Пример расчёта окупаемости инвестиций для DLP-системы

написано Александр Астахов | 14 июня, 2023
Покажем, как при помощи методов анализ информационных рисков и статистических сведений об утечках информации, которыми мы располагаем, оценить окупаемость DLP-систем.

Несмотря на следующие один из другим кризисы, доходы разработчиков DLP-систем в основном растут. Во многих компаниях уже либо используются DLP-системы, либо их предварительно тестируют, либо собираются тестировать в ближайшее время. И это несмотря на дороговизну с одной стороны и отсутствием каких-либо представлений об экономическом эффекте от их использования с другой. Если бы речь шла только о гос. организациях, то это еще можно понять, так там надо осваивать бюджеты, а значит чем дороже системе, тем лучше. Но коммерческие структуры тоже подвержены этой моде. Про эффективность, важность информации и губительных последствиях утечек нам уже все рассказали маркетинговые службы разработчиков этих систем. Но пора уже поговорить об экономике вопроса.

Безусловно DLP-система – очень мощный инструмент, внутренние угрозы – основной класс угроз ИБ, а утечки информации могут иметь очень серьезные последствия для бизнеса. Но достаточно ли этих абстрактных соображений для того, чтобы ежегодно тратить на DLP-систему от нескольких миллионов до нескольких десятков миллионов рублей, ухудшать моральный климат в коллективе и вступать в непростые отношения с законодательством, защищающим право граждан на личную жизнь (в том числе и на работе)? Являются ли DLP-системы экономически оправданными? При каких условиях? Для каких организаций? Как оценить их экономическую эффективность?

Например, отбойный молоток – тоже очень эффективный

инструмент, но им же не забивают гвозди. Безопасность должна быть экономически обоснована.

Продвижение DLP-систем осуществляется их разработчиками при помощи отчетов об инцидентах. Цель этих отчетов заключается не в предоставлении наиболее полных и достоверных данных для оценки окупаемости, а демонстрация того, что проблема утечек существует, носит достаточно общий характер и имеет тенденцию к увеличению.

Достоверных данных об утечках, особенно по России не существует. Информация берется в основном из открытых источников. Поэтому в данную статистику попадают только резонансные дела, просочившиеся в прессу. Многие инциденты не афишируются. Компании статистику своих инцидентов либо вообще не ведут, либо не предоставляют.

Тем не менее нам надо на что-то опираться. Поэтому будем опираться на наиболее свежие отчеты. Они не настолько не

достоверны. Ведь сами посудите все утечки по своим последствиям можно разделить на три группы: наносящие ущерб репутации (все они попадают в официальные отчеты), наносящие прямой финансовый ущерб (как правило не очень большой и наиболее легко оцениваемый) и приводящие к утрате конкурентных преимуществ в результате утечки коммерческой тайны, защищаемой законом (такие утечки разбираются в судах и должна быть судебная статистика по делам, связанным с нарушением интеллектуальной собственности).

Так может быть эта статистика как раз и дает представление о наиболее существенных утечках?

Из наиболее громких утечек прошедшего года мы можем видеть случаи, которые могли привести к утрате конкурентных преимуществ в результате нарушения коммерческой тайны и случаи, которые могли привести к прямому финансовому ущербу (судебные издержки и компенсации), а также к репутационному ущербу, но не привели. По мнению аналитиков, готовивших отчет,

во всех этих случаях «ущерб не очевиден».

Рассмотренные данные и служат обоснованием DLP-системы. Мы увидели что проблема существует по всему миру и Россия на одном из первых мест. Проблема выражается кругленькой суммой в 30 миллиардов долларов, и это только вершина айсберга. Проблема касается каждого и растет из года в год. Все, необходимость приобретения DLP-системы очевидна. Вопрос только в том, какую выбрать. Предположим выбрали вы систему. Все ли инцидента, о которых говорилось в рассмотренном отчете она позволит предотвратить? И сможет ли предотвратить? Насколько эффективно? Может быть на практике она только часть этих инцидентов позволит предотвратить и в основном только создает ложное чувство защищенности?

Рассмотрим архитектуру DLP-системы на примере КИБ SearchInform.

Модулей много. Как правило, клиенты покупают максимальную

комплектацию, т.к. это значительно выгоднее по цене. Исключение могут составлять случаи, когда клиенту нужен только 1-2 модуля. Например, контролировать только устройства или только принтеры. Но в таком случае бывает дешевле найти узкоспециализированное решение от какой-то другой компании.

В первую входят те компоненты, которые поставляются всегда. То есть не купить их не получится, т.к. без оных DLP-система не будет функционировать. Это:

DataCenter – центр управления «КИБ». Контролирует работоспособность модулей, а также управляет всеми созданными индексами и базами данных.

