Содержание:

ВВЕДЕНИЕ

В условиях рынка и конкуренции возникают проблемы, связанные с обеспечением безопасности не только физических и юридических лиц, их имущественной собственности, но и информации, имеющей коммерческое значение, других сведений, в частности о результаты интеллектуальной деятельности: секреты производства, служебные секреты и другие.

Информация - важнейший продукт общественного производства, постоянно наращиваемый ресурс человечества; сегодня это самый ценный и ходовой объект в международных экономических отношениях.

На международном уровне сформировалась система взглядов на информацию как на ценный ресурс жизнеобеспечения общества, который имеет социальное значение.

Информация, несомненно, является одним из самых ценных и одновременно уязвимых активов любой компании. Чем меньше людей имеет к ней доступ, тем большей ценностью обладает информация. В попытке обеспечить надлежащую защиту данных от любых угроз компаниям следует принимать все необходимые меры, которые позволят обеспечить их целостность и секретность. Одна из ключевых целей в связи с этим - предотвращения несанкционированного доступа и незаконном разглашения информации нынешними или бывшими сотрудниками.

Целью данной работы является обзор и анализ программных комплексов для анализа и защиты каналов утечки информации.

Для достижения поставленной задачи в работе необходимо решить следующие задачи:

- Проанализировать причины утечки конфиденциальной информации;
- Выполнить описание DLP-систем;
- Провести анализ существующих программных комплексов защиты от утечки данных.

1. Обеспечение доступа к конфиденциальной информации

1.1 Обзор и анализ основных причин утечки конфиденциальной информации

2016 год принес настоящий шквал инцидентов, связанных с конфиденциальной информацией, информационной безопасностью: от массового фишинга с использованием налоговой информации, брешей в WordPress, компрометации корпоративной электронной почты и DDoS-атак к подозрениям во «взломе» президентских выборов. При этом нет оснований считать, что в 2018-м ситуация улучшится - все может стать только хуже с учетом того, что злоумышленники продолжают развивать навыки социальной инженерии, находят новые способы подсовывать вредный продукт, взламывать уязвимые базы данных и с помощью мобильных технологий проникать в корпоративные сети и аккаунты частных лиц[1] .

По словам Дениса Макрушина, эксперта антивирусной компании «Лаборатории Касперского», количество направленных на бизнес атак программ-вымогателей и их отдельного вида – шифровальщиков - стремительно растет. Причем риску подвергаются практически все отрасли: образование, СМИ, финансы, шоу-бизнес, государственный сектор, производство, транспорт. особенно хотелось бы выделить здравоохранение - в 2016 году больницы стали популярной целью: например, медицинский центр в Голливуде заплатил 17000 долларов за разблокировку компьютеров; были атакованы несколько больниц в Германии и Великобритании.

Всего же с января по конец сентября 2016 количество атак на компании увеличилась в три раза: если в января 2016 года атаки делались в среднем каждые две минуты, то в сентябре 2016 года - уже каждые 40 секунд. В январе 2017 были сломаны серверы Министерства иностранных дел Королевства Таиланд, а также ряда других правительственных организаций, включая Министерство информации и коммуникационных технологий, Департамент налогов и сборов, Административный суд, Королевский флот и другие департаменты правительства Таиланда.

В результате утечки данных в сеть попала конфиденциальная информация о нескольких тысячах государственных служащих и соискателей работы, включая номера телефонов и банковских счетов, электронную почту и зашифрованные пароли. По данным издания Heakread.com, опубликованные в Интернете данные составляют всего 1% от общего количества украденных файлов[2]. В результате тайская армия планирует привлечь на службу «белых хакеров ». Кибервоины оказывать помощь правительства в борьбе с киберпреступностью и помогут улучшить систему безопасности государственных серверов, которая подверглась дискредитации многократными хакерскими атаками. Ежегодно «Лаборатория Касперского »проводит исследования, в ходе которого компании рассказывают что случилось с ними и о своих планах по информационной безопасности. Данные этого исследования свидетельствуют: от шифровальщиков страдают российские компании. При этом 15% организаций так и не смогли восстановить доступ к ценной информации.

Примечательно, что каждая пятая компания крупного бизнеса предпочла заплатить киберпреступникам выкуп, несмотря на то, что это не гарантировало возврат файлов[3].

Диана Соловьева, руководитель группы поддержки систем информационной безопасности компании ICL Services, считает, что для оперативного выявления атак нужны компетентные человеческие ресурсы.

Бизнесу необходимо больше инвестировать не в новые продукты, а в развитие компетенций сотрудников, которые смогут превращать эти многомиллионные «Модные игрушки» на инструменты, реально работают[4].

«У специалистов отрасли информационной безопасности гуляет такая шутка: все компании делятся на два типа: те, которые уже знают, что их взломали, и те, которых тоже сломали, но они об этом еще не в курсе». Раннее выявление, а тем более предотвращения инцидентов – это одна из актуальных и крайне тяжелых задач. Ее решение возможна при помощи поведенческого анализа Больших Данных, что представляется наиболее перспективным направлением, поскольку подобный функционал помогает выявлять аномалии, которые могут свидетельствовать о тех или иных ИБ-инцидентах.

В подтверждение вышесказанного можно привести пример ИБ-инцидента, который произошел в начале 2017 г .: утечка третьей серии четвертого сезона сериала «Шерлок» (Sherlock), который нелегально появился в Интернете 14 января 2017 - за

день до премьерного показа на телеканале BBC .

Как объясняет аналитический центр InfoWatch, число утечек информации растет во всем мире: за первые шесть месяцев 2018 года этот рост составил 16%[5], а в тройке лидеров по количеству утечек данных - США, Россия и Великобритания. В двух третях всех случаев утечки данных происходил по вине внутренних нарушителей.

Среди популярных телесериалов на Западе известны случаи утечек спойлеров и сценария к сериалу «Игра престолов» (Game of Thrones), а также фрагментов сериала «Ходячие мертвецы» (The Walking Dead).

Полуторачасовая серия «Шерлока» высокого качества не могла быть передана, например, по электронной почте из-за большого размера файла, но легко могла быть загружена на съемный носитель или загружена в облако, повлекшее утечку в силу даже непреднамеренных действий нарушителя.

Это подтверждает статистика аналитического центра InfoWatch: за последние три года доля утечек в результате случайных действий сотрудников организаций увеличилась на 34% до 79,7%.

На утечку данных через сетевой канал, включая отправление через браузер, приходится более половины всех случаев, растет доля утечек на съемных носителях.

С точки зрения вреда такая утечка могла сказаться на рейтинге показа серии, ведь часть зрителей уже видели ее в Интернете, а также привести к финансовым потерям и убыткам в аспекте имиджевой составляющей.

Сейчас большинство иностранных компаний выдвигают крайне жесткие требования по соблюдению соглашений о конфиденциальности, особенно если дело касается передачи исключительных прав на результаты интеллектуальной деятельности. Штрафы оговариваются заранее и могут доходить до сотен тысяч долларов. Подписывая такие соглашения, отечественные компании не могут не задумываться об обеспечении конфиденциальности полученных сведений.

Специфика обеспечения информационной безопасности в медиабизнесе такова, что в компаниях этой сферы, как правило, работают творческие люди, в немалом количестве используются мультимедийные данные больших размеров, а также тиражируются типовые ИТ-системы. Стандартные технологии защиты, которые

исторически применялись в медийном бизнесе, такие как использование «Слепого дубляжа», ограничения на доступ актеров озвучки ко всему материала, очередность предоставление серий правообладателем, так же как и традиционные методы охраны, сегодня уже не обеспечивают необходимой защищенности и технологии информационной безопасности могли бы в этом помочь.

Прошедший 2017 год стал поучительным для бизнеса в контексте информационной безопасности. Выражение «лучше один раз увидеть, чем сто раз услышать» — как раз о нем. Столкнувшись с вирусами-шифровальщиками, компании прочувствовали на себе важность элементарных правил ИБ-защиты. Отсутствие актуальных обновлений и привычка жить с уязвимостями привели к остановке заводов Renault во Франции, Honda и Nissan в Японии; пострадали банки, школы, энергетические, телекоммуникационные компании; только лишь одна компания Maersk потеряла 300 млн долларов. На фоне информационного цунами, вызванного вирусами-вымогателями, некоторые важные события остались за пределами массового внимания.

