюдения, с микрофона рабочей станции и ряда других. Запись звука поможет понять, как дежурный смены отреагировал на ситуацию, что говорил, связался ли с нужными специалистами, сделал ли необходимые звонки и т. п. Это, как черный ящик в самолете, – особенно полезно при расследованиях спорных и неоднозначных ситуаций.

Отметим, что оптимальным для такого сценария является функциональность, позволяющая выполнять запись только в те моменты, когда обнаружена человеческая речь (или иной шум). Иными словами, записывать тишину не нужно, чтобы не пришлось прослушивать большое количество пустых записей. Мы у себя в Solar Dozor реализовали запись звука с рабочей станции именно в таком рациональном режиме.



«Запись звука поможет понять, как дежурный смены отреагировал на ситуацию, что говорил, связался ли с нужными специалистами»

Украл ноутбук

Это может случиться абсолютно в любой организации. У сотрудника украл рабочий ноутбук, на котором хранилась конфиденциальная информация компании. Можно использовать запись звука с микрофона, чтобы выяснить, что происходит с ноутбуком, у кого он находится, где, как используется и прочие подробности. Установленный на ноутбуке агент DLP-системы при подключении машины к сети будет вести запись разговора злоумышленника и отправлять ее на сервер DLP-системы компании.

Как мы разрабатывали функцию записи звука с микрофона

А теперь поговорим о том, как мы реализовали функцию записи звука с микрофона так, чтобы она оптимально решала описанные задачи.

Часть первая. Аналитическая проработка

Прежде чем приступить к разработке этой функции, мы проанализировали полученные запросы на доработку от наших действующих и потенциальных заказчиков. В результате у нас получился весьма внушительных размеров список требований и пожеланий. На реализацию всего перечня ушли бы годы, поэтому мы приоритизировали требования и сначала решили реализовать то, что необходимо для решения ключевых задач. А именно:

- прослушивание записей прямо в интерфейсе DLP-системы,
- скачивание и удаление записей,
- просмотр снимков экрана, которые были сделаны во время записи звука,
- отображение записей за определенный промежуток времени (фильтр) и ряд других.

Стоит упомянуть, что перед нами был непростой выбор – сделать в первую очередь запись или трансляцию звука. Запрос был и на то, и на другое, но мы все же выбрали функцию записи. Как мы в итоге вышли из этой непростой ситуации – расскажу ниже.

В конце аналитического этапа мы получили концепцию, которая была согласована с архитекторами, владельцами продуктов и самое главное – со стейкхолдерами.

Часть вторая. PBR

После определения основного перечня функций и согласования концепции начался процесс под названием PBR. На этой стадии мы презентовали концепцию командам разработчиков и составили так называемый [Example Mapping](#). Иными словами, мы обсудили, как именно будем реализовывать данную функциональность. Разбили все на истории.

Так мы сформировали окончательные требования для функционала, подготовили все необходимые макеты, у всех участников процесса разработки появилось понимание всех особенностей фичи.

В случае с записью звука данный этап был весьма небыстрым. Наша DLP-система обладает очень обширными функциональными возможностями и особенностями. Пришлось многое проработать и учесть влияние изменений на уже имеющиеся в продукте функции. Ну и, конечно, на стороне endpoint-агента, который мы активно развиваем, необходимо было реализовать значительную часть доработок.

В итоге, благодаря слаженной коллективной работе, задача была решена, а все сформированные истории получили заветный статус «Ready for Development» (готов к разработке).

Часть третья. Разработка

Несмотря на то что на этапе PBR мы все подробно разобрали, в процессе разработки все же встречались моменты, которые мы упустили из виду.

Важно, что такие моменты вовремя подсвечивались и благодаря оперативным дополнительным обсуждениям все вопросы закрывались в кратчайшие сроки. В этом прелесть гибкой разработки.

При возникновении спорных ситуаций мы иногда подключаем наших заказчиков как основных выгодоприобретателей от будущей функциональности. Надо сказать, что это постоянная практика в нашем процессе разработки новых функций, которая позволяет нам не реализовывать лишние и одновременно не упустить важные для заказчика возможности.

В процессе создания функции записи звука с микрофона разработчики также увидели, какие возможности основного продукта можно дополнительно улучшить, а где можно оптимизировать код. То есть разработка дополнительной фичи принесла существенную пользу и основному продукту.

Что в итоге получили заказчики

Итак, какими возможностями записи звука с микрофона в Solar Dozor теперь может пользоваться офицер ИБ. Запись звука запускается в пару кликов: нашли нужную персону, открыли карточку и нажали кнопку «Запись звука».

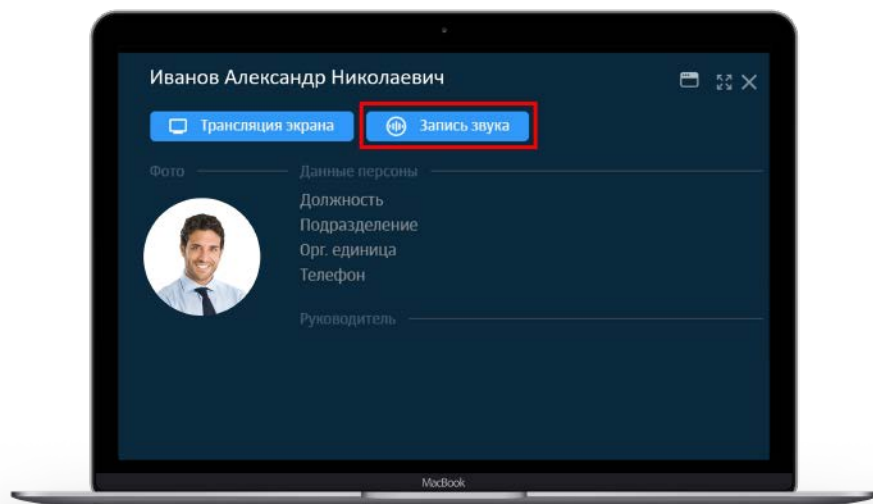


Рисунок 1. Запись звука в карточке персоны

Для прослушивания записей пользователю Solar Dozor нужно перейти в раздел «Записи с микрофона».

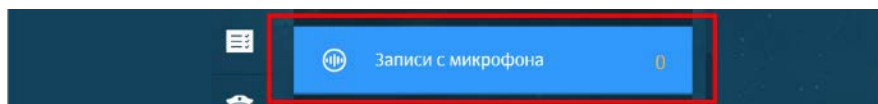
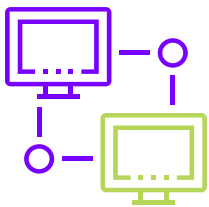


Рисунок 2. Раздел «Запись с микрофона»



«При наличии
у контролируемого сотрудника
нескольких рабочих станций
можно выбрать нужную
станцию для записи»

При наличии у контролируемого сотрудника нескольких рабочих станций можно выбрать нужную станцию для записи. Управление записью выполняется в специально предназначенном для этого окне.

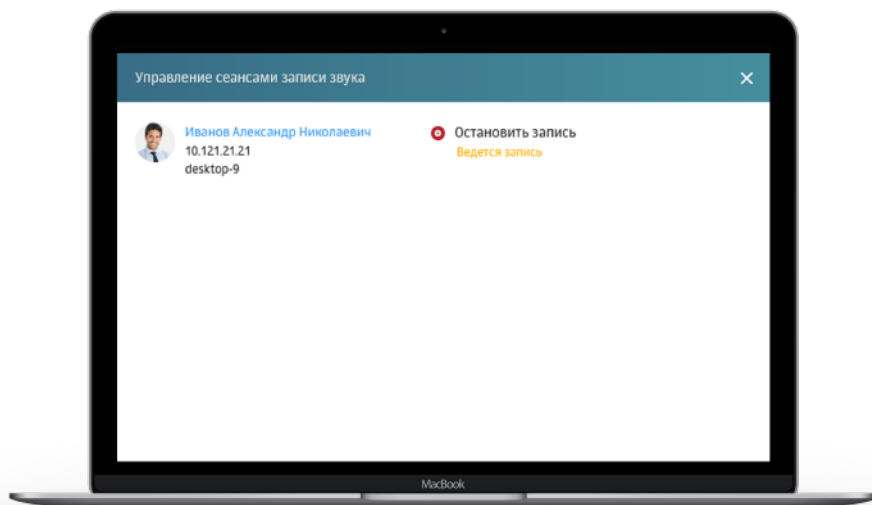


Рисунок 3. Управление сеансами записи звука

Окно открывается при нажатии на специальный значок в верхней части интерфейса системы. В данном окне выводится вся необходимая информация о процессе записи.



Рисунок 4. Значок управления функционалом звука

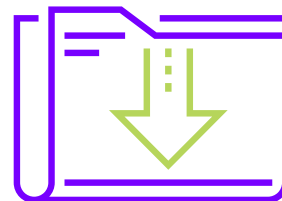
В процессе использования функции может возникать множество сценариев использования. Например, у записываемой персоны может оказаться выключен микрофон, или станция может быть отключена от сети. Подобные ситуации учтены, и в каждом отдельно взятом случае выполняется определенное действие со стороны системы: например, запись приостанавливается, если вокруг рабочей станции тишина.

Для всех таких случаев предусмотрен вывод соответствующих статусов и уведомлений, понятных пользователю.



Рисунок 5. Уведомления для пользователей

Прослушивать записи можно непосредственно в интерфейсе системы, но, если нужно, пользователь всегда может их скачать и прослушать любым удобным для себя способом.



«Прослушивать записи можно в интерфейсе системы, но, если нужно, пользователь может их скачать и прослушать любым удобным для себя способом»

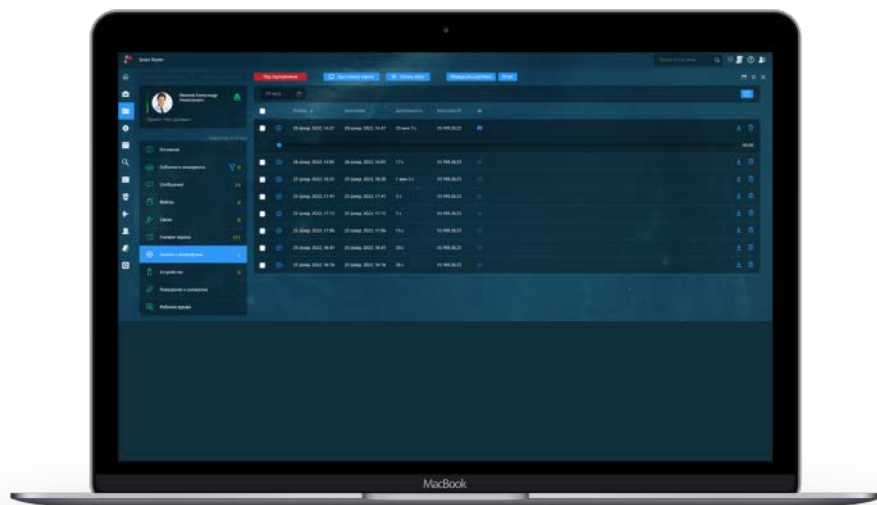


Рисунок 6. Функционал прослушивания и скачивания записей

Также в интерфейсе можно отобразить нужные аудиозаписи, воспользовавшись фильтром: за сегодняшний день, за вчерашний, за неделю.

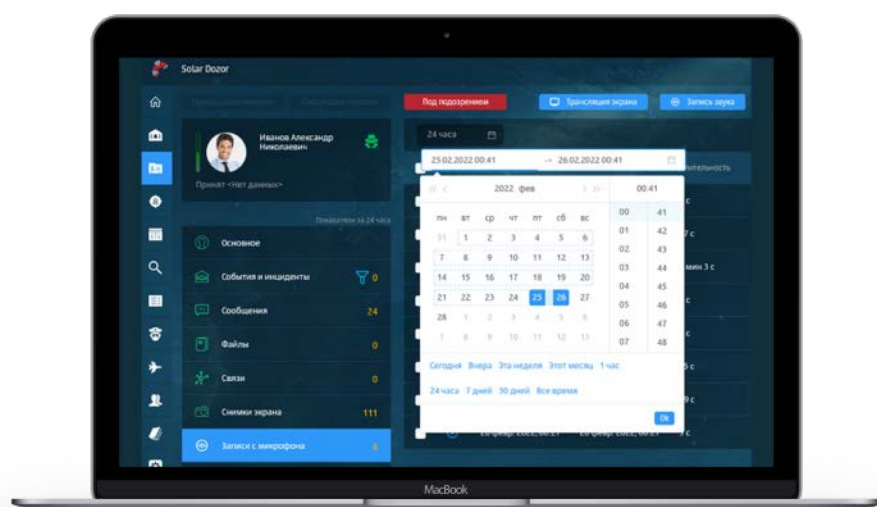


Рисунок 7. Выбор даты прослушивания записей

Для каждой аудиозаписи отображается следующая информация:

- индикатор воспроизведения аудиозаписи;
- дата и время начала и окончания записи;
- длительность записи;
- информация о рабочей станции;
- индикатор наличия снимков экрана, которые были сделаны в период формирования аудиозаписи;
- время воспроизведения (для прослушиваемой аудиозаписи).



«Можно дать пользователю DLP-системы права на запись и/или прослушивание записей конкретных сотрудников или групп сотрудников»

Для удобства работы с аудиозаписями можно их отсортировать по времени старта. Аудиозаписи помимо скачивания и прослушивания можно также и удалять, выбрав одну или сразу несколько записей.

В целях соблюдения дополнительных мер безопасности заказчику может быть необходимо разграничение доступа к функции записи звука, а также к прослушиванию аудиозаписей. При необходимости можно дать пользователю DLP-системы права на запись и/или прослушивание записей конкретных сотрудников или групп сотрудников.

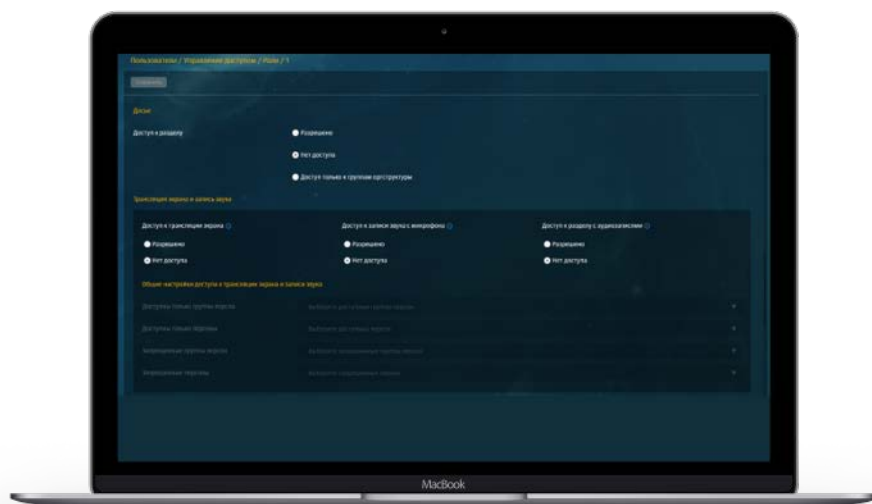


Рисунок 8. Управление доступом к записям

Пользователям Solar Dozor доступна настройка ротации хранилища аудиозаписей и срока хранения медиаинформации. Механизм ротации защищает хранилище аудиозаписей от переполнения. Можно задать автоматическое удаление старых записей для новых. Также можно перемещать записи на локальный носитель или FTP-сервер. Поэтому разработчики системы могут самостоятельно задавать режим и периодичность ротации.