Одна из платформ для перехвата информации. NetworkSniffer отвечает за сетевой перехват. EndpointSniffer – за перехват на конечных точках.

SoftInform SearchServer – модуль, отвечающий за индексацию перехваченной информации.

AlertCenter – «мозговой центр» всей системы безопасности. Опрашивает все модули и, при наличии в перехваченной информации заданных ключевых слов, фраз или фрагментов текста, атрибутов документов, немедленно оповещает об этом офицеров безопасности.

Общий клиент – предназначен для ручного мониторинга трафика различных каналов передачи данных (HTTP, Skype, почтовой переписки и др.), а также осуществления поиска по перехваченным данным.

ReportCenter – инструмент отчётности. Позволяет собирать статистику по активности пользователей и инцидентам, связанным с нарушениями политики безопасности, и представлять ее в виде отчетов;

В «необязательную» часть можно отнести некоторые инструменты, а также модули (сниферы) контроля отдельных каналов в рамках

платформ NetworkSniffer и EndpointSniffer. В предельном случае можно купить модуль для контроля только одного канала.

В платформе NetworkSniffer:

- SearchInform MailSniffer;
- SearchInform IMSniffer;
- SearchInform HTTPSniffer;
- SearchInform FTPSniffer;
- SearchInform CloudSniffer;
- SearchInform ADSniffer.

В платформе EndpointSniffer:

- SearchInform MailSniffer;
- SearchInform IMSniffer;
- SearchInform HTTPSniffer;
- SearchInform MicrophoneSniffer;
- SearchInform MobileSniffer;
- SearchInform MonitorSniffer;
- SearchInform KeyloggerSniffer;
- SearchInform FileSniffer;
- SearchInform FTPSniffer;
- SearchInform PrintSniffer;
- SearchInform DeviceSniffer;
- SearchInform SkypeSniffer;
- SearcInform ProgramSniffer;
- SearchInform CloudSniffer;
- Сервер индексации рабочих станций;

Дополнительные инструменты:

- EndpointSniffer Hub – позволяет внедрять КИБ в территориально распределенные филиалы компании, в каждом из которых используется небольшое количество рабочих станций и/или «узкий» канал связи с головным офисом;

- SearchInform IncidentCenter – предназначен для оказания помощи сотруднику службы безопасности в категоризации фактов нарушений информационной безопасности компании, ведении «Дел» по сотрудникам и проведении расследований

Подробнее обо всех модулях и платформах можно прочитать здесь: http://searchinform.ru/main/full-text-search-information-security-product.html

Эти соображения надо будет учесть при формировании моделей угроз и уязвимостей.

Перейдем теперь к оценке окупаемости и экономической эффективности DLP. Она характеризуется ROI, который определяется отношением ALE к TCO.

ROI = 0, сколько вложили, столько и съэкономили, ничего не выиграли и не потеряли

ROI < 0, стоимость DLP превышает оценочный ущерб, зря потеряли деньги время

0 < ROI < 1, с учетом большой неопределенности измерений, какая либо польза от DLP не очевидна

ROI = 1, мы получаем 100% экономию на вложенные средства

ROI > 10, ожидаемое сокращение потерь на порядок превышает затраты на DLP

Хоть мы и говорим об инвестициях в ИБ, не надо путать это с обычными инвестициями, которые значительно лучше

просчитываются и для которых ROI = 1 – это отличный результат (100% прибыль за год). Инвестиции в безопасность – это страхование, а страховая премия обычно составляет не более 10%, очень часто меньше 1%. Для страхования 10 < ROI <100. Таким же примерно должен быть ROI для DLP системы. Если ROI < 10 – это слишком большая страховая премия. Хотели бы вы застраховать свою машину или квартиру, например, за 20% процентов ее стоимости в год?

Т.о. простая формула ROI дает нам ответы на все экономические вопросы ИБ. ROI > 10 – хорошо, ROI < 10 – плохо, ROI < 0 – отвратительно. В этой формуле TCO достаточно легко и точно считается, а ALE является нескольких нелинейных величин, носящих очень неопределенный характер, таких как частота инцидентов, величина уязвимости и ценность актива.

Основная экономическая целью ИБ – обеспечения оптимального уровня возврата инвестиций в безопасность, т.е. Максимизация ROI. Для этого надо не только оценивать риски, но также регистрировать, анализировать и считать прямые и косвенные потери в результате инцидентов.

На схеме закрашены проблемные области с отрицательным возвратом инвестиций: область недофинансирования и область избыточного финансирования. В первом случае деньги на безопасность не выделяются, либо выделяются по остаточному принципу. Для этого случае характерны проблемы с вирусами, отсутствие планов непрерывности бизнеса и легкомысленное отношение персонала к вопросам безопасности. Во втором случае, осуществляется избыточное финансирование безопасности, но большая часть средств расходуется впустую. Для этого случая характерно процветание бюрократии, избыточная формализация, приобретение дорогостоящего оборудования без принятия необходимых организационных мер.