Злоумышленники начали перехватывать коды для двухфакторной аутентификации с помощью уязвимостей сигнального протокола SS7. Первыми пострадали абоненты O2-Telefónica. Киберпреступники стали подключаться к локальной сети банка и удаленно контролировать множество ATM, у банков появился серьезный повод для беспокойства. Весной 2017 года эксперты «Лаборатории Касперского» обнаружили сотни компьютеров в крупных компаниях, которые «майнили» криптовалюту для неизвестных взломщиков. Майнер использовал ту же уязвимость, что и WannaCry, и защищал от шифровальщика захваченные ПК. Не успел стихнуть шум вокруг безопасности IoT из-за ботнетов и DDoS-атак, как с помощью незащищенных «умных» кофемашин стали останавливать нефтехимические заводы, а смарт-аквариумы использовать для атак на казино. К концу года биткойн опередил по капитализации российский рубль, и хакеры сконцентрировали свое внимание на блокчейн-стартапах. Самая простая схема атаки стала наиболее популярной — найти уязвимости на сайте ICO и подменить адрес кошелька для сбора инвестиций. Израильский CoinDash таким образом лишился 7,5 млн $.

2017 год позволил выявить три основных тренда в области подходов к атакам на организации, которые будут весьма актуальны и в ближайший год. Всплеск популярности деструктивных массовых атак, когда злоумышленники нацелены на как можно более масштабный охват и причинение ущерба. Как это было, например, в случае с NotPetya, WannaCry (или другими шифровальщиками), которые

прокатились по миру в этом году. Иногда логика работы вредоносного ПО даже не подразумевала возможность расшифровывания данных, а используемые методы распространения были настолько эффективными, что позволили заражению в считанные часы распространиться по всей планете. Если в 2015–2016 годах подобных атак практически не было (исключением являлись, пожалуй, лишь атаки на IoT, например создание ботнета Mirai и DDoS-атаки, проводимые с его помощью), то в 2017 году, по экспертной оценке Positive Technologies, каждая 10-я организация столкнулась с вирусами-шифровальщиками. Использование инфраструктуры сторонних организаций для организации атак. Применявшийся ранее метод отправки писем с простой подменой адреса отправителя стал встречаться реже: большая часть фишинговых писем теперь блокируется спам-фильтрами на почтовых серверах. Поэтому злоумышленники изменили тактику и активно атакуют поставщиков и контрагентов компаний, для того чтобы использовать их инфраструктуру и учетные записи реальных сотрудников для развития атак. Подобная тактика уже использовалась злоумышленниками, например когда через инфраструктуру компании M.E.Doc нарушители распространили вирус NotPetya, который заблокировал рабочие станции во многих крупных организациях. Кроме того, подобный подход довольно часто использует группировка Cobalt, которая специализируется на атаках на финансовый сектор, производя взлом контрагентов банков, а уже потом от их имени осуществляя атаки на сами банки. Схожая ситуация сложилась и в истории с заражением вирусом BadRabbit, когда злоумышленники предварительно были нацелены на инфраструктуру легитимных новостных ресурсов, с которых далее происходила «раздача» вредоносного ПО. В среднем каждая вторая успешная атака на организацию, которую расследовал экспертный центр безопасности компании Positive Technologies в течение 2017 года, была проведена через скомпрометированный «ранее надежный» источник.

Можно доверять собственному персоналу, но контроль рабочей деятельности сотрудников должен осуществляться на уровне, адекватном рискам нарушения информационной безопасности, которые достаточно высоки. Минимально необходимые действия для защиты содержат введение систем мониторинга информационных потоков и предотвращения утечек данных. Это суровая рекомендация международных стандартов и лучших практик в сфере обеспечение информационной безопасности[6].

Утечка информации несет в себе те или иные негативные экономические последствия для компании. С этим мнением согласны и представители индустрии

информационной безопасности, которые говорят о том, что безвредных утечек данных не бывает – любая из них несет в себе вред для бизнеса, если не сейчас, то в будущем. Иногда достаточно трудно предсказать, где и когда «выстрелят» те документы, которые инсайдеры вынесли из вашего офиса сегодня.

Бывает, что проходит несколько месяцев или даже несколько лет, прежде чем информация сделает свое черное дело, попав, например, на глаза журналистам или конкурентам. Именно поэтому очень важно защищать данные комплексно, а не делить их на более важные и менее важные.

Информация, не предназначенная для публики, должна оставаться закрытой. А это значит, что ее следует защитить от возможных утечек.

В общем все каналы утечки можно разделить на две группы. К первой относятся злонамеренные похищения информации, к ним можно отнести все инсайдерские риски, то есть когда человек, группа людей или даже сами сотрудники компании пытаются похитить конфиденциальную информацию, преследуя при этом свои корыстные цели. Вторая группа - это утечка через неосторожность или ошибку со стороны сотрудников.

Как показывает практика, именно второй вариант чаще всего встречается. Конечно же, это ни в коем случае не говорит о том, что об угрозе инсайдеров или шпионаж конкурентов можно забыть.

За последние несколько лет сформировались несколько основных причин потери данных. Поэтому защита от утечки информации фокусируется в основном на них, не забывая при этом о других приемах хищения данных [6].

1. Потеря незащищенных носителей, то есть дисков, флешек, карт памяти, ноутбуков и тому подобное.

2. Случайные заражения программами-шпионами во время некорректного обращения с Интернетом, выхода без наличия защищенного доступа или подключения устройств, которые были ранее заражены.

3. Возникновение технических ошибок при работы с секретными и конфиденциальными данными, в случае их публикации в Интернете и тому подобное.

4. Отсутствие ограничений доступа к данным для сотрудников компании.

5. Атаки со стороны злоумышленников, которые пытаются проникнуть в систему, заразить вирусами тому подобное.

Сегодня специалисты предлагают защищать информацию с помощью системы DLP – Data Leak Prevention (предложено агентством Forrester в 2005 г.).

В рамках создания системы DLP решаются такие задачи:

- предотвращение утечек конфиденциальной информации по основным каналам передачи данных

- веб-трафик, следует (HTTP, FTP, P2P и др.)

- электронная почта общая, корпоративная (внутренняя)

- системы быстрого обмена сведениями, сетевая и локальная печать;

- контроль за доступом к устройствам и портам ввода-вывода, к которым относятся: дисководы, CD-ROM, USB-устройства, инфракрасные, принтерные (LPT) и модемные (COM) порты.

Как показывают опубликованные данные опроса Deloitte ведущих мировых финансовых компаний, 49% респондентов зафиксировали внутренние инциденты (связанные с IT-безопасностью) за последние 12 месяцев. В 31% случаев инсайдеры занесли вирусы изнутри корпоративной сети, а с инсайдерским мошенничеством столкнулись 28% респондентов, 18% организаций стали жертвами утечки частной информации клиентов, а 10% обнаружили, что инсайдеры скомпрометировали корпоративную сеть.

Организации, которые пострадали от внутренних утечек, признаются, что большая часть угроз является следствием безалаберности или халатности служащих (Человеческий фактор - 42%, операционные ошибки - 37%), а не злого умысла инсайдеров. Правда, 28% стали жертвой тщательно продуманного и профессионального мошенничества, а 18% компаний лишились частной информации клиентов именно потому, что инсайдеры целенаправленно допустили утечку. Чтобы не допустить такие инциденты в будущем, 80% опрошенных финансовых компаний осуществляют мониторинг действий служащих, а 75% вводят различные ограничительные мероприятия на использование тех или иных

технологий и устройств [6].

Поэтому современные вызовы информационной безопасности, конфиденциальной информации обусловлены не только внешними факторами, которые характеризуются попыткой субъектов влиять на информационное пространство с целью обеспечения собственных интересов, но и внутренними.

Каналы утечки конфиденциальной информации

Потеря информации предполагает незаконный переход конфиденциальных сведений к лицу, которое не имеет права использовать эти сведения в своих целях для получения прибыли или передачи другому лицу. В том случае, когда потеря информации происходит по вине персонала - потеря информации обозначается термином разглашение или огласка информации.