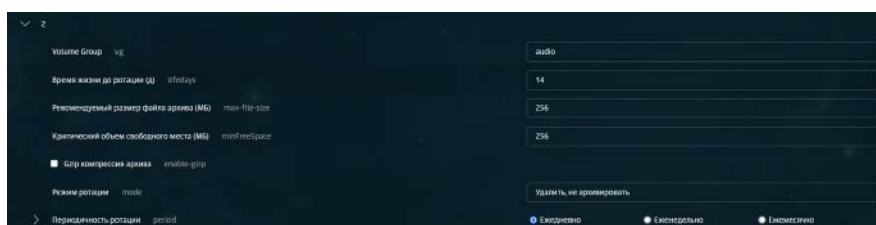
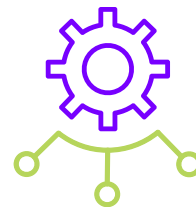


Рисунок 9. Периодичность ротации



Рисунок 10. Срок хранения аудиозаписей

Как уже видно из сказанного выше, мы реализовали развитый механизм настройки функции записи звука с рабочей станции. Так, например, можно задать максимальную длительность записи и длительность тишины для приостановки записи (эта возможность позволяет нашим заказчикам самим выбирать, через какое время после «наступления тишины» необходимо приостанавливать запись звука).



«Мы реализовали развитый механизм настройки функции записи звука с рабочей станции»

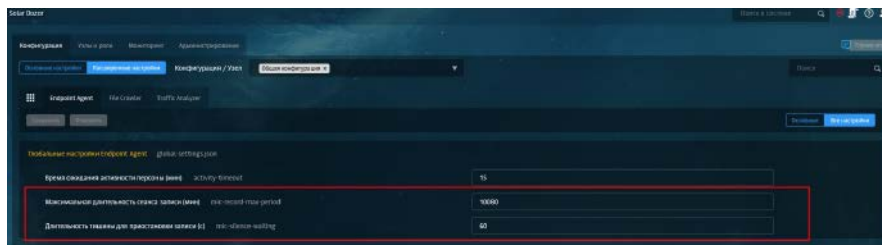


Рисунок 11. Настройка длительности записи и тишины

И самое главное – функция записи реализована таким образом, что после запуска буквально через пару минут в интерфейсе Solar Dozor можно начать прослушивание происходящего «на той стороне». Это возможно благодаря тому, что каждую минуту endpoint-агент присылает порции записей, а затем в интерфейсе Solar Dozor все части объединяются в единую аудиозапись. Так заказчик получает и запись, и практически онлайн-трансляцию звука с микрофона «в одном флаконе». Именно так мы изящно решили непростую задачу одновременной реализации двух механизмов, равно приоритетных для заказчика.



Автор: Михаил Моисеев,
старший аналитик Центра
продуктов Дозор компании
«Ростелеком–Солар»

Выводы

Сама по себе запись звука с микрофона рабочей станции сотрудника – это не что-то уникальное. Многие современные DLP-системы имеют эту функцию. Но что действительно важно, так это качество ее реализации, широта возможностей и масштаб решаемых с ее помощью задач.

Функция записи с микрофона рабочей станции в Solar Dozor, дополняя другие инструменты расследования, позволяет заказчику оперативно подтверждать или опровергать факты нарушений в организации. Очень важной для оперативных расследований является возможность получить запись звука именно в нужный момент и очень быстро, фактически в реальном времени. Это особенно значимо, когда есть информация о подозрительном поведении сотрудника или когда нарушение уже выявлено и необходимо собрать доказательства. А для проведения глубокого комплексного расследования функция поможет дополнить информацию, полученную из других источников.

Запись звука с микрофона рабочей станции полезна для выявления участников различных незаконных схем. Например, при анализе общения сотрудника компании с партнерами и клиентами.

А для руководителей это еще и помощь в анализе поведения ключевых сотрудников при принятии решения об их назначении на важные проекты.

Кроме того, функция является большим подспорьем в принятии предупредительных мер для профилактики различных нарушений.

Данные нуждаются в прикрытии: чем опасны неконтролируемые файловые хранилища

Темой защиты данных в покое в 2022 году сложно кого-то удивить. Напомним, данные в состоянии покоя – это информация, которая хранится в любой цифровой форме (в файловых, облачных хранилищах, в базе данных, на рабочих станциях сотрудников и др.). Несмотря на то что тема далеко не новая, до сих пор встречается много организаций с проблемами и «дырами» в обеспечении безопасности данных в покое. При этом наш опыт внедрения и проведения пилотных проектов по DLP за последние 3 года показывает: в первую очередь организации обеспечивают контроль и защиту данных в движении, защищают каналы передачи информации – почту, мессенджеры, USB и съемные носители и др.

О защите данных в покое порой не задумываются вообще. И это понятно: если обратиться к статистике по утечкам, то в лидерах оказываются именно каналы передачи информации. Например, по данным «РТК-Солар» за апрель–май 2022 г., лидирующую позицию по каналу реализации мошеннических схем занимают мессенджеры.



«В первую очередь организации обеспечивают контроль и защиту данных в движении, защищают каналы передачи информации – почту, мессенджеры, USB и съемные носители и др.»

- Мессенджеры
- Флешки и другие съемные носители
- Облачные хранилища
- Личная почта
- Корпоративная электронная почта
- Мобильная связь
- Сговор
- Подкуп ИТ-специалиста
- Весь набор каналов, включая публикации в научных журналах

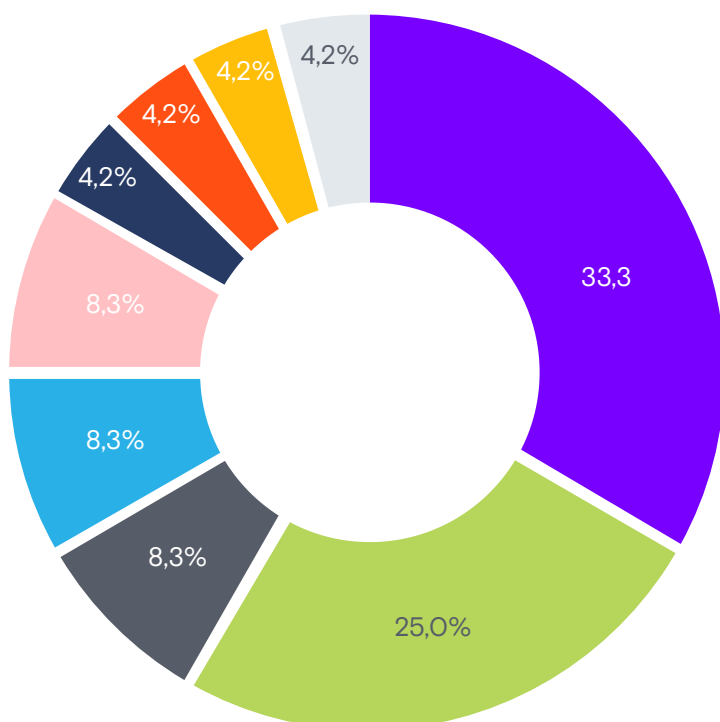
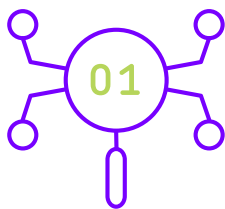


Рисунок 1. Наиболее частые каналы реализации мошеннических схем



«Первоисточником утечки являются данные в покое, – все начинается с них!»

Глядя на диаграмму выше, можно подумать, что проблемы безопасности данных в покое отсутствуют, но это не так.

Данные до попадания в каналы передачи (то есть прежде, чем стать данными в движении) были откуда-то взяты, где-то хранились, в месте, где может произойти нарушение, – в файловых хранилищах или на рабочих станциях сотрудников. Причем размер утекающей информации часто не имеет для нарушителя значения. За последний год мы часто наблюдали публикации в СМИ о различных базах данных, утекших в интернет с вроде бы защищенных ресурсов.

То есть получается, что первоисточником утечки являются данные в покое, – все начинается с них!

Превращение файловых хранилищ в файловые помойки

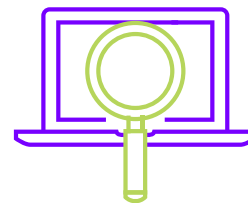
Примерно в 70% организаций файловые хранилища находятся в беспорядочном состоянии. Как правило, когда хранилище только создано, в первые 2 года его существования все им активно пользуются, в нем поддерживается порядок, все прекрасно. Но через пару лет хранилище постепенно захламляется, особенно это характерно для организаций с высокой текучкой кадров. Приходят новые сотрудники, никто не хочет разбираться в структуре хранения информации, которую создали предшествующие коллеги, а уж тем более наводить там порядок. Ведь гораздо проще и быстрее создать новую папку отдела и туда начать складирование. Вот так и появляется куча дублирующей и неактуальной информации, которая раздувает файловое корпоративное хранилище.

И все бы ничего (ну подумаешь, помойка, просто неоптимальное использование корпоративных ресурсов), но с точки зрения безопасности данных файловая помойка — лакомый кусок для инсайдера. Случайно затерявшаяся в огромном «муравейнике» данных конфиденциальная информация может быть легко скопирована и передана третьим лицам.

Сотрудники игнорируют правила хранения конфиденциальной информации

Пренебрежение правилами обращения с конфиденциальной информацией наблюдается в организациях, которые внедрили правила хранения недавно (менее полугода назад). Культура соблюдения правил хранения конфиденциальных данных в компании еще не сформировалась, и поэтому ввод новых правил часто воспринимается сотрудниками в штыки и вызывает внутренний протест, поэтому уже на этапе внедрения правил важно обеспечить контроль их соблюдения.

Он должен сразу включать в себя как постоянный мониторинг всех мест хранения информации, так и работу с выявленными нарушителями. Автоматизированный контроль мест хранения с помощью модуля в DLP-системе Solar Dozor – **Dozor File Crawler** – позволяет проверять как файловые корпоративные хранилища, так и рабочие места сотрудников (ПК, ноутбуки). Также в случае игнорирования сотрудниками правил хранения бывает недостаточно просто осуществлять мониторинг, поскольку нужно оперативно противодействовать нарушению. Для этого рекомендуется воспользоваться функцией «Активный краулер», с помощью которой файлы, хранящиеся с нарушением правил обращения с конфиденциальной информацией, будут автоматически изъяты и перемещены в карантин (специальное файловое хранилище, путь к которому укажет пользователь DLP-системы).



«Dozor File Crawler позволяет проверять как файловые корпоративные хранилища, так и рабочие места сотрудников (ПК, ноутбуки)»

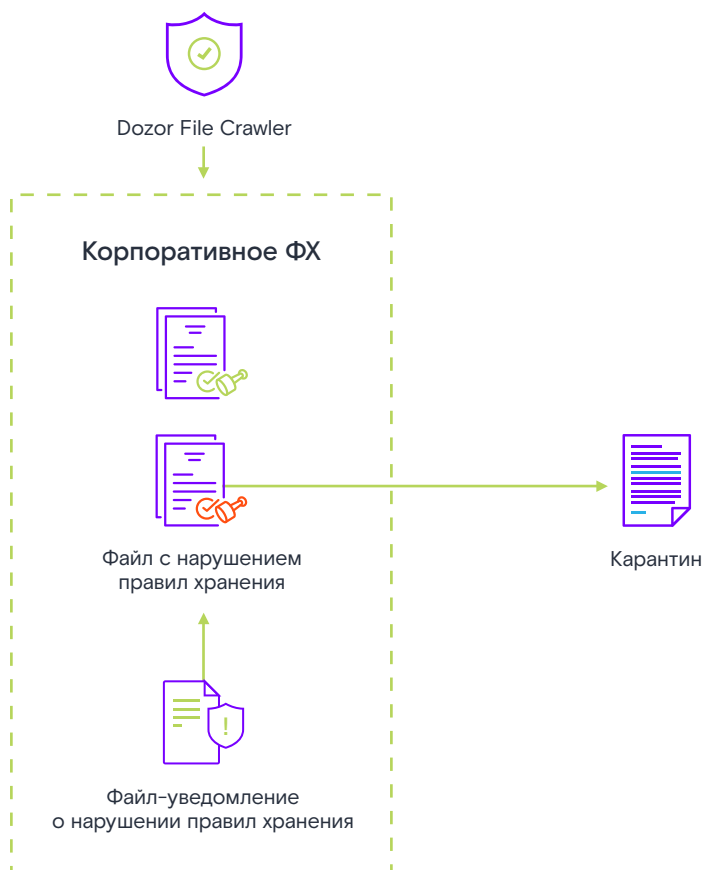


Рисунок 2. Схема работы функции «Активный краулер»

Чтобы предотвратить возможную панику у сотрудника-нарушителя (звонки в ИТ-службу с вопросом «Куда делся мой файл?»), предусмотрена функция автоматической замены изъятого файла одноименным файлом-заглушкой, содержащим информационное уведомление о причинах изъятия файла и необходимых действиях сотрудника для восстановления к нему доступа (текст настраиваемый, пример уведомления от одного из заказчиков представлен ниже).