Будем двигаться от простого к сложному, поэтому начнем с оценки TCO.

В стоимость лицензии может входить тех. поддержка, обучение, проектирование, внедрение.

Если же обозначать вилку, то цена за 1 модуль на 1 компьютер будет от 900 до 3900 рублей. Зависит от сложности модуля. К примеру, MonitorSniffer будет дешевле, т.к. его задача делать снимки экрана и отсылать их на сервер. MailSniffer, в свою очередь, будет дороже, т.к. должен уметь работать с большим количеством протоколов, разбирать множество атрибутов и т.д.

100 машин – 2,3 млн. рублей

500 машин – 8,5 млн. рублей

1000 машин – 14 млн. рублей

Цена указана для случая, когда покупаются все модули. Также покупка, эквивалентная 1,5 млн. рублей обеспечивает бесплатное обучение 1 специалиста в учебном центре SearchInform по любой из

программ http://searchinform.ru/training/training-center.html

Если купили на 3 млн., можно бесплатно обучить двоих, на 6 млн. – троих и т.д. Контур информационной безопасности SearchInform (далее КИБ) по составу можно представить в виде «обязательной» и «необязательной» части.

Конфигурации серверов для 1000 агентов:

- CPU от 2×2.0 GHz 8 Core
- RAM от 64 Gb
- HDD1 от 512Gb – ОС, ПО, очередь от агентов (рекомендуется SSD RAID 1)
- HDD2 данные (базы)* (рекомендуется RAID 10 или 50, SAS 10000)
- HDD3 20% от HDD2 – индексы, кеш Alert (рекомендуется RAID 10 или 50, SAS 10000)
- LAN 1 Gbps

Примерно: 766 585,00 руб.

OS от Windows 2008R2 и выше

Примерно: 30000 руб.

DB от Microsoft SQL Server 2008R2 (Standard, Enterprise)

* при условии хранения данных 6 месяцев – около 20Tb

Примерно: 70000 руб.

Итого: 866585 рублей

При покупке КИБ первый год техподдержки входит в стоимость. В дальнейшем каждый год оплата составляет 30% от стоимости лицензий (см. п.1).

В техподдержку входит:

- обновление софта (выпуск новых версий, расширение функционала, оптимизация работы, исправление багов и т.д.);
- обслуживание по инженерной части (к примеру, если клиент по какой-то причине не может или не знает, как разбить индексы, настроить автоматический запуск компонент, прописать альтернативные адреса серверов и т.д.);
- первичное обучение по части аналитики (создание и настройка политик, составление отчётов и т.д.) и дальнейшая поддержка со стороны отдела внедрения;
- бесплатное обучение в учебном центре по любой программе. В том случае, если сумма техподдержки кратна 1,5 млн. рублей.

Количество этапов рознится и зависит от требований заказчика. По цене можно сказать, что полный цикл внедрения DLP-системы стоит порядка 10% от стоимости покупки. У нашей компании стоимость всех этапов уже заложена в итоговую цену (см. п.1),

поэтому они «бесплатны». Как правило, клиенты более позитивно воспринимают тот, факт, что озвученная стоимость окончательна и «вдруг» в большую сторону не увеличивается.

План внедрения DLP-системы «На пальцах» план таков:

Клиент заполняет типовую анкету, в которой указывает, что хочет контролировать, в каком объёме и каким мощностями (оборудованием) на данный момент он планирует это обеспечить. Часто бывает так, что «коробочное» решение (предустановленное на сконфигурированное железо) не нужно клиенту, т.к. оно либо не вписывается в существующую инфраструктуру, либо у клиента есть свои мощности (сервер или виртуальные мощности под него, SQL-сервер и т.д.)

Технический отдел проверяет анкету и даёт свои рекомендации по оборудованию и необходимым действиям (внести исключения в антивирус, создать учётные записи с определёнными правами и т.д.)

Клиент выполняет рекомендации и рапортует, что он готов к тестовому внедрению.

Тестовое внедрение бесплатно. Так как DLP-система – штука дорогая, мало кто хочет брать «кота в мешке». Одни хотят посмотреть, что происходит внутри компании и понять, нужно ли им вообще её покупать (до последнего надеются, что у них всё хорошо, сотрудники не воруют, конфликтов нет и т.д.). Другие точно знают, зачем им DLP и хотят выбрать лучшую под их задачи. Для этого могут одновременно развернуть несколько систем от разных вендоров, запросить проведение сравнительных испытаний, нагрузочных тестирований и т.д. В начале нулевых преобладала первая группа. В последние лет 5 больше заказчиков из второй.

Назначается дата развёртывания КИБ. В оговоренное время инженеры подключаются удалённо или приезжают непосредственно к заказчику.