Разглашение информации всегда осуществляется человеком устно, письменно, с помощью жестов, мимики, условных сигналов. Термин "утечка информации" в большей степени касается потери информации за счет ее перехвата с помощью технических средств разведки.

Потеря информации возможна при наличии каналов разглашение или утечки. Канал потери информации означает переход ценных сведений от законного источника, во-первых или непосредственно, к конкуренту или злоумышленнику, во-вторых, к третьему лицу в несанкционированном режиме.

Под третьим лицом понимаются любые лица, которые получили знания конфиденциальной информации в силу обстоятельств или в результате безответственности персонала следует учитывать, что эти лица не заинтересованы в полученной информации. Переход информации к третьему лицу образует случайный или стихийный канал потери информации в результате:

1) потери документов или конфиденциальных записей;

2) незнание или игнорирование персоналом фирмы требований по защите информации;

3) излишняя болтливость сотрудников с коллегами по работе, другими лицами в местах общего пользования, в транспорте и т.д.;

4) работы с конфиденциальными документами при посторонних лицах за счет несанкционированной передачи их другому сотруднику;

5) в результате наличия в документах излишней конфиденциальной информации;

6) в результате самопроизвольного копирования сотрудником документов в служебных или коллекционных целях.

В отличие от третьего лица злоумышленник целенаправленно пытается получить конкретную информацию и поэтому намеренно и тайно находит или формирует канал разглашение или утечки информации. Каналы потери конфиденциальной информации делятся на организационные и технические.

Организационные каналы разглашения информации, основанной на установлении различных, в том числе законных отношений с фирмой или сотрудником фирмы для последующего несанкционированного доступа к интересующей злоумышленника информации. Основными видами организационных каналов могут быть:

- устройство злоумышленника на работу в фирму, как правило, на техническую, вспомогательную или второстепенную должность;

- установление злоумышленником доверительных взаимоотношений с сотрудником фирмы или лицами, имеющими право свободного доступа к информации в данной фирме;

- криминальный, силовой доступ к информации, то есть кража документов, дел, дискет, дисков, компьютеров, шантаж к сотрудничеству отдельных работников, подкуп работников, инсценировка экстремальных ситуаций;

- получение информации из случайного канала.

Утечка конфиденциальной информации - это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе, известна в процессе работы. Эта утечка может быть следствием;

- разглашение конфиденциальной информации;

- ухода информации по различным, главным образом техническим, каналам;

- несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем является умышленными или неосторожными действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе

или по работе, которые привели к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

Несанкционированный доступ - это противоправное умышленное овладение конфиденциальной информацией лицом, которое не имеет права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

- перехват электронных излучений;

- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей частоты;

- применение подслушивающим устройств (закладок);

- дистанционное фотографирование;

- перехват акустических излучений и восстановление текста принтера;

- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;

- копирование носителей информации с преодолением мер защиты;

- маскировка под зарегистрированного пользователя;

- маскировка под запросы системы;

- использование программных ловушек;

- использование недостатков языков программирования и операционных систем;

- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ к информации;

- преступный вывод из строя механизмов защиты;

- расшифровка специальными программами зашифрованной информации;

- информационные инфекции.

Перечисленные пути несанкционированного доступа требуют достаточно больших технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Например, технические каналы утечки - это физические пути от источника конфиденциальной информации к злоумышленнику, посредством которых возможно получение охраняемых сведений.

Причиной возникновения каналов утечки являются конструктивные и технологические несовершенства схемных решений или эксплуатационный износ элементов. Все это позволяет взломщикам создавать действующие на определенных физических принципах преобразователи, образующие присущий этим принципам канал передачи информации - канал утечки.

Однако есть и достаточно примитивные пути несанкционированного доступа:

- хищение носителей информации и документальных отходов;

- инициативное сотрудничество;

- склонение к сотрудничеству со стороны взломщика;

- выспрашивание;

- подслушивание;

- наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для пользователей. Менеджерам следует помнить, что довольно значительная часть причин и условий, создающих предпосылки и возможность не правомочного овладения конфиденциальной информацией, возникает из-за нескольких элементарных недоработок руководителей организаций и их сотрудников. Например, к причинам и условиям, создающим предпосылки для утечки коммерческих секретов, могут относиться следующие:

- недостаточное знание работниками организации правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения;

- использование не аттестованных технических средств обработки конфиденциальной информации;

- слабый контроль за соблюдением правил защиты информации правовых, организационных и инженерно-технических мер;

- текучка кадров, в том числе, владеющих сведениями, составляющими коммерческую тайну;

- организационные недоработки, в результате которых виновниками утечки информации являются люди - сотрудники ИС.

Большинство из перечисленных технических путей несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализованной на практике системе обеспечения безопасности. Но борьба с информационными инфекциями представляет значительные трудности, так как существует и постоянно разрабатывается огромное количество вредоносных программ, цель которых - порча информации в БД и ПО компьютеров. Большое количество разновидностей этих программ не позволяет разработать постоянные и надежные средства защиты против них.

Технические каналы утечки информации возникают при использовании злоумышленником специальных технических средств разведки, которые позволяют получать защищенную информацию без непосредственного контакта с источником этой информации. Основными видами этих каналов являются акустические, электромагнитные и визуально-оптические акустические каналы, связанные с образованием акустического поля, возникающего при наличии звуковой волны. Канал образуется в кабинетах, офисах, строительных конструкциях, вентиляционных шахтах; при вибрации стекла в окнах, перегородок в помещениях, дверей и т.д. Акустический канал образуется за счет микрофонного эффекта, при котором появляются посторонние и ритмические сигналы. Эти сигналы обусловлены механическим воздействием звуковой волны. Канал образуется в динамиках радиотрансляции, элементах телефонных сетей, а также в холодильниках, электрозвонках и т.д.

Электромагнитные каналы утечки информации возникают в линиях радиосвязи при работе радиотелефонов, бытовых приборах аудио-, видеотехники и любой вычислительной техники.

Визуальный или визуально-оптический канал образуется за счет наблюдения за объектом, в том числе с помощью оптических приборов фото- и видеоаппаратуры.

2. Системы анализа и предотвращения утечки конфиденциальных данных

2.1. Системы защиты от утечки конфиденциальных данных (DLP)

Эффективность бизнеса во многом зависит от сохранения конфиденциальности, целостности и доступности информации. В настоящее время одной из наиболее актуальных угроз в сфере информационной безопасности является утечка конфиденциальных данных от несанкционированных действий пользователей.

Это обусловлено тем, что большая часть традиционных средств защиты, таких как антивирусы, межсетевые экраны и системы аутентификации не способны обеспечить эффективную защиту от внутренних нарушителей. Целью такого рода нарушителей (инсайдеров) является передача информации за пределы компании с целью дальнейшего несанкционированного использования - продажи, опубликования ее в открытом доступе и т.д.

Системы DLP это технологии, позволяющие предотвратить утечку конфиденциальной информации. В течении последних нескольких лет использовалась различная терминология: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) и др. Но окончательным и наиболее точным термином принято считать Data Leak Prevention (DLP, предложенный агентством Forrester в 2005 г.). В качестве российского аналога принято словосочетание «системы защиты конфиденциальных данных от внутренних угроз». При этом под внутренними угрозами подразумевают как умышленные, так и неумышленные злоупотребления сотрудниками своими правами доступа к данным.

В DLP-системах обычно используются три метода идентификации: вероятностный, детерминистский и комбинированный. Системы, основанные на первом методе, в основном используют лингвистический анализ контента и «цифровые отпечатки»

данных. Такие системы просты в реализации, но недостаточно эффективны и характеризуются высоким уровнем ложных срабатываний. Системы, использующие детерминированный подход (метки файлов), очень надежные, но им не хватает гибкости. Комбинированный подход сочетает оба метода с аудитом среды хранения и обработки данных, что позволяет достичь оптимального решения проблемы защиты конфиденциальности информации.