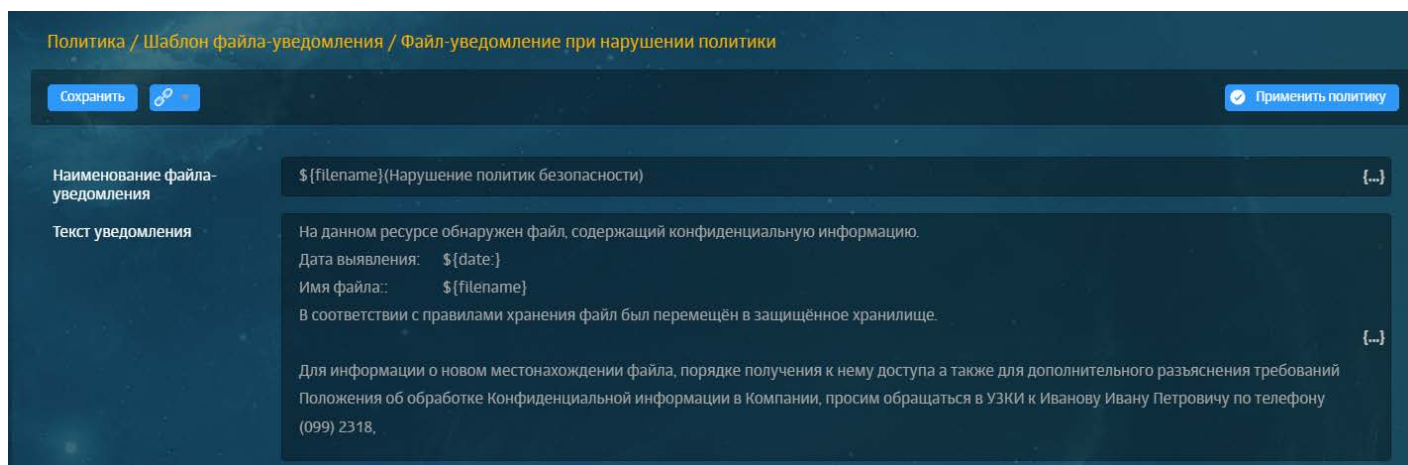


Рисунок 3. Пример настройки текста уведомления в DLP Dozor

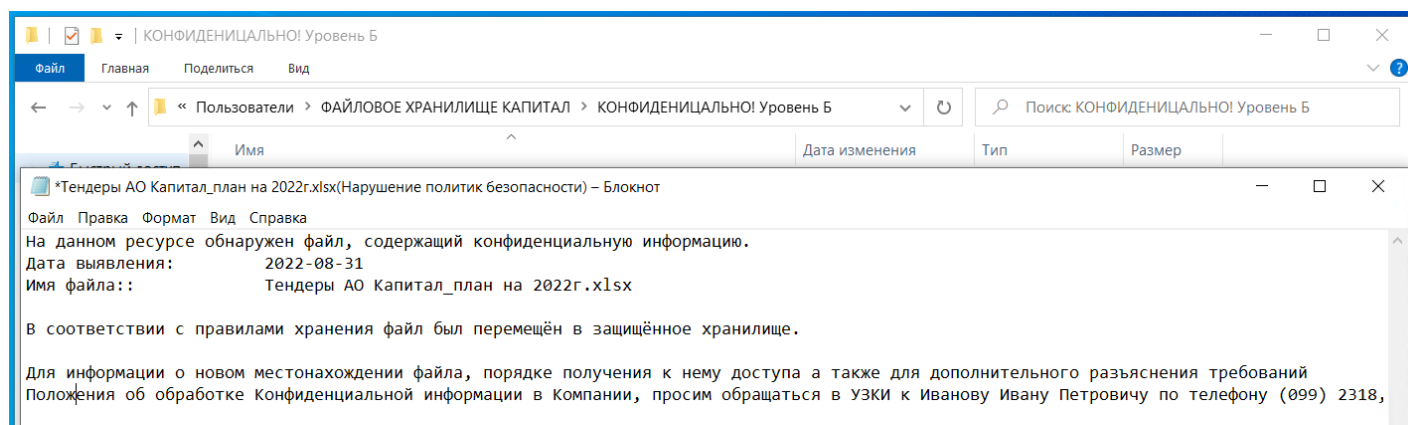


Рисунок 4. Пример отображения текста-уведомления в файловом хранилище, откуда был изъят файл в связи с нарушением правил хранения

Сотрудники не осведомлены, где какую информацию можно хранить

Эта проблема встречалась:

- в организациях, у которых правила хранения и классификации конфиденциальной информации недостаточно конкретизированы;
- в крупных компаниях (количество сотрудников превышает 5000 человек), в которых правила были доведены не до всех сотрудников должным образом либо до некоторых сотрудников/подразделений вообще не доведены.

Ошибочно полагать, что для соблюдения сотрудниками правил хранения достаточно лишь ознакомить с ними работников. Зачастую правила доводятся формально, путем информационной рассылки персоналу и сбора подписей о том, что сотрудники с правилами ознакомились и их принимают. Практика показывает, что больше 60% работников не читают рассылки, подписываются под правилами не глядя. Причина банальна: сильная загруженность, огромный поток информации в течение дня, – тут уж не до вычитки кучи нормативных актов.

Пример. Вот реальный случай у одного из наших заказчиков, демонстрирующий, к чему привело незнание сотрудником правил хранения информации. Иванов Михаил (все имена вымышленные, а совпадения – случайные) из отдела закупки одного из электроэнергетических предприятий уходил в отпуск.

Он и все его коллеги из отдела работали с системой электронного документооборота (ЭДО), в их задачи входило согласование конкурсных технических заданий на закупку. За неделю до отпуска Михаил доделывал все нереализованное за предыдущий квартал.

Наступил вечер последнего рабочего дня перед отпуском, и тут Михаил вспоминает, что забыл оформить замещение и как полагается передать дела. Чтобы не нарушить критичный бизнес-процесс и не подставить весь отдел закупки (несвоевременное согласование ТЗ на закупку может лишить квартальной премии весь отдел), Михаил создал текстовый файл с логином и паролем от своей учетной записи в системе ЭДО.

Он припомнил, что недавно вроде бы приходила какая-то рассылка с правилами хранения информации в корпоративном файловом хранилище. Но вспомнить, где лежат эти правила, не смог. Михаил был твердо уверен, что эти правила не касались папки их отдела (ведь папка создана специально для отдела закупки и никакое другое подразделение к ней доступа не имеет), выложил файл с учетными данными и приложил к нему электронную записку с просьбой к коллегам на время его отсутствия отслеживать статус согласования ТЗ.

По возвращении из отпуска сотрудника ожидала неприятность. Оказалось, что один из коллег переписал на бумагу учетные данные и передал их другому коллеге, Николаю – автору ТЗ, которое Михаил должен был согласовать. Николай увольнялся, и ему нужно было срочно согласовать ТЗ, чтобы получить заслуженную премию. Пока Михаил отдыхал, Николай за него согласовал ТЗ. Документ содержал ошибки и не мог быть согласован. При разборе инцидента Михаил утверждал, что не виноват, так как был в отпуске, а правил хранения не знал.

Что показывает этот пример? Недостаточно просто опубликовать правила ИБ, необходимо еще получать обратную связь, подтверждающую понимание сотрудниками доведенных до них правил. Мы рекомендуем проводить контрольные проверки, интерактивы (периодически давать задания, в которых сотрудник будет распределять файлы по местам хранения), проводить мониторинг всех мест хранения. С помощью File Crawler (модуля DLP-системы Solar Dozor) можно не только выявить само нарушение, но и определить нарушителя (система автоматически определяет, кто выложил файл в неположенное место) с целью обучения правилам хранения.



«С помощью File Crawler (модуля DLP-системы Solar Dozor) можно не только выявить само нарушение, но и определить нарушителя»



«В результате инвентаризации Dozor File Crawler автоматически сформирует полную карту сети компании»

Наверняка вам знакомы ситуации, когда файловые ресурсы появлялись в компании бесконтрольно и без ведома сотрудников ИБ.

Для решения этой проблемы можно использовать Dozor File Crawler. Функция инвентаризации ресурсов корпоративной сети позволяет выявить слабые и серые места в корпоративной сети компании: все неучтенные файловые хранилища, сетевое оборудование (принтеры, сканеры, и др.), рабочие станции, СУБД и другое теневое оборудование. В результате инвентаризации Dozor File Crawler автоматически сформирует полную карту сети компании для просмотра пользователем в DLP-системе.

Человеческий фактор

Все вышеперечисленные проблемы являются управляемыми и решаются с помощью грамотного внедрения правил хранения информации и обеспечения автоматизированной защиты данных в покое. Но есть отдельная категория проблем, которую принято называть «человеческий фактор».

Пример. В одной крупной строительной компании (тоже наш заказчик) установлен порядок хранения и обработки информации под грифом «Коммерческая тайна». По правилам данная информация должна храниться только в специальном файловом хранилище; для документов с коммерческой тайной – назовем их документами категории А. Это самая ценная категория информации в компании, стоимость ущерба в случае ее утечки измеряется десятками миллионов рублей. Также есть еще одна категория информации «Персональные данные», которая должна храниться в другом файловом хранилище, пусть она будет называться информацией категории Б. К файловому хранилищу для документов категории А доступ имеет только 2 сотрудника, Саша и Юра. К файловому хранилищу для данных категории Б доступ имеет больше сотрудников: Миша, Света, Катя и Саша (последний также имеет доступ к информации категории А).

В процессе создания документы еще не являются конфиденциальными и могут храниться в общедоступном файловом хранилище или на рабочей станции сотрудника, который их готовит.

Но часто бывает, что в процессе подготовки в документ добавляется информация, составляющая коммерческую тайну. В таком случае по правилам хранения документу присваивается гриф, производится его регистрация и ответственный за документ сотрудник обязан переместить его в специализированное файловое хранилище с ограниченным доступом.

Как мы видим, в компании есть классификация конфиденциальной информации, установлены правила ее хранения, сотрудники не игнорируют эти правила, они осведомлены, где что должно храниться. Ни одна из проблем, перечисленных выше, не проявилась. Можно считать, что трудностей с защитой данных в покое у компании нет. Однако...

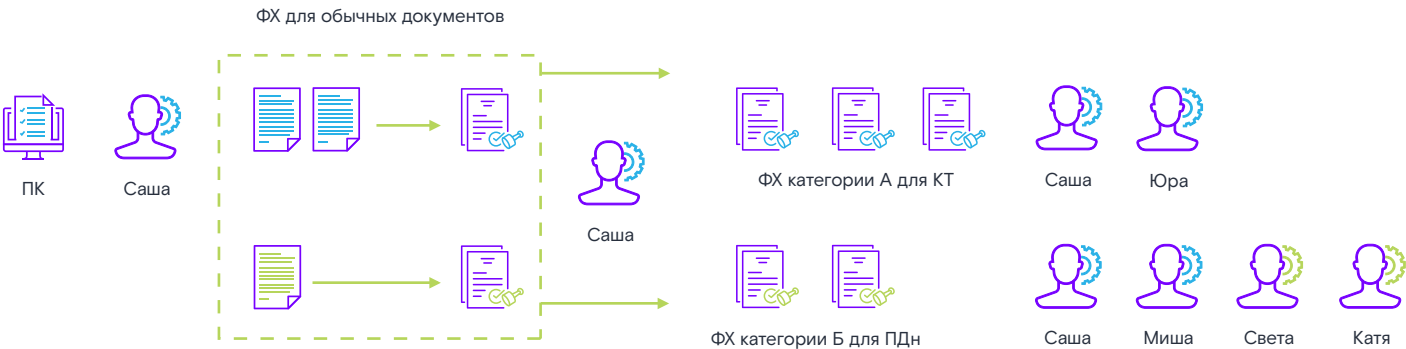


Рисунок 5. Схема хранения информации категории А и Б

Во время пилота были проверены все файловые хранилища компании и рабочие станции сотрудников, занимающихся подготовкой документов и имеющих доступ к конфиденциальной информации. В результате проверки обнаружались проблемы.

Проблема 1. Информация категории А «Коммерческая тайна» находилась в неполюженном месте – в хранилище, предназначенном для информации категории Б.

Для организации это стало серьезной проблемой, так как сотрудники Миша, Света и Катя, имеющие доступ только к информации категории Б, получили доступ к запрещенной информации категории А. Dozor File Crawler показал, что информацию в неполюженное место выложил сотрудник Саша.

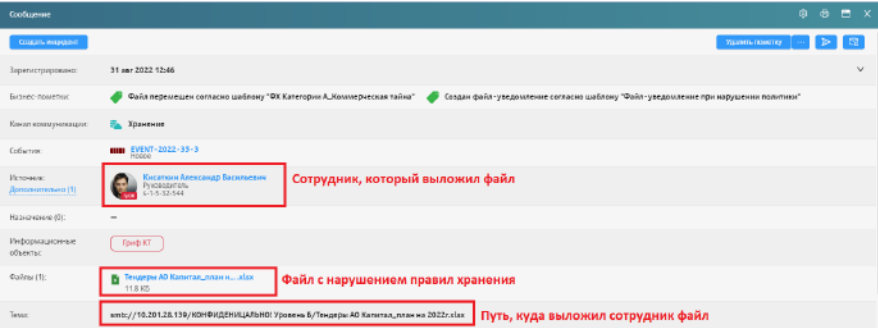
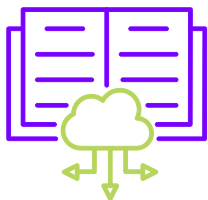


Рисунок 6. Пример отображения сообщения

Выяснилось, что злого умысла у сотрудника Саши не было. Он ошибся в классификации информации. Позже было установлено, что в документе содержались и персональные данные, и коммерческая тайна.



«Dozor File Crawler ежедневно проверял выложенные файлы и самостоятельно перемещал в нужное файловое хранилище»

Саша увидел в документе персональные данные и, не заметив сведений, являющихся коммерческой тайной, поспешил поместить его в файловое хранилище для информации категории Б.

Риск утечки коммерческой тайны возрос, ведь нельзя исключить факт, что Миша, Света и Катя, получившие доступ к документам категории А, не воспользуются ситуацией и эти данные не скопируют.

Проблема 2. После переноса документа, классифицированного как коммерческая тайна, в защищенный контур его копии/исходники оставались на рабочей станции сотрудника или на общедоступном файловом хранилище.

Саша и Юра, занимающиеся подготовкой документа, забывали удалять его копии/исходники. Саша готовил одну часть документа, Юра – другую. При этом после объединения частей в единый документ оба сотрудника продолжали работу над общим документом и ежедневно создавали копии с разными версиями на своих рабочих станциях.

Финальная версия документа, в которой содержалась коммерческая тайна, перемещалась в закрытое файловое хранилище для категории А. Но при этом Саша и Юра созданные ранее копии удалить забывали. Вспомнить позже, где какие исходники/копии хранятся, уже было трудно (над документом работали 6 месяцев).

Этот пример показал, что, несмотря на внедренные в компании правила хранения документов и полноценное обучение сотрудников этим правилам, нарушения все равно происходят.

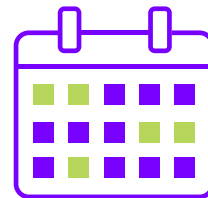
Люди могут ошибаться, это неизбежно. Но обеспечить защиту данных в покое от человеческого фактора необходимо. Обе проблемы были решены у заказчика с помощью функции активного краулера.

Во-первых, активный краулер начали использовать в качестве пропускного пункта. С этого момента каждый сотрудник мог выкладывать свои документы только в свою папку. Dozor File Crawler ежедневно проверял выложенные файлы и самостоятельно перемещал в нужное файловое хранилище. Если файл относился к коммерческой тайне, то по настроенным правилам хранения краулер автоматически переносил его в хранилище для документов категории А. По сути, задачу классификации информации переложили на Dozor File Crawler.

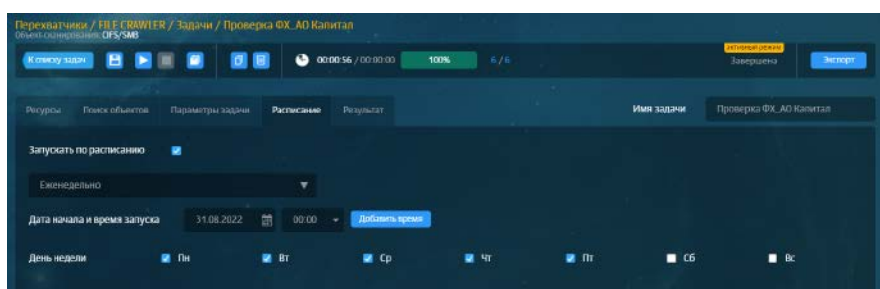
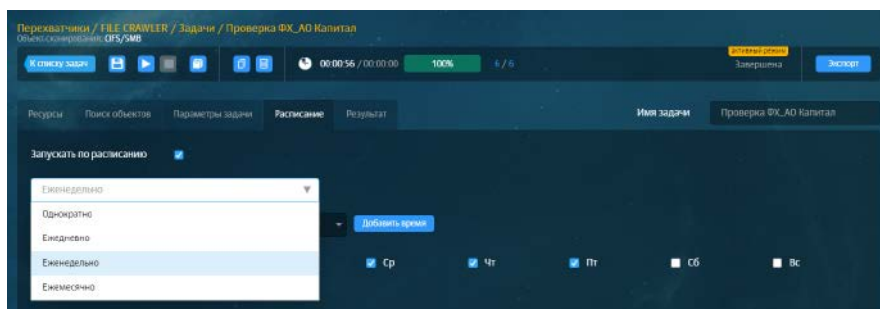


Рисунок 7. Схема работы активного краулера в качестве пропускного пункта

Во-вторых, в компании настроили периодическую проверку с помощью Dozor File Crawler рабочих станций и общедоступных файловых хранилищ на предмет наличия исходников/копий конфиденциальных документов с функцией их автоматического изъятия.



«С 2022 года
импортозамещение в ИТ-
отрасли стало обязательным»



Рисунки 8 и 9. Пример отображения в интерфейсе Solar Dozor настройки проверки Dozor File Crawler по расписанию

Импортозамещение

С 2022 года импортозамещение в ИТ-отрасли стало обязательным (Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»). Многие компании уже начали переходить с иностранных облачных хранилищ на российские решения, в том числе на локальные физические файловые хранилища.

При любой замене оборудования и ПО всегда встает вопрос миграции – обеспечения корректного переноса всех данных. В своей практике мы сталкивались со случаями, когда перенос с облачного на физическое файловое хранилище производился с нарушением иерархии документов. В результате миграции данные из одной директории оказывались уже в другой. Это чревато тем, что некоторая конфиденциальная информация окажется незащищенной (разные правила хранения для разных директорий). Вручную проанализировать все директории и проверить корректность расположения файлов – весьма трудоемкая задача, которая может прервать бизнес-процессы компании.

Ситуация усугубляется тем, что в любой момент доступ к используемому в компании иностранному облачному хранилищу может быть закрыт.

В такой ситуации пассивный режим работы (мониторинг) Dozor File Crawler поможет обнаружить конфиденциальную информацию, которая находится в неподобающем месте, а его активный режим (перемещение) позволит автоматически переместить информацию в нужное место.



Выводы

Данные в покое так же, как и данные в движении, требуют особого внимания сотрудников служб ИБ. Об утечках данных в движении мы слышим довольно часто (в новостях, в официальных статистиках). Но первоисточником многих утечек являются именно данные в покое. Обеспечить их защиту означает на раннем этапе выявить и предотвратить возможную утечку конфиденциальной информации. Данные в покое находятся в тылу организации и требуют надежного прикрытия!



Автор: Анастасия Васильева,
ведущий аналитик Центра
продуктов Дозор
компании «Ростелеком-Солар»

Анализ поведения пользователей во благо экономической безопасности

Зачем компании нужна экономическая безопасность (ЭБ)? Правильно, чтобы экономить (сберегать от злоумышленника) деньги компании. В век информационных технологий принято ловить за руку нечистоплотных сотрудников с помощью специальных систем контроля коммуникаций – DLP. Но проблема в том, что они реагируют непосредственно на инцидент, когда нечто нехорошее уже сделано. А можно ли выявить первые звоночки будущего инцидента?

Оказывается, можно. С помощью технологии UBA – анализа поведения пользователей и выявления аномалий на ранней стадии. Вот вам жизненный пример работы этой технологии: как специалист отдела ЭБ с помощью UBA решал задачу мониторинга недавно принятого на работу сотрудника и что из этого вышло.

Итак, специалист по экономической безопасности одной из компаний производственной сферы решал довольно тривиальную для ЭБ задачу: профилактический мониторинг активности недавно принятого в организацию сотрудника (в данном случае – главного инженера).

Так как UBA осуществляет неустанный качественный и количественный контроль активности сотрудников, был зафиксирован всплеск внешней активности главного инженера по каналу коммуникации «Корпоративная почта». Ранее не писавший и не получавший писем инженер вдруг резко активизировал переписку с внешними лицами.



Рисунок 1. Зафиксирован качественный персональный всплеск внешней активности главного инженера

Специалисту по экономической безопасности сразу бросились в глаза явные признаки нетипичного поведения главного инженера. Так, в день фиксации аномалии внимание безопасника привлекло письмо в почте инженера, полученное с электронного ящика бесплатной российской почтовой системы.

В письме лицо, позже идентифицированное как должностное лицо контрагента, со своей личной, а не корпоративной почты (что само по себе уже подозрительно) направило главному инженеру не официальное коммерческое предложение, а приблизительный план-набросок предстоящих трат.

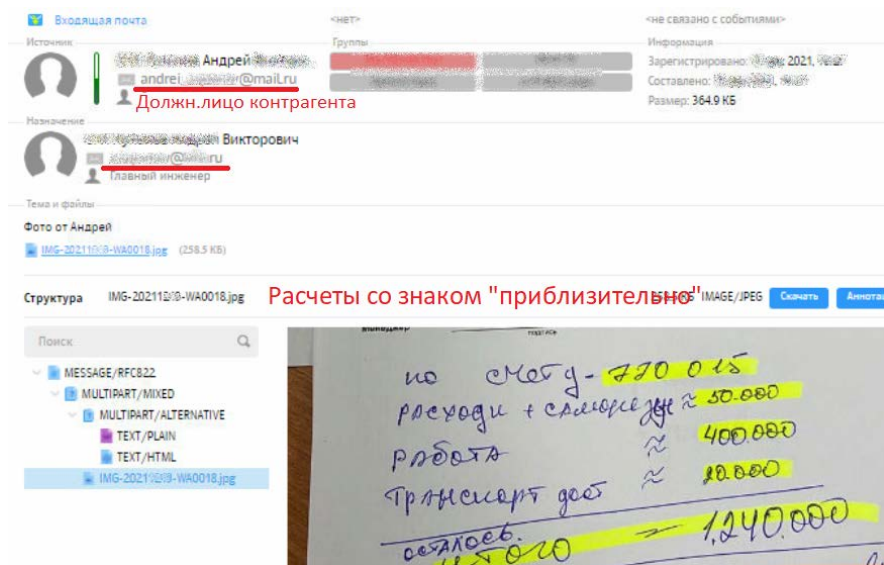
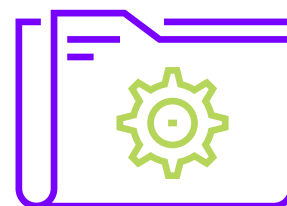


Рисунок 2. План-набросок предстоящих трат, оформленный от руки и полученный от должностного лица контрагента

Данного факта было достаточно, чтобы внимательнее изучить все письма, относящиеся к периоду аномалии, и попробовать оценить масштаб деятельности, развернутой главным инженером. Офицер безопасности обратился в раздел «Особые контакты» модуля UBA, чтобы посмотреть, с кем взаимодействовал инженер в период аномальной активности.



«Особые контакты – это внешние неизвестные контакты, с которыми еще никто в организации не взаимодействовал»

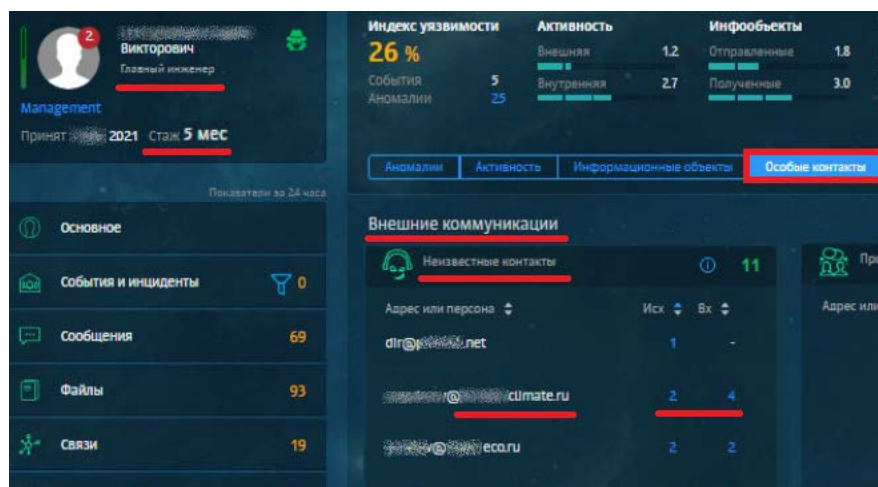


Рисунок 3. Контакты с «потенциальным поставщиком» в сфере вентиляции и климатического оборудования

Специалист по экономической безопасности обратил внимание на контакты главного инженера с «потенциальным поставщиком» в сфере вентиляции и климатического оборудования, доменная часть почты которого оканчивается на @__climate.ru. Так как с контактом явно осуществлялась переписка, безопасник обратился к ее содержанию, заподозрив в качестве причины направления двух коммерческих предложений в один день возможную корректировку не сроков, а суммы.

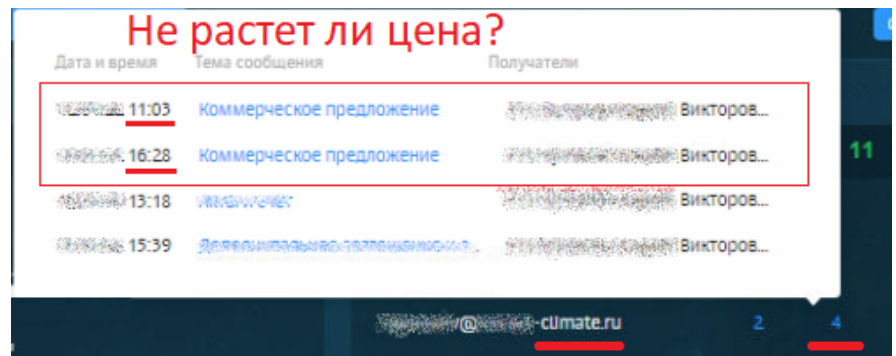


Рисунок 4. Сравнение цен между утренним и вечерним коммерческими предложениями

Коммерческо-техническое предложение от 11.03.2023 г.
на устройство вытяжной систем П19 из полипропилена

№	Наименование оборудования и материалов	Ед. изм.	Кол-во	Стоимость материалов и оборудования		Стоимость работ	
				Цена, руб.	Сумма, руб.	Цена, руб.	Сумма, руб.
Вытяжная система В19							
1	Демонтаж воздуховодов	м.кв.	21	-	-	1485,00	32 185,00
2	Демонтаж/монтаж вентилятора	шт.	1	-	-	8 780,00	8 780,00
3	Пруток полипропиленовый	шт.	2	4 390,00	8 780,00	8 780,00	8 780,00
4	Сборка разборка лесов	м.пог	9	1 190,00	10 710,00	10 710,00	10 710,00
5	Крепежный и расходный материал	шт.	1	84,00	84,00	7 780,00	7 780,00
6	Труба канализационная д.50 с фасонными элементами	шт.	1	1 190,00	1 190,00	7 780,00	7 780,00
7	Сборка разборка лесов	м.пог	9	1 190,00	10 710,00	10 710,00	10 710,00
8	Крепежный и расходный материал	шт.	3	84,00	252,00	7 780,00	7 780,00
9	Демонтаж/монтаж вентилятора	шт.	1	-	-	7 780,00	7 780,00
10	Пруток полипропиленовый	шт.	4	2 190,00	8 760,00	7 780,00	7 780,00
11	Пруток полипропиленовый	кг	2	2 190,00	4 380,00	7 780,00	7 780,00
12	Труба канализационная д.50 с фасонными элементами	м.п	20	3 950,00	79 000,00	7 780,00	7 780,00
13	Сборка разборка лесов	компл	1	16 980,00	16 980,00	7 780,00	7 780,00
14	Крепежный и расходный материал	компл	1	2 190,00	2 190,00	7 780,00	7 780,00
Итого за оборудование:							1 107 608,00
Итого за работы:							58 680,00
Транспортные расходы:							16 980,00
Итого:							1 166 288,00

Рисунок 5. Коммерческое предложение от 11:03 (утреннее)

Коммерческо-техническое предложение от 16.03.2023 г.
на устройство вытяжной систем П19 из полипропилена

№	Наименование оборудования и материалов	Ед. изм.	Кол-во	Стоимость материалов и оборудования		Стоимость работ	
				Цена, руб.	Сумма, руб.	Цена, руб.	Сумма, руб.
Вытяжная система В19				Повысил в 5 раз			
1	Демонтаж воздуховодов	м.кв.	1	-	-	116 185,00	116 185,00
2	Демонтаж/монтаж вентилятора	шт.	1	-	-	8 780,00	8 780,00
3	Пруток полипропиленовый	шт.	2	4 390,00	8 780,00	8 780,00	8 780,00
4	Сборка разборка лесов	м.пог	9	1 190,00	10 710,00	10 710,00	10 710,00
5	Крепежный и расходный материал	шт.	1	84,00	84,00	7 780,00	7 780,00
6	Труба канализационная д.50 с фасонными элементами	шт.	1	1 190,00	1 190,00	7 780,00	7 780,00
7	Сборка разборка лесов	м.пог	9	1 190,00	10 710,00	10 710,00	10 710,00
8	Крепежный и расходный материал	шт.	3	84,00	252,00	7 780,00	7 780,00
9	Демонтаж/монтаж вентилятора	шт.	1	-	-	7 780,00	7 780,00
10	Пруток полипропиленовый	шт.	4	2 190,00	8 760,00	7 780,00	7 780,00
11	Пруток полипропиленовый	кг	2	2 190,00	4 380,00	7 780,00	7 780,00
12	Труба канализационная д.50 с фасонными элементами	м.п	20	3 950,00	79 000,00	7 780,00	7 780,00
13	Сборка разборка лесов	компл	1	16 980,00	16 980,00	7 780,00	7 780,00
14	Крепежный и расходный материал	компл	1	2 190,00	2 190,00	7 780,00	7 780,00
Итого за оборудование:							896 196,00
Итого за работы:							71 190,00
Транспортные расходы:							16 980,00
Итого повышение на 400тыс.руб.							1 585 960,00

Рисунок 6. Коммерческое предложение от 16:28 (вечернее) с подросшей ценой

Разница между утренним и вечерним коммерческими предложениями составила более 400 тыс. рублей. Далее офицер безопасности попытался установить пути распространения данного «модернизированного» коммерческого предложения, чтобы знать всю хронологию развития событий. Обратившись к функции «Умный поиск», специалист установил цепочку поступления утреннего коммерческого предложения, а затем вечернего «модернизированного» со значительно подросшей ценой. Также был установлен факт пересылки «модернизированного» коммерческого предложения директору по производству, не входившему в круг лиц, помогающих освоить бюджет.