2.2. Анализ передаваемой информации

На данный момент на рынке представлено довольно много DLP-решений, которые позволяют идентифицировать и предотвращать утечку конфиденциальной информации с определенного канала. Однако действительно сложных решений, которые охватывают все существующие каналы, значительно меньше. В этих условиях чрезвычайно важно выбрать технологию, обеспечивающую защиту источников конфиденциальной информации с максимальной эффективностью и минимальным количеством ложных срабатываний. Первое, что нужно учитывать при выборе DLP -решения - как это решение анализирует переданную информацию и какие технологии используются для определения доступности конфиденциальных данных.

Всего существует пять методов анализа:

1. Поиск по словарям (точным соответствием слов, в некоторых случаях, с учетом морфологии).

2. Регулярные выражения. Регулярные выражения - система анализа текстовых фрагментов по формализованным шаблоном на основе системы записи образцов для поиска. Например, номера кредитных карт, телефоны, адреса электронной почты, номера паспортов, лицензионные ключи и т.д.

3. Сравнение типов файлов. Политика безопасности может запретить отправку некоторых типов файлов. В то же время, если пользователь изменяет расширение файла, системе все равно необходимо «распознать» тип файла и выполнить необходимые действия. Большинство решений используют технологию автономии.

4.· Статистический («поведенческий») анализ пользовательской информации. Если у пользователя есть доступ к конфиденциальной информации, и в то же время он посещает определенные сайты (веб-хранилище, веб-почту и т.д.), то он попадает в

«группу риска», и можно применить дополнительные ограничительные политики безопасности.

5. Технология цифровых отпечатков. Наиболее перспективные и довольно сложные технологии, на которых сделаны определенные математические преобразования исходного файла (алгоритмы преобразований производителей не разглашаются). Процесс преобразования строится следующим образом: исходный файл - математическая модель файла - цифровой отпечаток. Такой процесс может значительно сократить объем обрабатываемой информации (объем цифрового отпечатка не более 0,01 от размера файла). Затем цифровые отпечатки помещаются в базу данных (Oracle, MS SQL) и могут дублироваться в ОЗУ устройства, которое выполняет анализ информации. Затем отпечатки используются для сравнения и анализа передаваемой информации. В то же время отпечатки переданных и «образцовых» файлов могут не совпадать обязательно на 100%, процентное совпадение может быть задано (или запрограммировано производителем программного обеспечения). Технологии устойчивы к редактированию файлов и применимы к защите практически любого типа файлов: текстового, графического, аудио, видео. Количество «ложных срабатываний» не превышает одного процента (все остальные технологии дают 20-30% ложных срабатываний). Эта технология устойчива к различным текстовым кодировкам и языкам, используемым в тексте.

Также необходимо обратить внимание на систему отчетности и наборы предварительно разработанных политик безопасности, предоставляемых решением DLP, поскольку это поможет избежать некоторых проблем и трудностей при реализации.

2.3. Критерии оценки DLP – систем

Существует четыре критерия оценки продуктов DLP, сформулированных компанией Forrester Research.

Первый критерий - многоканальность. Решение DLP не должно быть сосредоточено только на одном канале утечек. Это должно быть комплексное решение, охватывающее максимальное количество каналов: e-mail, Web и IM, а также мониторинг файловых операций.

Второй критерий - унифицированный менеджмент. Система должна иметь унифицированные средства управления всех компонентов, которые она в себя включает. Их, как правило, три: менеджмент-сервер, на котором хранятся политики групп пользователей; устройство, которое отслеживает утечку через сеть; агенты для рабочих станций, серверов, файловых-хранилищ. Главное требование второго критерия - возможность управлять этими тремя компонентами с одной консоли.

Третий критерий - активная защита. Система должна не только фиксировать утечку конфиденциальной информации, но и давать возможность ее блокировать.

Четвертый критерий - классификация информации с учетом, как содержания, так и контекста. Утечка конфиденциальной информации должен базироваться не только на содержании информации, пересылаемой, но и на контексте, в котором она происходит: используемый протокол, приложение, от которого пользователя, куда и т.д.

2.4. Обзор существующих DLP – систем

В сравнении принимали участие:

- Securit ZGate;
- InfoWatch Traffic Monitor;
- Symantec Data Loss Prevention;
- Search Inform Контур безопасности;
- FalconGaze SecureTower.

DLP-система Securit Zecurion Zgate (рис.1) предназначена для предотвращения утечки конфиденциальной информации по электронной почте, социальным сетям, интернет-пейджерам и любым другим каналам передачи данных по сети.

Securit Zecurion Zgate позволяет отслеживать и архивировать:

- переписка в корпоративной электронной почте;
- письма и вложения, отправленные через службы электронной почты;
- общение в социальных сетях, форумах и блогах;
- сообщения пейджера в Интернете;
- файлы, переданные по FTP.

Zecurion использует гибридный анализ для обнаружения конфиденциальных данных в сообщениях, комплекс современных технологий обнаружения, которые точно определяют уровень конфиденциальности передаваемой информации и категории документов с учетом характеристик бизнеса, требований отраслевых стандартов и законов России, СНГ, Европе и США. Использование гибридного анализа позволило повысить эффективность обнаружения в среднем на 60-70% для существующих DLP-систем до 95% для Zecurion Zgate.

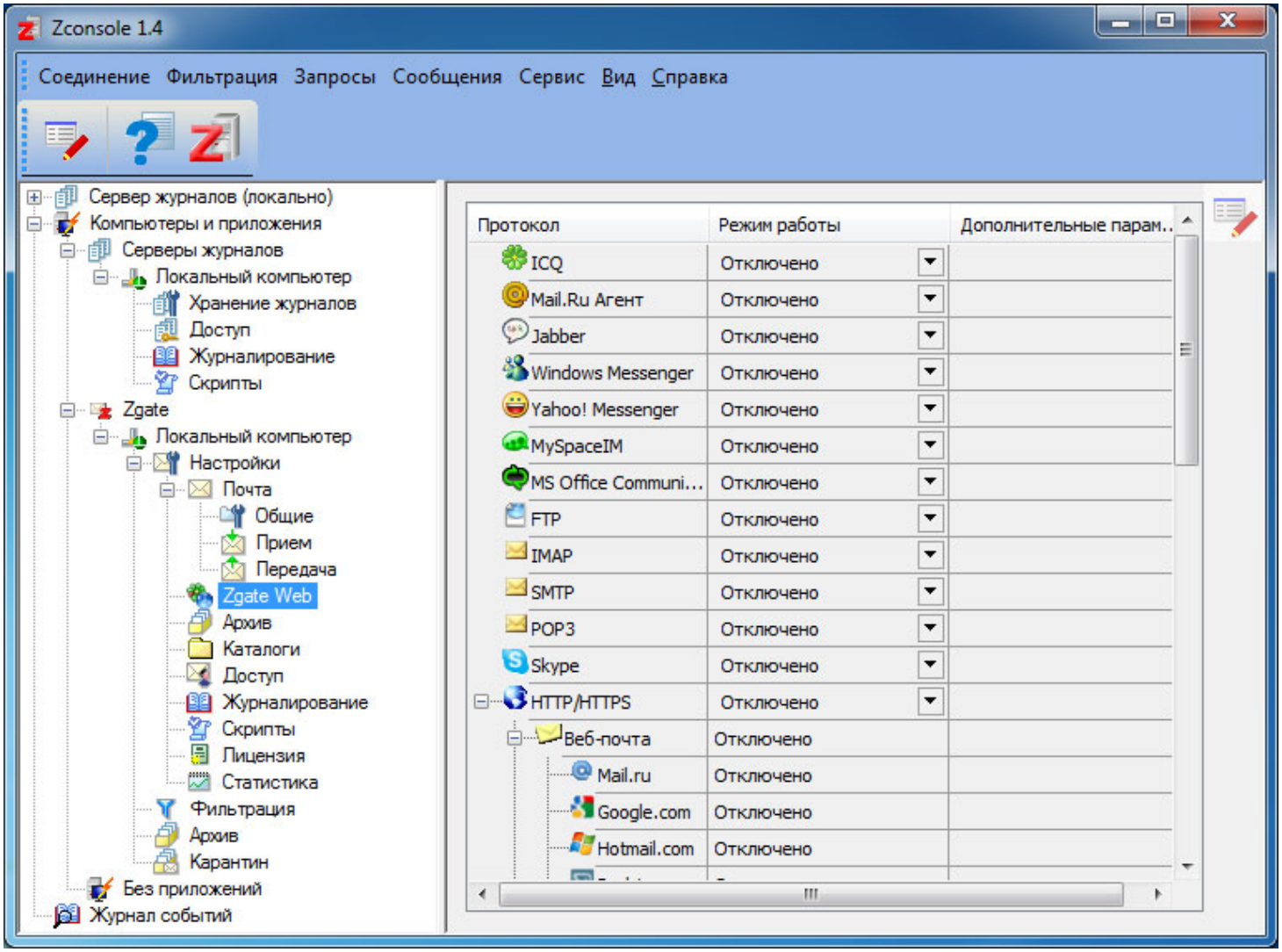

Рисунок 1. - SecurIT Zgate 3.0

InfoWatch Traffic Monitor (рис.2) - это высокотехнологичное интегрированное решение, которое защищает организации от действий внутренних злоумышленников и обеспечивает надежную защиту корпоративных данных от преднамеренных или непреднамеренных утечек (несанкционированное распространение). Технологии InfoWatch позволяют рассматривать все документы клиента, делить их на категории, структурировать информационные активы,

идентифицировать конфиденциальные данные из большого объема информации. Концепция InfoWatch заключается в управлении перемещением информации на всех этапах: от аудита, для определения маршрутов трафика контента и хранения информации (от кого, какая категория данных передается или хранится) до контроля распространения конфиденциальной информации с использованием DLP-системы и настроенных политик информационной безопасности.

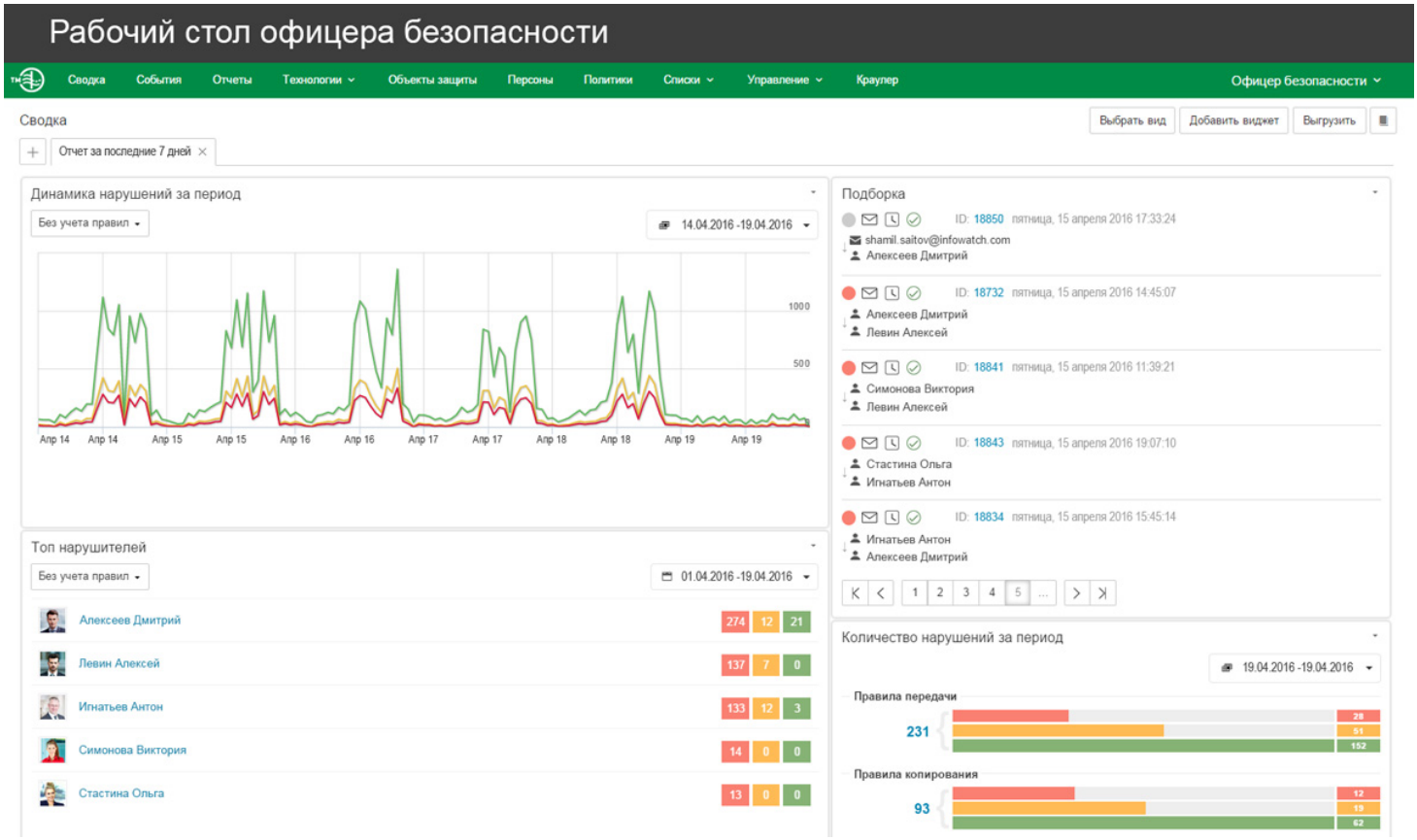

Рисунок 2. - InfoWatch Traffic Monitor

Symantec Data Loss Prevention (рис.3) — комплексное решение для обнаружения и предотвращения утечки информации, призванное помочь в формировании корпоративной культуры обработки конфиденциальной информации, обучать сотрудников существующим правилам обработки и передачи информации внутри организации и за ее пределами , уменьшить количество случайных утечек и облегчить обнаружение и расследование намеренного.

Symantec Data Loss Prevention обеспечивает защиту информации обо всех ресурсах ИТ-инфраструктуры компании:

- отслеживание и блокирование перемещения информации как внутри организации, так и за ее пределами;

- обнаружение конфиденциальной информации в открытом доступе в хранилищах файлов, веб-серверах, базах данных, почтовых системах обмена и рабочем процессе;
- защита конфиденциальной информации на рабочих станциях и ноутбуках, в том числе находящихся за пределами корпоративной сети;
- контроль мобильных приложений, облачных и веб-сервисов, а также полученных и отправленных сообщений на смартфонах и планшетных компьютерах.