«Также был установлен факт пересылки «модернизированного» коммерческого предложения директору по производству, не являющемуся участником круга лиц, помогающих освоить бюджет»

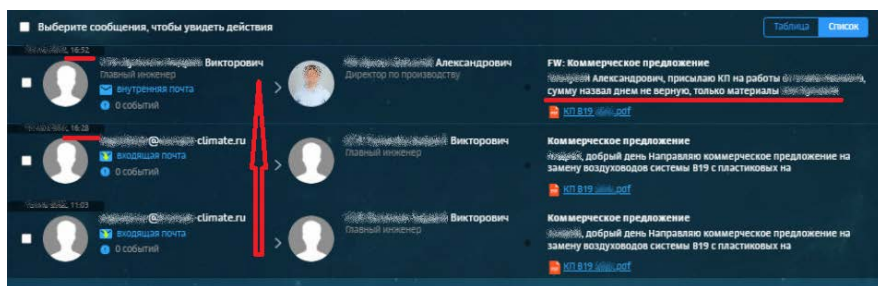


Рисунок 7. Цепочка поступления извне и пересылки внутри организации коммерческих предложений



Автор: Максим Бузинов,
руководитель
исследовательской группы
Центра продуктов Дозор
компании «Ростелеком-Солар»



Автор: Виталий Петросян,
ведущий аналитик Центра
продуктов Дозор компании
«Ростелеком-Солар»

Выводы

Перед подразделением экономической безопасности стояла задача по сопровождению принятого сотрудника в период его испытательного срока. С помощью тонкой подсветки системой UBA были выявлены аномалии в его поведении. Таким образом, службе ЭБ удалось изобличить сотрудника, пытавшегося реализовать на новом месте работы свой корыстный умысел.

«С этим сотрудником что-то не так». Как анализ поведения пользователей предотвращает инциденты в фармкомпаниях

Информационная и экономическая безопасность любого предприятия во многом зависит от действий его сотрудников. Не исключением является и фармацевтическая отрасль, где любые инциденты могут привести к очень серьезным последствиям, многомиллионным убыткам, а также ущербу для здоровья людей. Сегодня многие крупные компании используют DLP-системы, которые предназначены для предотвращения утечек информации и противодействия корпоративному мошенничеству.

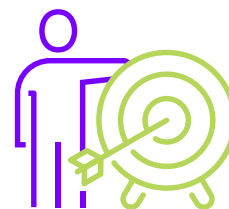
С недавних пор в отдельных DLP-системах, например в Solar Dozor, появилась возможность анализа поведения пользователей. В данном случае это отдельный модуль, который формирует профили сотрудников, определяет их типичное поведение и выявляет отклонения.



«Информационная и экономическая безопасность любого предприятия во многом зависит от действий его сотрудников»

Как устроен анализ поведения в DLP-системе

Модуль, который отвечает за анализ поведения пользователей, собирает и обрабатывает данные по активности сотрудника в рабочей почте. Система смотрит на количество сообщений, соотношение входящих и исходящих сообщений, почтовый трафик, который идет за пределы компании, время отправки сообщений, круг адресатов и адресантов. На основе истории коммуникаций модуль Dozor UBA автоматически формирует личный профиль каждого сотрудника, а затем фиксирует аномалии в его поведении, если они появляются. Также модуль ищет работников, попадающих под значимые для безопасности паттерны поведения (группы поведенческих особенностей и аномалий). Например, сотрудники, которые часто работают ночью или в выходные дни; возможные инсайдеры – те, у кого отмечается высокая внешняя активность и частая отправка писем с вложениями; работники с нулевой активностью и т. д.



«На основе истории коммуникаций модуль Dozor UBA автоматически формирует личный профиль каждого сотрудника»

Модуль анализа поведения пользователей позволяет эффективно предотвращать инциденты. Повышенная активность коммуникаций, запрос у коллег различных документов, получение большого количества писем с вложениями – все это может свидетельствовать о готовящемся сливе информации. Кроме того, с помощью поведенческого анализа можно выявлять экономические преступления. Как это работает, покажем на реальных ситуациях из практики фармацевтических компаний.

После внедрения модуля анализа поведения пользователей в одной из фармацевтических компаний офицеры безопасности зафиксировали всплеск внешней активности у ряда сотрудников. Среди прочих такая аномалия была замечена у исполняющего обязанности начальника цеха фасовки. Учитывая, что к руководителям внимание всегда более пристальное, сотрудники службы безопасности решили детально разобраться в ситуации.

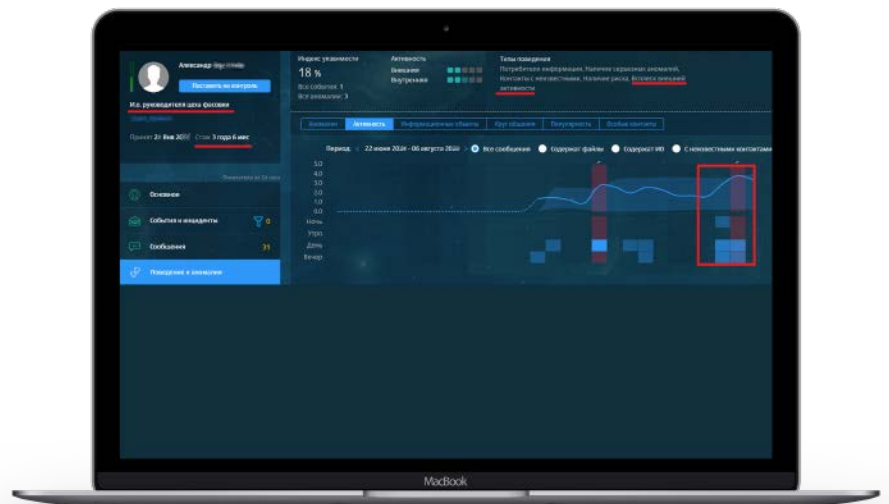


Рисунок 1. Фиксация всплеска внешней активности и. о. руководителя цеха фасовки

Всплеск активности был связан с общением с поставщиками паллетоупаковщиков. И. о. начальника стал погружаться в специфику закупочной деятельности, что объясняло появление аномалии. Но решение изучить коммуникации все же было принято.

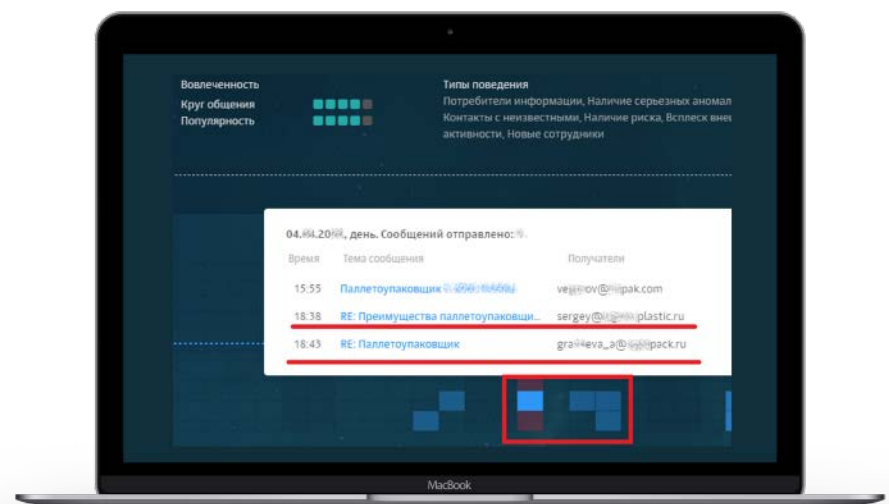


Рисунок 2. Переговоры и. о. руководителя с потенциальными поставщиками

После анализа писем стало ясно, что некоторые потенциальные поставщики, которые присылали свои коммерческие предложения по паллетоупаковщикам, пытались ввести в заблуждение неопытного руководителя, навязывая невыгодные для компании условия. В частности, один из поставщиков выставлял в качестве преимущества техническую характеристику своего оборудования (см. скриншот ниже), которая в итоге привела бы к необходимости заключать договор на дополнительное обслуживание поставляемых аппаратов.

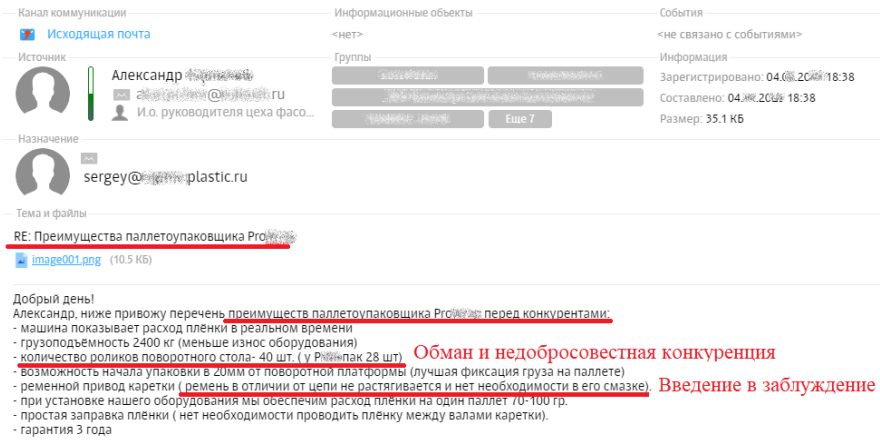


Рисунок 3. Часть текста из переписки с потенциальным поставщиком, пытавшимся ввести в заблуждение и. о. руководителя цеха фасовки

Очевидно, что большое количество роликов фактически дороже в содержании и обслуживании, а резиновый ремень менее практичен и недолговечен по сравнению с цепью. Однако в итоге новый руководитель повелся на уговоры и начал обсуждать условия с ушлым поставщиком.

Кроме того, при анализе коммуникаций и. о. начальника цеха фасовки офицеры безопасности заметили, что он вел рабочую переписку в выходной день, что раньше было для него нетипично.

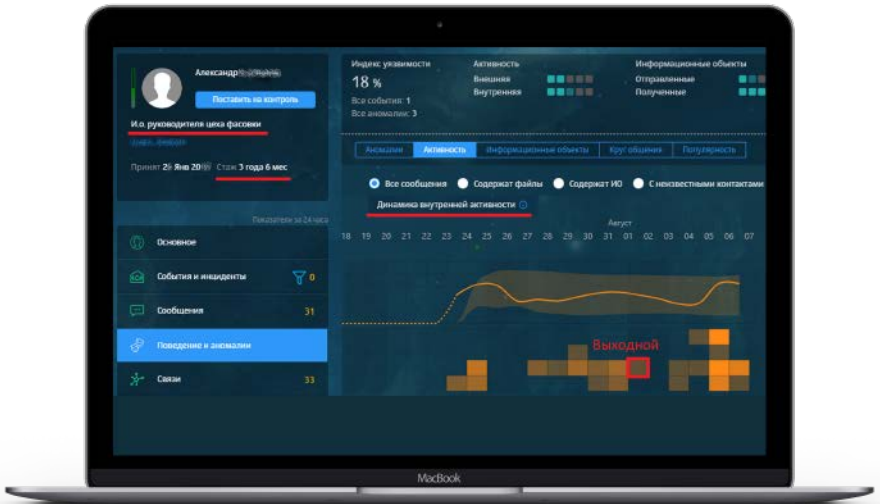


Рисунок 4. Только вступил в должность и уже вынужден решать рабочие вопросы по выходным



«Анализ поведения пользователей позволил офицерам безопасности в центральном офисе более эффективно отслеживать коммуникации сотрудников всех филиалов»

Случайная находка позволила выявить попытку скрыть произошедший на производстве инцидент. Из переписки выяснилось, что за несколько дней до этого был обнаружен брак при упаковке продукции, а запись об этом не была внесена в соответствующие журналы, и никакие меры предприняты не были. Одна из сотрудниц цеха интересовалась, как ей спустя несколько дней оформлять акт о недостатке. И. о. начальника цеха в ответном письме порекомендовал зафиксировать проблему текущим днем, закрыв глаза на уже нанесенный компании за предыдущие несколько дней ущерб.