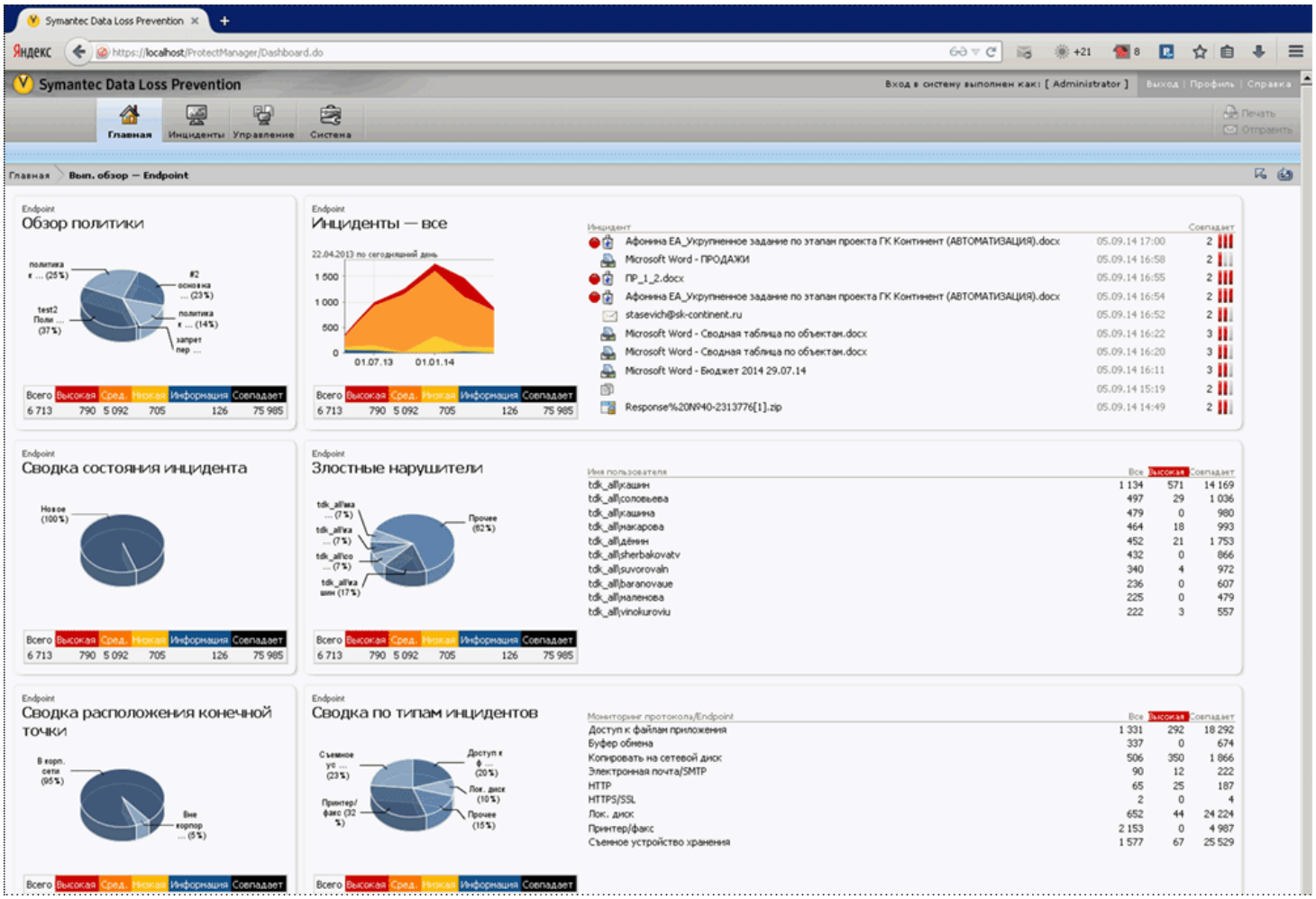

Рисунок 3. - Symantec Data Loss Prevention

«Контур информационной безопасности SearchInform» (рис.4) предназначен для управления потоками информации в локальной сети. Мониторинг возможен двумя способами, в зависимости от используемого серверного компонента: SearchInform EndpointSniffer или SearchInform NetworkSniffer. Серверные компоненты - это платформы, на которых работают модули перехвата. Каждый модуль перехвата действует как анализатор трафика и контролирует его канал передачи данных.

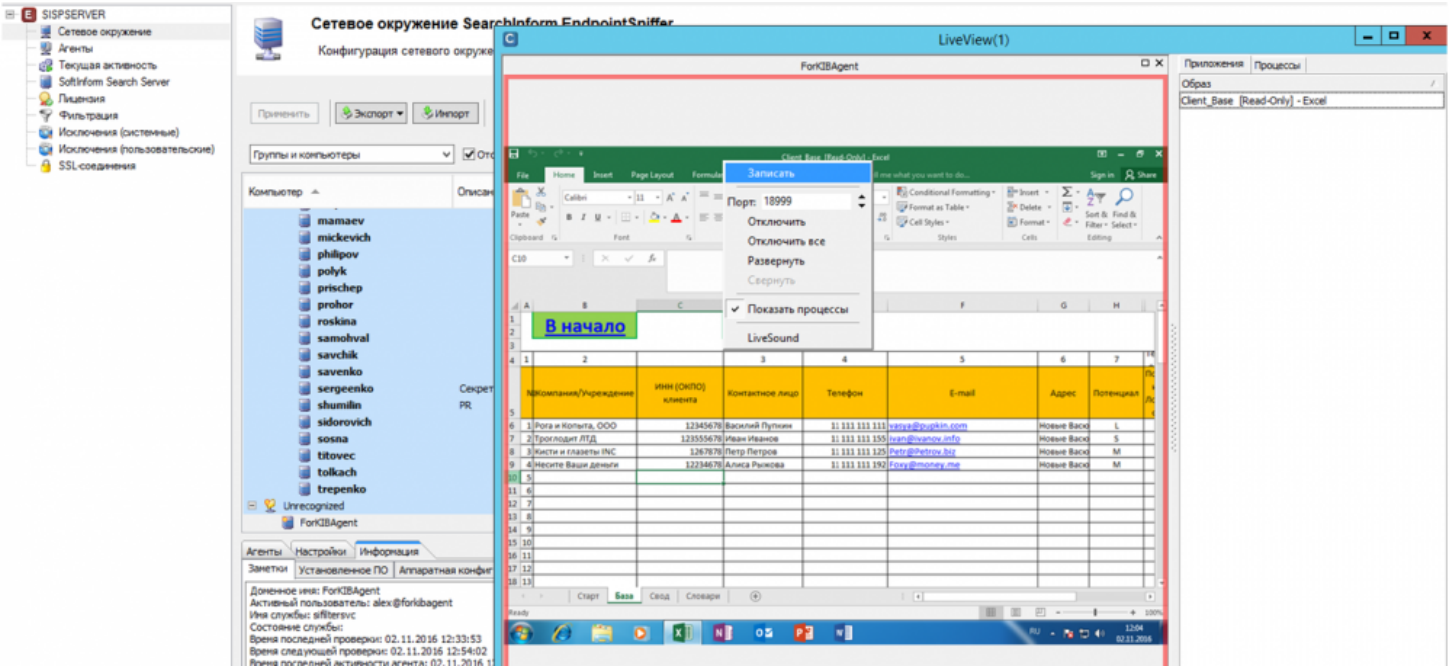

Рисунок 4. - Search Inform Контур безопасности

SearchInform EndpointSniffer - платформа для перехвата и блокировки информационных потоков через агентов, установленных на рабочих станциях (рис.5). Платформа Endpoint позволяет перехватывать информацию с помощью агентов, установленных на ПК сотрудников. Интернет, корпоративная и личная электронная почта, все популярные мессенджеры (Viber, ICQ и т. Д.), Skype, облачное хранилище, FTP, Sharepoint, печать документов на принтеры, использование внешних устройств хранения данных. Мониторинг файловой системы ПК, процессы и сайты активны, информация, отображаемая на мониторах ПК и захваченная микрофонами, нажатые клавиши, удаленный онлайн-мониторинг ПК. Кроме того, агент позволяет вам зашифровать любые пользовательские данные, которые записываются на носитель. Доступны как открытые, так и зашифрованные соединения. Вы можете установить запрет на использование портов ввода-вывода или определенных устройств. Кроме того, система реализует защиту локальных ресурсов. Функциональность позволяет вам регулировать доступ к критическим данным: скрывает / закрывает верхние папки управления, запрещает доступ к информации даже для привилегированных пользователей (системных администраторов, техников и т. Д.). Доступ к ресурсам (папкам и дискам) ограничен только уровнем DLP и не может быть отменен ни на системном уровне, ни на уровне домена. Агенты SearchInform EndpointSniffer делают теневую копию перехваченной информации и отправляют полученные данные на сервер SearchInform EndpointSniffer. Сервер помещает перехваченные данные в базу данных под управлением Microsoft SQL Server. Рисунок 2. Типичная схема работы

SearchInform EndpointSniffer SearchInform NetworkSniffer - платформа для перехвата и блокировки информационных потоков на сетевом уровне. SearchInform NetworkSniffer позволяет работать с зеркальным трафиком, прокси-серверами (ICAP или ISA \ TMG), почтовыми серверами (интеграция почтовых ящиков (POP3, IMAP, EWS), SMTP, транспортные правила или ведение журнала), другое корпоративное программное обеспечение, например Lyns. Перехват сетевого трафика выполняется на уровне сетевых протоколов (Mail, HTTP, IM, FTP, Cloud). Возможна фильтрация по доменному имени пользователя, имени компьютера, IP- и MAC-адресам. Перехваченные сообщения помещаются в базу данных SQL.

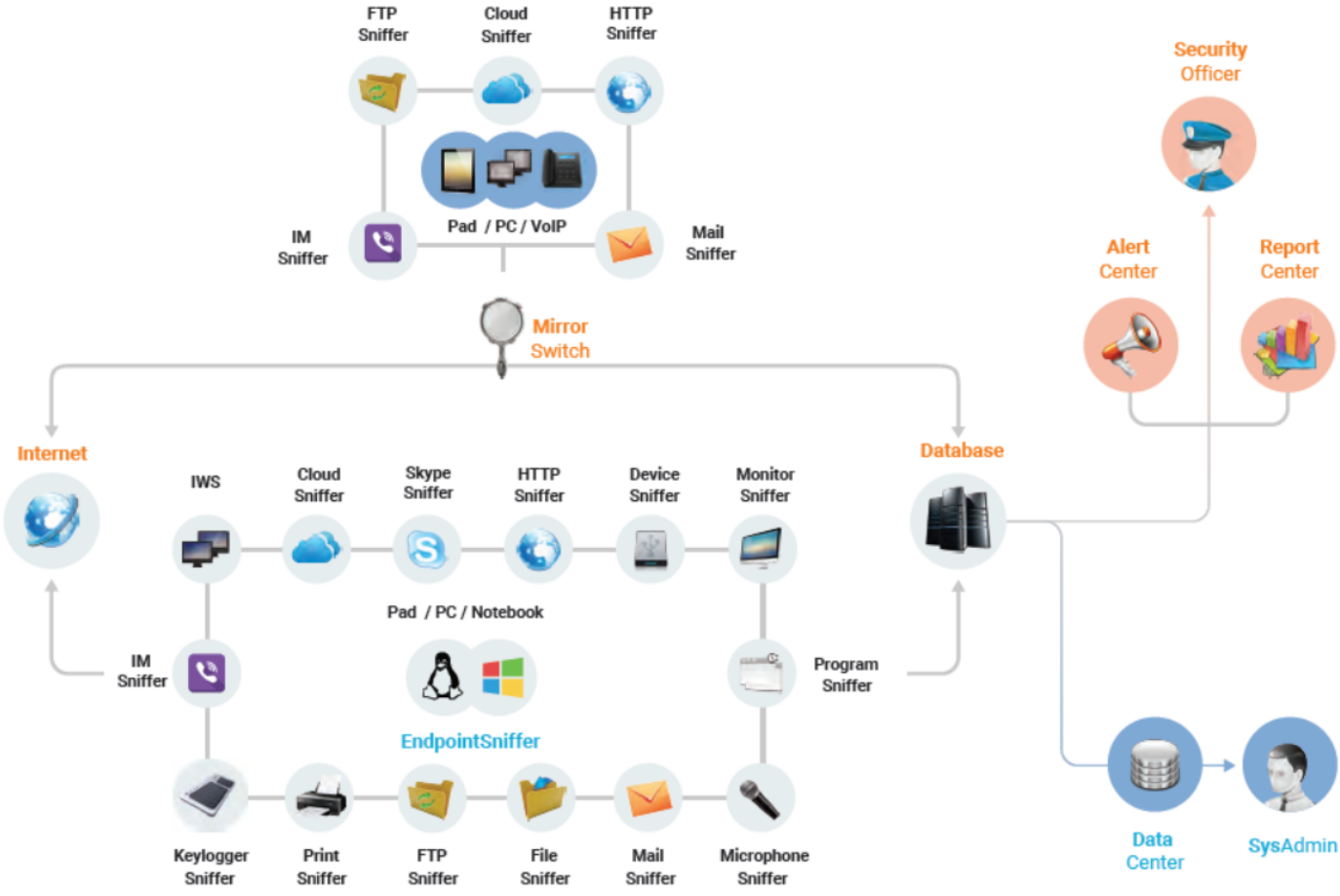

Рисунок 5. – Архитектура Search Inform Контур безопасности

DLP-система SecureTower 6.0 (рис. 6) компания Falcongaze перехватывает и анализирует сетевой трафик, передает данные на внешние устройства, сетевые ресурсы, локальные и сетевые принтеры, а также контролирует содержимое буфера обмена, историю нажатия клавиш на клавиатуре, входящие и исходящие сообщения электронной почты, корреспонденции и голосовые вызовы в самых популярных мессенджерах, переданные документы, файлы, веб-страницы и многое

другое. Одной из основных функций DLP-системы является противодействие внутренним угрозам. Инсайдерская деятельность часто недооценивается, однако на нее приходится львиная доля утечек. Основные функции: SecureTower 6.0 обеспечивает: полный контроль документооборота и перехват данных в информационных каналах. Система перехватывает все отправленные и принятые сообщения, идентифицирует отправку конфиденциальных документов, контролирует принтеры и подключенные устройства (например, устройства USB), контролирует почтовые серверы, мониторы, контролирует использование облачного хранилища. Гибкая система для создания правил безопасности и многое другое; контроль действий персонала. Система предоставляет графический анализатор, в котором для каждого сотрудника система создает профиль, который может импортировать данные из ActiveDirectory и автоматически генерировать из перехваченной информации. В этом профиле отображаются сообщения сотрудников с другими людьми, адреса электронной почты сотрудников, имена в мессенджерах, учетные записи в социальных сетях и других сайтах. Кроме того, постоянный веб-мониторинг посещаемых сайтов и активность в социальных сетях. Можно получать профили и полную историю общения сотрудников; Определение передачи конфиденциальной информации с помощью различных методов анализа. Метод контроля над цифровыми отпечатками позволяет идентифицировать совпадения (даже фрагментарные) в потоке информации с конфиденциальными документами. Также SecureTower позволяет идентифицировать в документах и корреспонденции регулярные выражения (такие как номера кредитных карт, TIN, данные паспорта и т. Д.) И анализировать тематические словари. Во время анализа система учитывает морфологические особенности русского языка, распознает транслитерацию, определяет формат «маскированного» файла, а также анализирует текст, распознанный на изображениях. сбор данных для расследования инцидентов. В дополнение к предотвращению инцидентов, связанных с безопасностью, система также используется в качестве средства для расследования причин и обстоятельств утечки данных. SecureTower 6.0 предоставляет все необходимые инструменты для расследования инцидентов в горячем поиске. В связи с тем, что система хранит все сообщения и действия сотрудников в архиве, она позволяет в кратчайшие сроки идентифицировать виновного, определять наличие намерения и определять дальнейшие действия руководства. Данные, собранные системой, могут быть приняты судами в качестве доказательств; контроль мобильных рабочих станций.