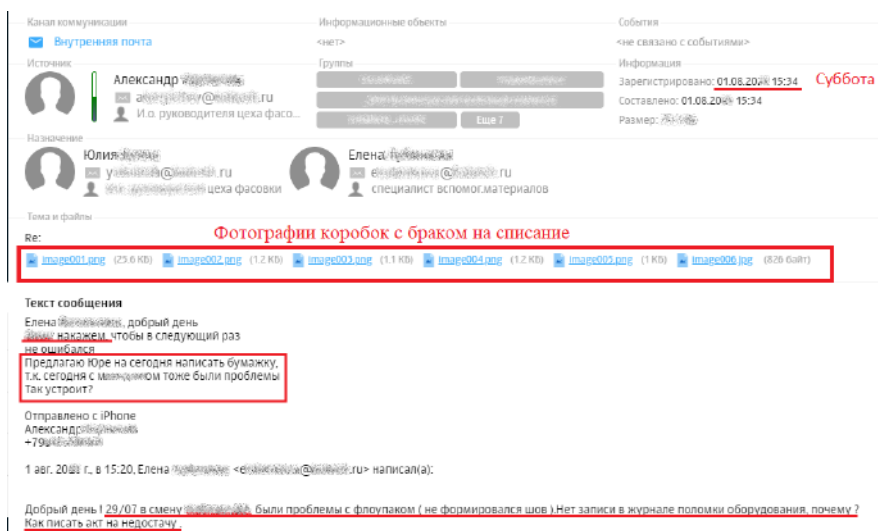


Рисунок 5. Предложение о подложном списании бракованной продукции, высказанное и. о. руководителя цеха фасовки

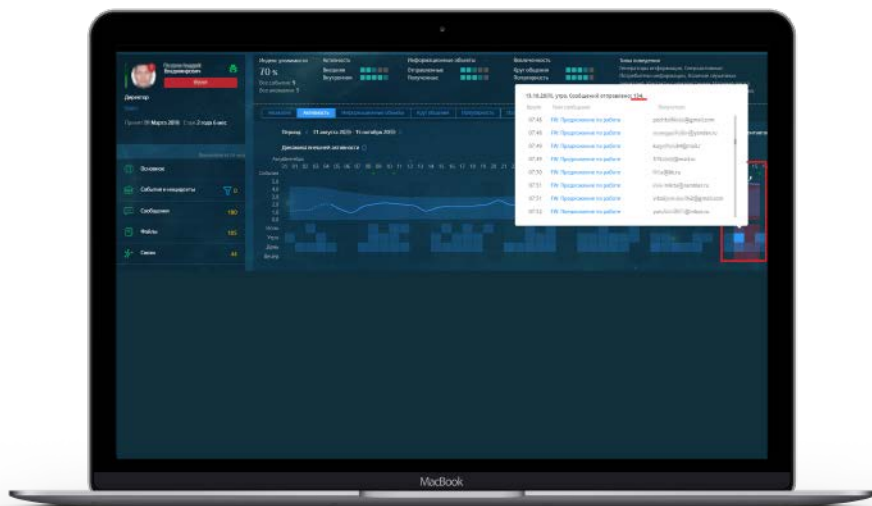
Благодаря работе DLP-системы и анализу поведения пользователей, недобросовестный исполняющий обязанности должность начальника цеха в итоге не получил.

Спасение команды от руководителя

В компании – поставщике фармацевтической продукции, в которой уже была внедрена DLP-система, взяли на вооружение технологию анализа поведения пользователей. Это позволило офицерам безопасности в центральном офисе более эффективно отслеживать коммуникации сотрудников всех филиалов.

Поводом для проведения расследования снова стал всплеск внешней активности, который был зафиксирован у директора регионального склада.

Благодаря другим каналам получения информации, служба безопасности выяснила, что у деспотичного руководителя возник конфликт с подчиненными, которых не устраивали его методы работы. Работники склада планировали уволиться всей командой и поставили ультиматум директору склада.



«Выявленный инцидент
позволил предотвратить
вероятный и существенный
финансовый ущерб»

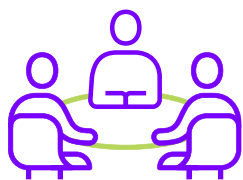
Рисунок 6. Всплеск не характерной для лица внешней активности

Чтобы не подвергать риску занимаемую должность, новый руководитель склада принял осознанное решение скрыть этот факт от высшего руководства, и поэтому заранее поставил себе задачу организовать поиск новых сотрудников.

Об этом стало известно только после детального и тщательного изучения внешней активности данного руководителя. Как выяснилось, он разместил объявления с вакансиями работников склада на различных агрегаторах по поиску работы и через корпоративную почту регулярно рассылал письма с предложениями о работе соискателям, чтобы в подходящий момент "бесшовно" заменить покидающих компанию сотрудников и избежать наказания за возможный сбой и простой в работе склада.

На первый взгляд ситуация может показаться безобидной, но специфика работы крупного склада, где хранится фермпродукция и постоянно происходят различные процессы в виде поступлений и отгрузок, подразумевает четкую и бесперебойную работу. Замена опытных работников на неопытных, к тому же сразу в полном составе, может привести к серьезным проблемам и убыткам для компании.

Выявленный инцидент позволил предотвратить вероятный и существенный финансовый ущерб от действий директора склада. Команду работников склада удалось сохранить в полном составе, а руководителю, с которым не могли сработать подчиненные, пришлось покинуть данную компанию. Кроме того, именно благодаря DLP-системе стало известно о том, что рассылка писем кандидатам на позиции работников склада была практически единственной рабочей активностью директора. Все оставшееся рабочее время руководитель предпочитал посвящать онлайн-играм, а однажды был замечен за копированием клиентской базы на флешку.



«Для менеджеров по продажам
отсутствие внешней
активности – явный показатель
ненормального поведения»

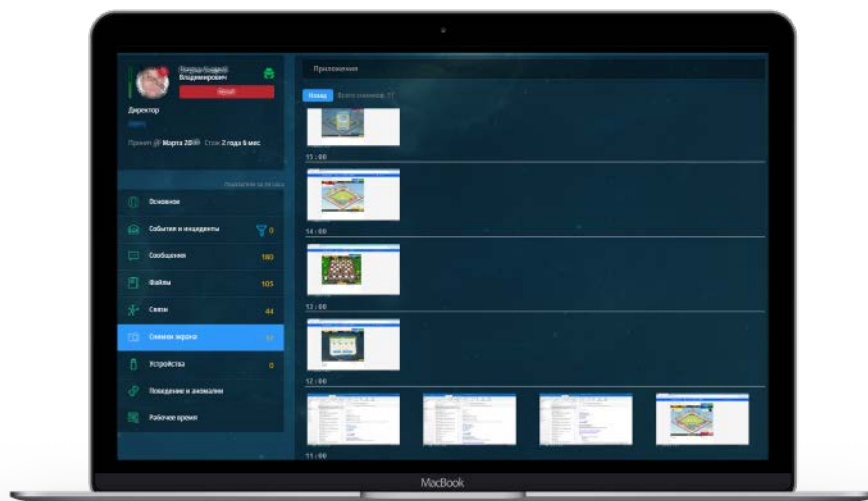


Рисунок 7. Стандартное времяпрепровождение нерадивого начальника

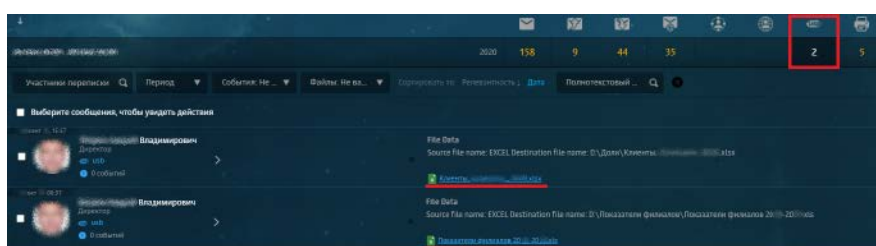


Рисунок 8. Копирование клиентской базы и показателей всех филиалов на USB
нерадивым руководителем

Мертвые и полумертвые души

В той же компании из предыдущего кейса офицеры безопасности решили проанализировать поведение сотрудников, которые попали в группу поведенческих аномалий «Отсутствие».

К такому паттерну поведения система относит тех, у кого на протяжении долгого времени нет ни внутренней, ни внешней активности в корпоративной почте.

Обратили внимание на то, что в список попали несколько менеджеров по продажам, для которых отсутствие внешней активности – явный показатель ненормального поведения.

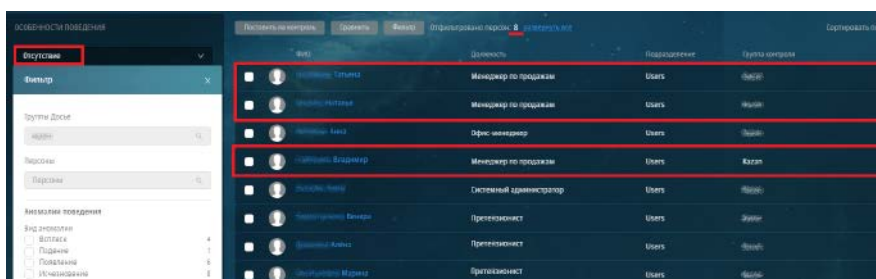


Рисунок 9. Подозрительное присутствие менеджеров по продажам
в списке паттерна «Отсутствие»

Даже с учетом того, что такие сотрудники много времени проводят на встречах, договоренности с клиентами все равно фиксируются в почте. В результате расследования выяснилось, что менеджеры практически не взаимодействовали с партнерами, не занимались поиском новых, а довольствовались процентом с уже заключенных контрактов.



«Менеджеры не взаимодействовали с партнерами, не занимались поиском новых, а довольствовались процентом с уже заключенных контрактов»

Дополнительный доход им обеспечивал слив конкурентам закрытой корпоративной информации. Благодаря DLP-системе было зафиксировано, что менеджеры, попавшие в список отсутствующих, регулярно пересылали себе на личную почту список позиций, которые поступят на реализацию и к которым будут применяться разные акции.

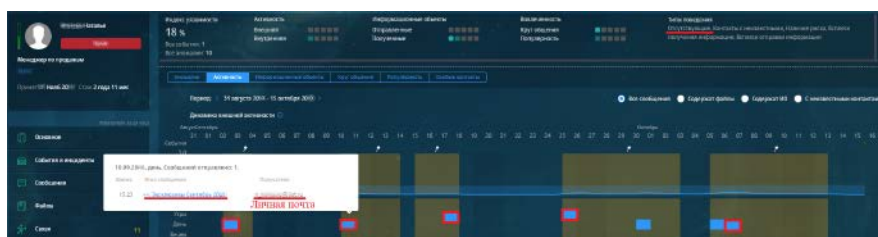


Рисунок 10. Пример отправки закрытой корпоративной информации на личную почту менеджером, включенным в паттерн «Отсутствие»

Выявить такую ситуацию без анализа поведения было бы сложнее. В отсутствие инцидентов DLP-система не срабатывала: поскольку менеджеры регулярно отправляли подобные файлы партнерам, что является нормой.

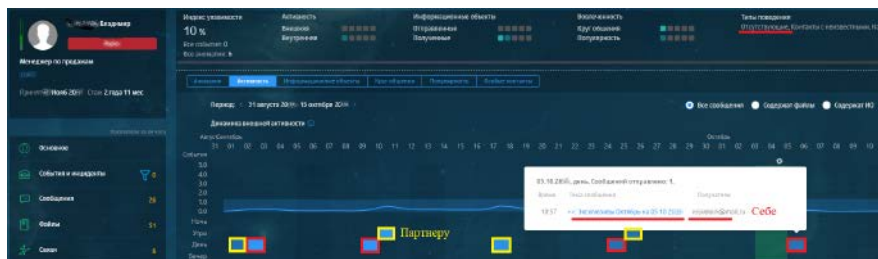


Рисунок 11. Пример отправки менеджером по продажам закрытой корпоративной информации себе на личную почту и партнерам

По итогам расследования отдел продаж реорганизовали, а рабочие процессы перестроили.

Отдельная драма разыгралась вокруг паттерна «Мертвые души». Было обнаружено, что помощница одного из директоров не проявляет никакой активности в течение нескольких месяцев. Оказалось, что девушка была уволена несколько месяцев назад, а ее учетная запись осталась. Экс-сотрудница также получала закрытые рассылки. Она заходила в свой почтовый ящик через веб-интерфейс, сохраняла документы на свой компьютер, после чего передавала информацию заинтересованным людям.



Авторы: Виталий Петросян,
ведущий аналитик
Центра продуктов Дозор
компании «Ростелеком-Солар»

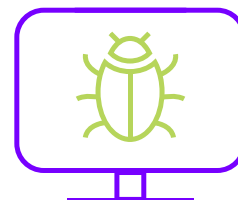
Выводы

Без модуля анализа поведения пользователей (UBA), который отслеживает аномалии с точки зрения активности коммуникаций в корпоративной почте и мессенджерах, поиск нарушителей становится трудоемкой задачей. Проверка сотрудников по паттернам является эффективным инструментом для профилактики утечек, а также выявления уязвимостей в бизнес-процессах.

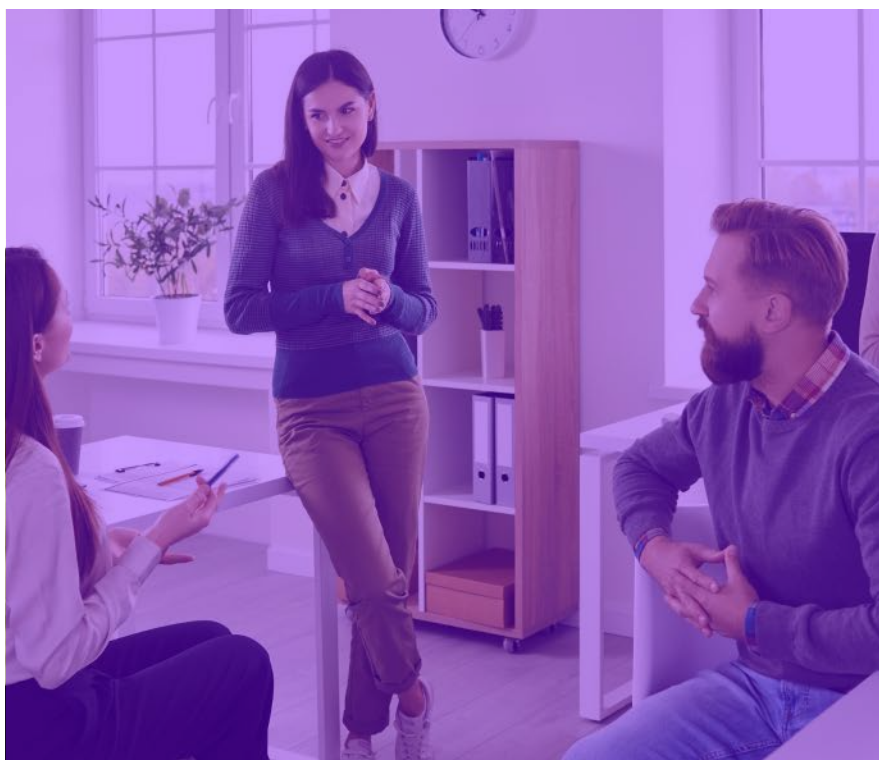
Новости из будущего: прогнозируем поведение пользователя

Что такое поведение?

В повседневной жизни, общаясь с людьми, мы наблюдаем за поведением собеседника, и оно многое может о нем сказать: о его воспитании, привычках, увлечениях, принципах и о личности в целом. Для нас, как для социальных существ, это очень ценная информация, так как позволяет сделать важные выводы: можно ли доверять человеку, на что обратить внимание, стоит ли с ним вообще иметь дело.

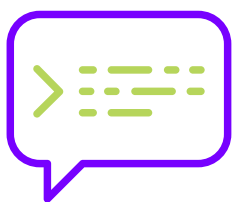


«Гораздо лучше знать о потенциальной угрозе и контролировать ее, чем постфактум узнать об утечке секретных данных»



При чем здесь информационная безопасность? Согласитесь, гораздо лучше знать о потенциальной угрозе и контролировать ее, чем постфактум узнать об утечке секретных данных. И как раз в моменте «необходимости знания о потенциальной угрозе» мы возвращаемся к тому, что мы можем прогнозировать поведение человека. Давайте введем формальное определение: поведением называется определенный сложившийся образ взаимодействия индивидуума с окружающей средой.

А можем ли мы сопоставить его с набором поступков и действий, которые могли бы быть важны для ИБ? Конечно, ведь в повседневной жизни мы делаем вывод о личности человека на основе того, что он делает и говорит.



«Собирается и обрабатывается информация о переписке в корпоративной почте, а также в мессенджерах»

После того как мы узаконили отношения «Поведение – Действия», встает вопрос: «А что с этим делать и как нам это поможет поймать негодяя?» Ответ находится в состоянии суперпозиции: он и прост, и сложен одновременно. Но мы не ищем простых путей, поэтому вводим в игру математику и определяем поведение как случайный процесс. Как мы знаем, случайный процесс – это некоторая функция, значениями которой являются случайные величины. Держим в голове, что «поведение – это действия» и углубляемся в специфику решения задачи в условиях модуля UBA (User Behavior Analytics).

Наши случайные величины на самом деле параметры, которые рассчитываются на основе действий и коммуникаций сотрудника на рабочей станции. Собирается и обрабатывается информация о переписке в корпоративной почте, а также в мессенджерах. Интересует нас в переписке сотрудника почти все: направление переписки – входящая или исходящая, количество отправленных файлов, является ли собеседник внутренним пользователем или же это кто-то вне компании и так далее. Вся эта информация (и даже больше) используется в расчете показателей поведения. Сколько человек отправляет файлов, сколько получает, его активность внутри компании, активность, направленная за пределы компании, суточная активность, его деловой диапазон. Каждый день эти показатели пересчитываются на основе окна предыдущих 7 дней.

Посмотрим на примере, как же выглядит поведение человека глазами бездушной машины и беспристрастной математики. Возьмем значения показателя внешней активности. Очень интересный показатель для офицера службы безопасности: а вдруг всплеск внешней активности связан с тем, что сотрудник пытается слить секретные данные компании конкурентам? Итак, мы берем значения показателя внешней активности за 80 дней и визуализируем, банально соединяя точки значений.

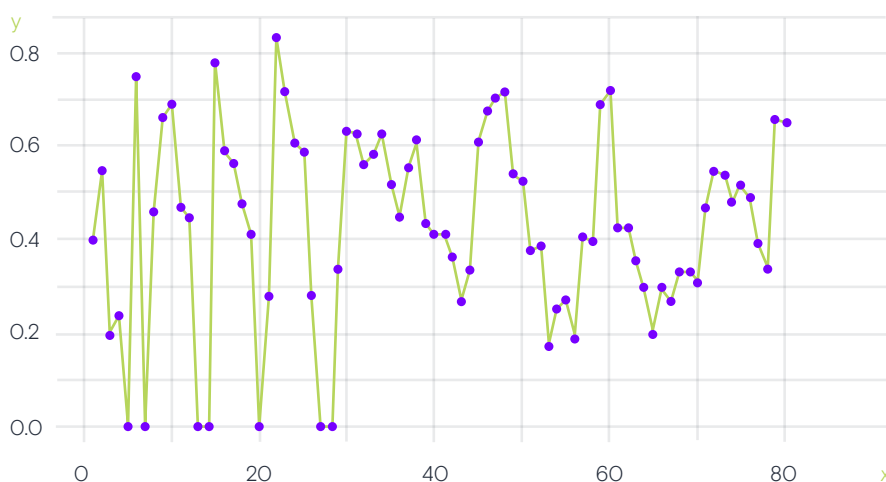


Рисунок 1. Исходная функция показателя внешней активности

Как же мы собираемся предсказывать поведение? В момент проработки постановки задачи возникла гипотеза: поведение сотрудника циклично: ему свойственно вести себя в разные промежутки времени определенным образом. Периодичность может быть за совершенно разные отрезки времени: день, неделя, месяц. В решении задач определения периодичности используются совершенно разные методики: скользящие средние, статистический анализ временных рядов (выявление тренда и сезонности) и т. д. Но одним из главных инструментов является гармонический анализ, в частности анализ Фурье, который и будет применяться в дальнейшей разработке задачи.

Анализом Фурье называют разложение сложных периодических сигналов на элементарные гармонические составляющие, а также оценку или измерение их характеристик. Основывается анализ на преобразовании Фурье. Формальное определение: преобразование Фурье – это математическая операция, которая преобразует функцию от времени в частотные компоненты. В основе этого преобразования лежит простая идея: почти любую периодическую функцию можно представить суммой отдельных гармонических составляющих (ряда Фурье) – синусоид и косинусоид с различными амплитудами A , периодами T и, следовательно, частотами ω . Гармонические составляющие, они же гармоники, – это некоторые функции вида

$$\cos(2\pi f_k) \text{ и } \sin(2\pi f_k), \text{ где } f_k = \frac{1}{L}k$$

– частота k -й гармоники.

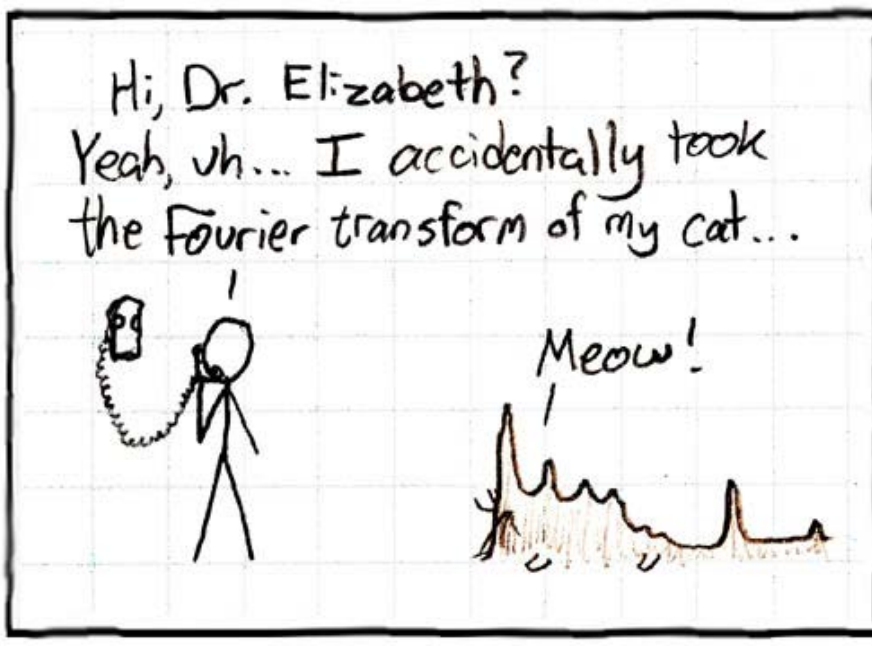


Рисунок 2. Комикс xkcd (с)



«Одним из главных инструментов является гармонический анализ, в частности анализ Фурье, который и будет применяться в дальнейшей разработке задачи»

Продолжим с математикой: ряд Фурье записывается следующим образом:

$$u(x) = \frac{1}{2}a_0 + \sum_{k=1}^{\infty} [a_k \cos(2\pi f_k x) + b_k \sin(2\pi f_k x)]$$

Преобразование Фурье в обыкновенном своем виде содержит экспоненту, в степени которой мнимая единица:

$$\hat{f}(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(x) e^{-ix\omega} dx$$

(Прим. Множитель – так называемый нормировочный множитель, который становится необходимым в момент перехода к дискретному спектру, – перед интегралом может разниться от источника к источнику, что связано, во-первых, с разными подходами к нормировке, а во-вторых, с возможностью корректного выведения формулы обратного преобразования). Поэтому, чтобы избавиться от комплексных чисел, используют косинус-преобразование Фурье. Прямое:

$$f(x) = \sqrt{\frac{2}{\pi}} \int_0^{\infty} F(\alpha) \cos \alpha x d\alpha.$$

И обратное:

$$F(a) = \sqrt{\frac{2}{\omega}} \int_0^{\infty} f(t) \cos \alpha t dt.$$

Дискретное преобразование Фурье в общем виде имеет следующий вид.

Прямое:

$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{2\pi i}{N} kn} = \sum_{n=0}^{N-1} x_n \left(\cos \frac{2\pi kn}{N} - i \sin \left(\frac{2\pi kn}{N} \right) \right), k = 0, \dots, N-1$$

Обратное:

$$x_n = \sum_{k=0}^{N-1} X_k e^{\frac{2\pi i}{N} kn} = \frac{1}{N} \sum_{k=0}^{N-1} X_k \left(\cos \frac{2\pi kn}{N} - i \sin \left(\frac{2\pi kn}{N} \right) \right), n = 0, \dots, N-1$$

После разложения сигнала (то есть нашей «функции поведения») каждому периоду будет соответствовать гармоника. Из формул выше X_n и будет соответствовать значению вклада гармоники.

А вот на практике мы столкнулись с множеством нюансов, о которых мы дальше поговорим.

Быстрое преобразование Фурье

$$\int x^n dx = x^{n+1}/(n+1) + c$$



«Если несколько гармоник достаточно полно описывают сигнал, то справедлив вывод, что мы можем с некоторой вероятностью судить о закономерностях поведения»

Раньше уже упоминался момент расчета вклада гармоник в общий вес функции, и у этого есть свое название – спектр. Спектральный анализ – один из методов обработки сигналов, который позволяет выявить частотный состав сигнала. Напомним, что каждая гармоника соответствует некоему периоду. Соответственно, выдвигая гипотезу о существовании закономерностей поведения, мы бы хотели увидеть на этих спектрах преобладающие составляющие, которые наиболее полно описывают весь сигнал. Что это значит?

Возвращаемся к идее, что периодический сигнал может быть разложен на простые составляющие, где каждая гармоника отвечает за свою частоту. И каждая гармоника имеет свой вклад, то есть описывает определенный процент сигнала. Вывод следующий: если несколько гармоник достаточно полно описывают сигнал, то справедлив вывод, что мы можем с некоторой вероятностью судить о закономерностях поведения. Человеческим языком – человек ведет себя последовательно, наша гипотеза верна, и мы все можем спрогнозировать!

Но вернемся к теории: вообще говоря, спектр периодического сигнала – дискретный и для наших данных за 85 дней – будет иметь следующий вид.

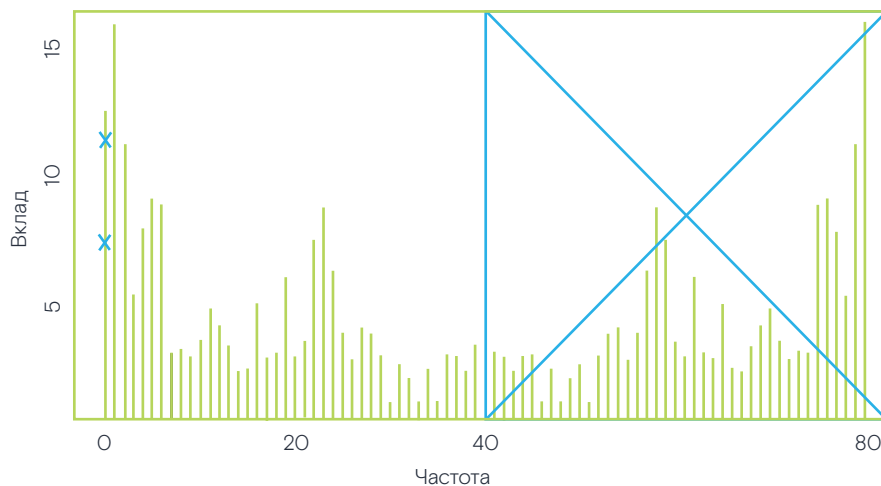


Рисунок 3. Спектр исходного сигнала

На рисунке зачеркнута половина гармоник. Это очень важно обозначить в явном виде, потому что согласно теореме Котельникова максимальная частота гармоники должна быть такой, чтобы на нее приходилось как минимум два отсчета, поэтому число гармоник равно половине числа отсчетов дискретного сигнала. Для выборки размера N отсчетов количество гармоник равно $N/2$. Уже тут мы видим выделяющиеся гармоники, но для хоть сколько-то точного анализа и последующего прогнозирования это, конечно, не годится. Стоит отметить, что первая гармоника на графике не должна учитываться

в последующих исследованиях, поскольку это период самого сигнала, то есть отражает цикл всего сигнала в 85 дней, а это особой информации не несет. Поэтому правильный спектр будет выглядеть следующим образом:

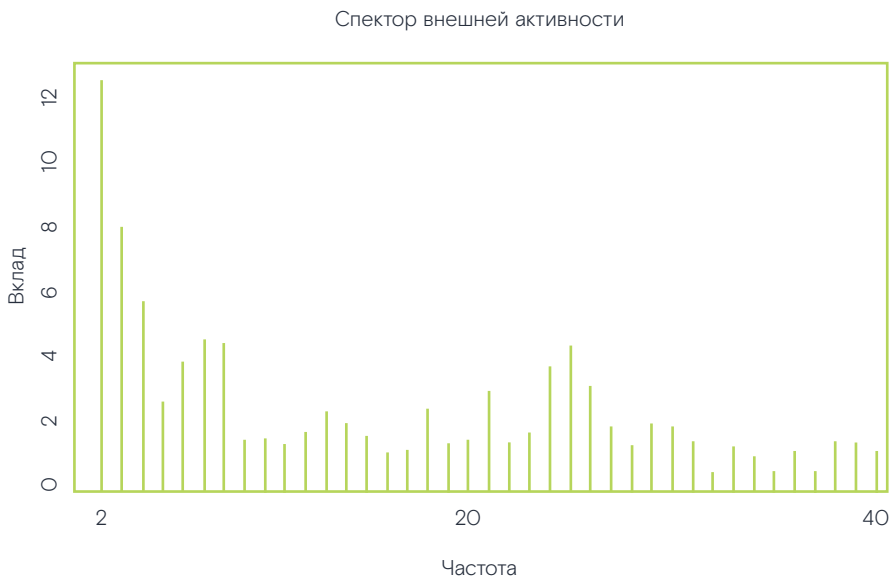


Рисунок 4. Правильный спектр исходного сигнала

Чтобы перейти от частоты к периоду, следует воспользоваться формулой, известной со школьных времен:

$$T = \frac{1}{f}, \text{ где,}$$

T – период,

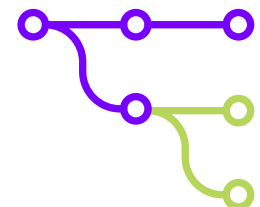
f – частота.