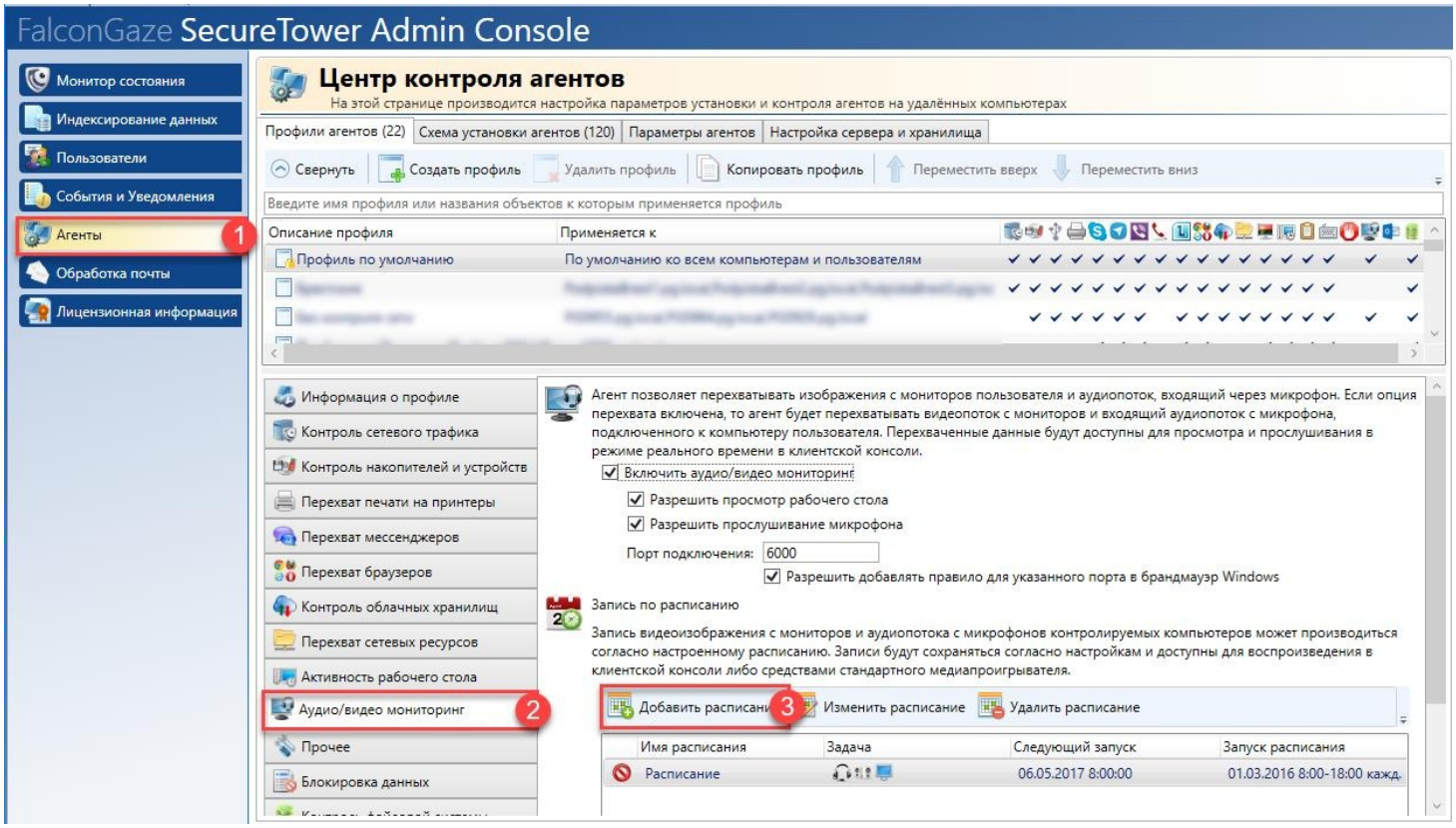

Рисунок 6. – Falcongaze SecureTower 6.0

В SecureTower 6.0, как и в предыдущих версиях системы, реализован метод удаленного контроля рабочих станций. Агент в автономном режиме снимает те же данные, что и в стационарных компьютерах, а после подключения устройства к корпоративной сети отправляет собранный архив на сервер; гибкую систему формирования отчетности. Для сотрудников службы безопасности и руководителей структурных подразделений доступны полностью настраиваемые отчеты по инцидентам безопасности и ежедневной работе сотрудников. Можно настроить автоматическое создание отчетов по расписанию и отправку их на электронную почту. SecureTower 6.0 позволяет осуществлять автоматическую репликацию данных из филиалов на центральный сервер в головном офисе, что упрощает большим организациям с распределенной структурой обработку и хранение перехватываемой информации. Для организаций, занимающихся проектной и производственной деятельностью (например, научно-исследовательские центры), критичным требованием к DLP-системам является поддержка анализа чертежной документации. SecureTower 6.0 умеет перехватывать и анализировать на предмет передачи конфиденциальных данных файлы САПР-программ в формате DWG и DXF, с которыми работают инженеры и проектировщики.

ЗАКЛЮЧЕНИЕ

Существующие угрозы и вызовы в сфере информационной безопасности, большая часть которых приходится на утечку конфиденциальной информации, указывают необходимость дальнейшего совершенствования правового и технического урегулирования в рассматриваемом направлении и кардинальной трансформации системы защиты информационной сферы в целом.

В работе рассмотрена актуальная тема, связанная с обзором программных комплексов для анализа и предотвращения утечки конфиденциальной информации.

Работа состоит из введения, двух глав, заключения и списка литературы из 6 источников.

Во введение обоснована актуальность рассматриваемой темы, определена цель и задачи работы.

В первой главе выполнен обзор и анализ основных причин утечки конфиденциальной информации. Проведенный обзор основывается на материалах исследований компаний «Лаборатория Касперского» и «InfoWatch». Проведенный обзор показал увеличение рисков, связанных с утечкой конфиденциальной информации организаций и фирм.

Также проведен обзор основных каналов утечки информации. Рассмотрены и описаны основные каналы утечки информации: организационные, визуально-оптические, акустические, электромагнитные и другие каналы.

Во второй главе работы выполнено описание систем DLP, которые позволяют предотвратить утечку конфиденциальной информации. В России , в качества аналога, используется словосочетание «системы защиты конфиденциальных данных от внутренних угроз». Для идентификации угроз, в DLP-системах, чаще всего используются такие методы: вероятностный, детерминистский и комбинированный. В системах, для которых реализован вероятностный метод идентификации используют лингвистический анализ контента и «цифровые отпечатки» данных. В системах, которые построены с использованием детерминированного подхода используются специальные метки файлов. Такие системы являются достаточно надежными, но они не отличаются гибкостью настроек и администрирования. В комбинированных системах используются как

вероятностный, так и детерминистский подходы, что дает возможность построения оптимального программного решения для обеспечения защиты конфиденциальности информации.

В главе также приведены критерии оценки DLP-системы, которые могут быть использованы для их выбора при внедрении таких системы в организации.

Для примера приведен обзор наиболее популярных программных комплексов анализа и защиты от утечек данных:

- Securit ZGate;
- InfoWatch Traffic Monitor;
- Symantec Data Loss Prevention;
- Search Inform Контур безопасности;
- FalconGaze SecureTower.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. КИБЕРБЕЗОПАСНОСТЬ (2017–2018): ЦИФРЫ, ФАКТЫ, ПРОГНОЗЫ // www.ptsecurity.com URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf (дата обращения: 28/08/2018).
2. Прогнозы в области информационной безопасности на 2018 год: [Электронный ресурс]. – URL: http://aladdin-rd.ru/company/pressroom/ articles/45115/. (дата обращения: 28/08/2018).
3. Роговский Е.А. Глобальные информационные технологии – фактор международной безопасности /Е.А. Роговский // США и Канада : экономика – политика– культура. – 2011. – № 6. – С. 3–26.
4. Харрис Ш. Кибервойн@: пятый театр военных действий / Ш. Харрис. – М: Альпина нон-фикшн, 2016. – 390 с.
5. Lehtinen R. Computer Security Basics O’Reilly / R. Lehtinen, D. Russell, G.T. Gantemi. – O’Reilly Media? 2006. – 312 с. –[Электронный ресурс]. – URL: http://www.kaspersky.ru. (дата обращения: 28/08/2018).
6. The future of cybersecurity. Analytics and automation are the next frontier // www.deloitte.com URL: https://www2.deloitte.com/insights/us/en/topics/analytics/future-of-cybersecurity-in-analytics-automation.html?icid=dcom_promo_featured|global;en (дата обращения: 28/08/2018).

1. КИБЕРБЕЗОПАСНОСТЬ (2017–2018): ЦИФРЫ, ФАКТЫ, ПРОГНОЗЫ // www.ptsecurity.com URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf (дата обращения: 28/08/2018). ↑

2. Прогнозы в области информационной безопасности на 2018 год: [Электронный ресурс]. – URL: http://aladdin-rd.ru/company/pressroom/ articles/45115/. (дата обращения: 28/08/2018). ↑

3. Роговский Е.А. Глобальные информационные технологии – фактор международной безопасности /Е.А. Роговский // США и Канада : экономика – политика– культура. – 2011. – № 6. – С. 3–26. ↑

4. Харрис Ш. Кибервойн@: пятый театр военных действий / Ш. Харрис. – М: Альпина нон-фикшн, 2016. – 390 с. ↑

5. Lehtinen R. Computer Security Basics O’Reilly / R. Lehtinen, D. Russell, G.T. Gantemi. – O’Reilly Media? 2006. – 312 с. –[Электронный ресурс]. – URL: http://www.kaspersky.ru. (дата обращения: 28/08/2018). ↑

6. The future of cybersecurity. Analytics and automation are the next frontier // www.deloitte.com URL: https://www2.deloitte.com/insights/us/en/topics/analytics/future-of-cybersecurity-in-analytics-automation.html?icid=dcom_promo_featured|global;en (дата обращения: 28/08/2018). ↑