Так получается, например, что графически первая гармоника (фактически – вторая) соответствует 1/2 всего сигнала: 40 дням.

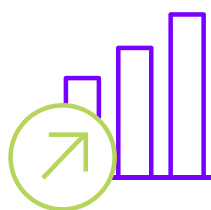
Оконное преобразование Фурье

Но даже если построить простой спектр за меньшее количество времени, например за месяц, это все равно не будет нести в себе сакральное знание периодичности. Поэтому работаем дальше. Ведь искать месячную периодичность в сигнале «длительностью» в месяц бессмысленно. Но есть выход – оконное преобразование Фурье. Суть оконного преобразования Фурье заключается в разбиении исходного сигнала на короткие временные промежутки, к которым к каждому по отдельности применяется преобразование Фурье. Формально это выглядит так:

$$F(t, \omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(\tau) W(\tau - t) \cos 2\pi \omega t d\tau$$



«Искать месячную периодичность в сигнале «длительностью» в месяц бессмысленно»



«Вклад максимальных гармоник определяет норму (объем) исходной функции (показателя поведения)»

Существуют разные виды оконных функций: прямоугольное, треугольное, преобразование Гаусса, Хеннинга, Хэмминга, Чебышева и еще много-много разных оконных функций, носящих имена известных (и не очень) ученых. Отличаются они способами реализации улучшения частотного спектра на границе разрыва.

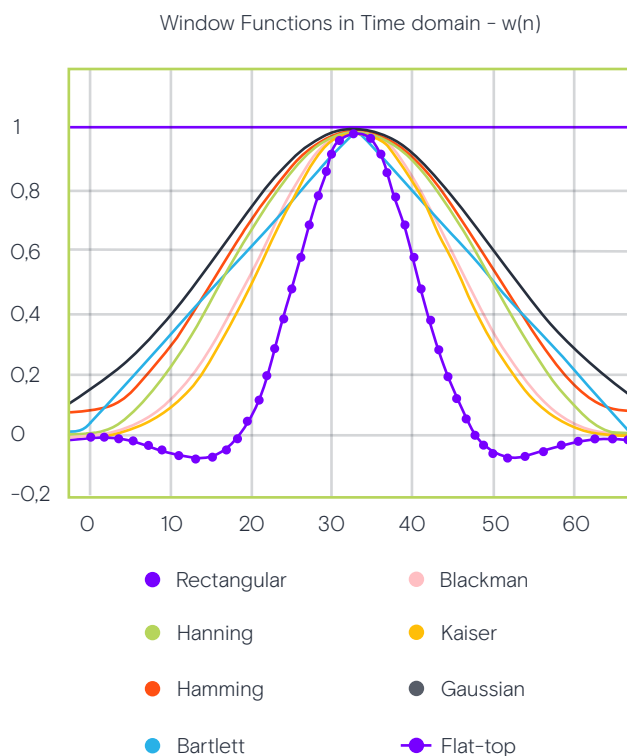


Рисунок 5. Пример некоторых оконных функций

В нашем случае мы используем самое обычное прямоугольное окно, так как вопрос контролирования боковых лепестков (частей сигнала на границах разрыва) актуален скорее для исключения дефектов сигнала при обработке аудио. В нашей задаче разрыв не влияет на данные. На практике это реализуется применением преобразования Фурье к окну в n дней с шагом в i дней. Мы брали $n = 30$ и $i = 15$ (в дальнейшем $i = 7$). Такие числа берутся из бизнес-контекста. В рабочем процессе есть основные периоды – месяц, две недели и неделя. В бизнес-контексте есть предположение, что будут доминировать именно гармоники, соответствующие таким периодам, поскольку они соответствуют периодам рабочих процессов. Например, обычная неделя → спринты → бухгалтерия за месяц. Ожидалось, что такая периодичность проявится и на тестовых данных (которые, напомним, представляют собой показатель внешней активности персоны).

В итоге мы получаем 8 спектров, со своими доминирующими гармониками. Но радоваться все еще рано. А вообще корректна ли такая игра со спектрами и частотами? Давайте это докажем. Формально нам нужно доказать следующее: вклад максимальных гармоник определяет норму (объем) исходной функции (показателя поведения).

У нас есть функция на дискретном множестве. Мы ее продолжаем на всю числовую прямую, ступеньками или отрезками соединяя значения в точках. Получаем интегрируемую с квадратом на всей прямой хорошую функцию f .

Такие функции образуют гильбертово пространство функций, интегрируемых с квадратом функций. На этом пространстве можно корректно задать линейный оператор – преобразование Фурье. В нашем случае функция начинается в нуле. Чтобы избавиться от комплекснозначности ее преобразования Фурье, мы допустим, что она принимает значения и при отрицательных значениях аргумента. Сделаем ее четной. В этом случае мнимая часть преобразования Фурье равна нулю и остается только косинус-преобразование.

Мы знаем, что по теореме Планшереля преобразование Фурье сохраняет норму функции. Сопряженное пространство образов преобразования Фурье (проще говоря, спектров) тоже представляет собой пространство интегрируемых с квадратом функций, поскольку преобразование Фурье является унитарным оператором.

Представим спектр в виде двух слагаемых (три макс. гармоники + остальные).

Их скалярное произведение равно 0, т. е. они ортогональны.

Также для L_2 справедливо равенство Парсеваля (аналог теоремы Пифагора для функций). Таким образом,

$$\begin{aligned} \|f\|_2 &= \|s\|_2 = \left\| \sum_{i=1}^3 X_i \right\|_2 + \left\| \sum_{i=4}^n X_i \right\|_2, \text{ где,} \\ \|f\|_2 &\text{ — норма исходной функции,} \\ \|s\|_2 &\text{ — норма спектра,} \\ \left\| \sum_{i=1}^3 X_i \right\|_2 &\text{ — норма трех максимальных гармоник,} \\ \left\| \sum_{i=4}^n X_i \right\|_2 &\text{ — норма остальных гармоник.} \end{aligned}$$

Следовательно,

$$\left\| \sum_{i=1}^3 X_i \right\|_2$$

прямо определяет вклад в исходную функцию. Что и требовалось доказать.



«По теореме Планшереля преобразование Фурье сохраняет норму функции»

Разобравшись с математикой, давайте посмотрим, как на самом деле эти гармоники описывают сигнал:

1) Выбираем в каждом окне по 3 гармоники с максимальным вкладом.

Для нашего примера они будут такие:

Номер окна	Номер гармоники	Период
1	1 5 10	2 недели, 6 дней, 3 дня
2	1 5 6	2 недели, 6 дней, 5 дней
3	1 3 5	2 недели, 10 дней, 6 дней
4	1 3 5	2 недели, 10 дней, 6 дней
5	1 2 3	2 недели, 15 дней, 10 дней
6	1 3 4	2 недели, 10 дней, 6 дней
7	1 3 4	2 недели, 10 дней, 6 дней
8	1 3 4	2 недели, 10 дней, 6 дней

2) Считаем процентный вклад трех максимальных гармоник от 100%.

3) Строим график динамики изменения процента вклада «по ходу скольжения» окна.

Динамика изменения вклада 3 максимальных гармоник

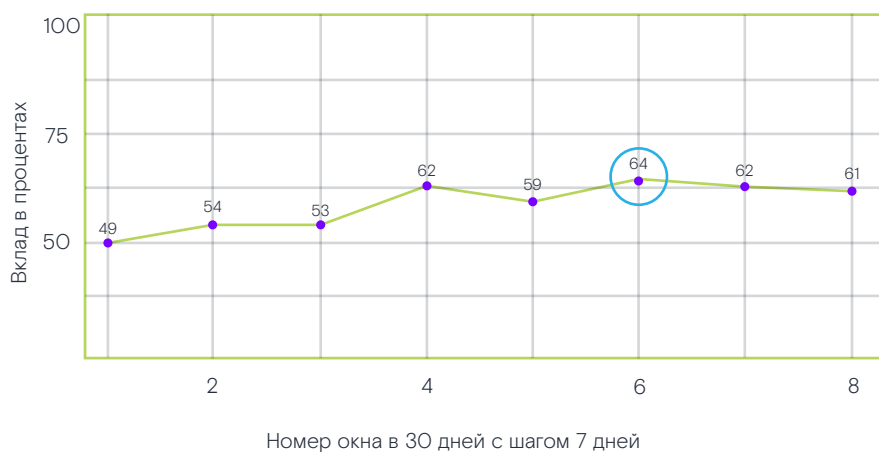


Рисунок 6. График динамики изменения процентного вклада 3 максимальных гармоник в сигнал

Мы видим, что в среднем процент вклада держится больше 50%. Наиболее выделяется окно с 64% под номером 6. Попробуем восстановить разложенный сигнал в данном окне по 1-й, 3-й и 4-й гармонике.

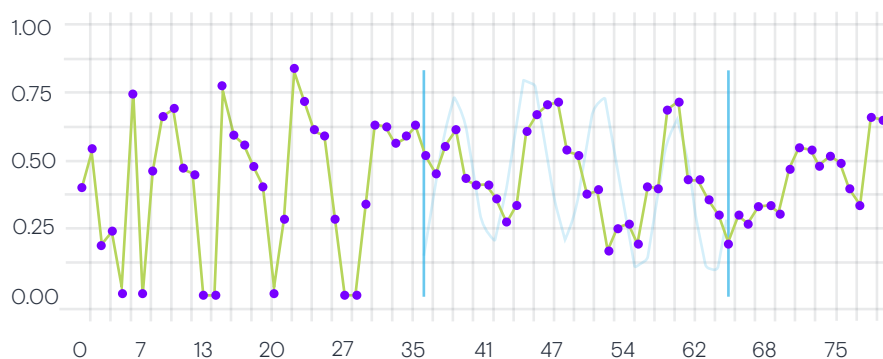


Рисунок 7. Построение графика поведения по максимальным гармоникам окна сигнала

Итак, на рисунке 7 мы видим сигнал, построенный по трем максимальным гармоникам, в наложении на реальный сигнал.

Где-то они совпадают достаточно точно, и пик активности сигнала трех максимальных гармоник совпадает с фактическими данными, где-то он пророчит пики, которых де-факто не случилось. Все же наша функция описывает сигнал лишь на 64%.

И наконец... Прогнозирование!

На основе полученной информации попробуем спрогнозировать поведение персоны. Прогнозировать можно было бы разными способами: брать 3 самые популярные гармоники по всем окнам сигнала, брать максимальные гармоники за период, вводимый вручную в зависимости от решаемой задачи (взгляд в будущее использование фичи), прогнозировать на две недели / месяц вперед... и так далее, очень много комбинаций временных промежутков, на которых брать гармоники и на которые прогнозировать.

В итоге мы остановились на гипотезе, которая заключается в следующем алгоритме:

- выбираем окно с максимальным процентным вкладом 3 максимальных гармоник,
- определяем по процентному вкладу, на какой период мы будем прогнозировать:

$$K = V \cdot W,$$

где K – количество дней, на которые будет строиться прогноз;
 V – наибольший процентный вклад трех максимальных по спектру гармоник; W – размер окна;

- строим функцию прогноза по 3 максимальным гармоникам выбранного окна.

В нашем случае входные данные таковы:

- «рабочее» окно – номер 6 (35–65 дни);
- максимальные гармоники – 1, 3 и 4 (2 недели, 10 дней, 6 дней);
- процентный вклад – 64%;
- период предсказания – 20 дней.

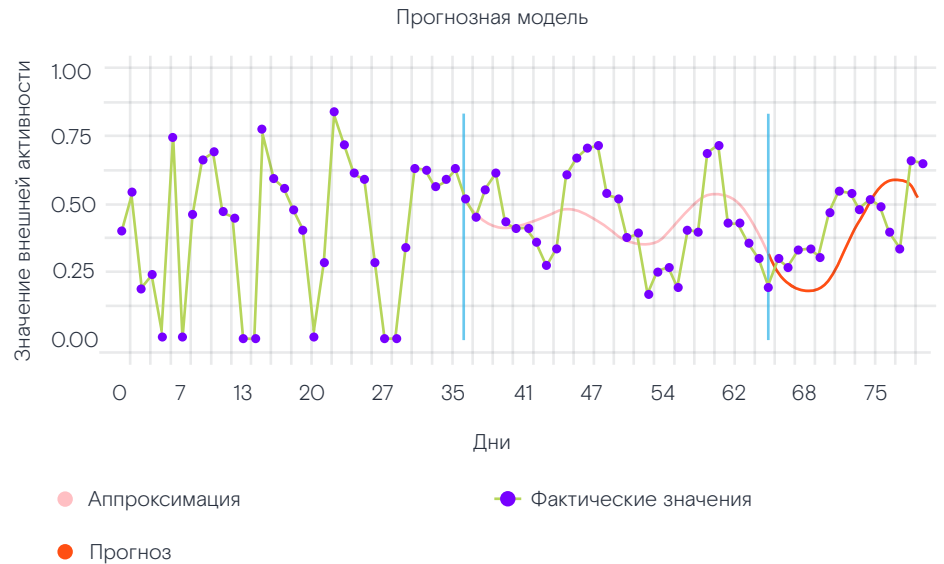


Рисунок 8. Фактические значения, аппроксимация и прогнозная модель

Для того чтобы оценить степень достоверности прогноза, посчитаем точность прогнозной модели. Точность рассчитываем по формуле:

$$\Delta = 1 - \sigma_{\text{ОПМ}} * 100\%,$$

где $\sigma_{\text{ОПМ}}$ — среднеквадр. отклонение ошибки прогнозной модели.

В нашем примере точность составила 80%. Таким образом, поведение, предсказанное моделью на 20 дней вперед, совпадает с реальными значениями на 80%.

Выводы

Мы разработали методику предсказания будущего поведения персоны с использованием методик спектрального анализа, в частности с использованием преобразования Фурье. Разумеется, нам есть куда расти, что усовершенствовать и что еще уточнить.



Автор: Максим Бузинов,
руководитель
исследовательской группы
Центра продуктов Дозор
компании «Ростелеком-Солар»



Автор: Татьяна Рябова,
аналитик Центра продуктов
Дозор компании
«Ростелеком-Солар»