После установки подключается отдел внедрения для проведения первичного обучения работы с софтом, оказания помощи в настройке политик безопасности, анализе перехваченной информации, составлении отчётов и т.д.

Стоимость разработки ОРД для DLP-системы

№	Наименование	Трудоемкость, чел./дн.	Стоимость, тыс. руб.
1	Обследование организации, инвентаризация и классификация информационных активов	20	400
2	Разработка политики обеспечения конфиденциальности информации	10	200
3	Разработка политики и регламента управления инцидентами ИБ	10	200
4	Разработка политики допустимого использования ресурсов корпоративной сети и правил работы пользователей	8	160
6	Разработка положения о предотвращении утечек информации	8	160
7	Разработка инструкции администратору DLP системы	6	120
8	Разработка инструкции эксперту-аналитику по настройке правил фильтрации контента	6	120
9	Разработка форм отчетности по предотвращению утечек информации и по инцидентам	5	100
Итого:		73	1 460 000

Такая документация в каждой компании своя. Её состав и содержание «на совести» компании. В предельном случае можно внедрить систему неофициально, без внесения соответствующих пунктов в трудовой договор и прочего. Вот только использование такой системы будет незаконно.

Стоимость человеко-дня = 20 т.р. Без правильного комплекта ОРД DLP будет конфликтовать с законодательством защищающим права на частную жизнь и, не будучи поддержана орг. Мерами, останется просто дорогой игрушкой.

TCO = 9 070 т.р. в год.

Теперь переходим к оценке вероятного среднегодового ущерба.

Для расчета ALE используется следующая знакомая многим формула. В этой формуле:

Вероятность угрозы – частота инцидентов ИБ

Величина уязвимости – % успешных инцидентов

Размер ущерба – совокупная стоимость скомпрометированных информационных активов

Угрозы будем рассматривать те, от которых защищается DLP-система, группа активов, критичных с точки зрения конфиденциальности (различные виды тайн, ПДн, финансовая информации).

Для оценки этих факторов риска нам необходимо будет пройти все этапы, предусмотренные методикой управления рисками ИБ, которая изначально была описана BSI в 3-й части стандарта BS 7799-3, затем была заложена в стандарты ISO 27000, и была адаптирована GlobalTrust для практического применения.

Все эти этапы управления риском мы разбираем на практическом тренинге, который будет проходить в конце июля в рамках учебного курса SearchInform «DLP от А до Я» и начнется как-раз с буквы А, т.е. с нашего тренинга по оценки рисков и эффективности DLP-систем.

Основной документ, который формируется по результатам применения данной методики – рисков ИБ (ПР) – документ, характеризующий риски ИБ объекта защиты (ОЗ).

Там есть все составляющие риска ИБ, в том числе и ROI DLP. Но пойдем дальше. Первое, что нам необходимо сделать для оценки риска – разобраться с активами. Нужна инвентаризация активов и оценка их ценности для бизнеса. Ценность актива выражается размером потенциального ущерба, который может быть нанесен в результате его компрометации. Для оценки этого ущерба необходим анализ последствий инцидентов (в нашем случае – утечек информации).

Все последствия утечек можно разделить на три группы. Рассмотреть соответствующие сценарии для каждой группы критичных активов, дать свои оценки наихудшему сценарию и наиболее вероятному сценарию развития событий. Далее сопоставить свои результаты с усредненными оценками, полученным различными исследователями.

В качестве примера посмотрим на расчеты Forrester Research.

Пример: Стоимость утечки одной записи (Forrester Research)

Cost Category	Description	Cost per Record
Discovery, response, and notification	Outside legal fees, customer notification, increased call center activity, marketing and PR, discounted product offers	$50
Lost employee productivity	Employees diverted from normal duties, contractor labor	$30
Restitution	Compensating affected customers for direct losses	$30
Opportunity costs	Loss of future business opportunities	$98
Total Direct Cost per Record		*$218*

Figure 2: Direct Cost per Record of a Leak

Global Trust Solutions

В данному примере оцениваются прямые убытки, связанные с утечкой ПДн клиентов, в расчете на одну порцию данных. Если утекла клиентская база насчитывающая 100 000 записей, то прямой ущерб составит $21,8 млн.

Пример: Оценка репутационного ущерба от утечки (Forrester Research)

	Repeat Customers	New Customers	Total
Total annual revenue	$800 million	$200 million	$1 billion
Lost business as a percentage of revenues	10%	20%	12%
Lost business in dollars	$80 million	$40 million	$120 million

Figure 5: Estimated Revenue Impact of a Leak

Global Trust Solutions

Далее оцениваются последствия репутационного ущерба для компании с годовым оборотом в $1 млрд. В данном случае он может составлять более 60% маржи (валовой прибыли) – $120 млн.

Пример: Оценка воздействия утечки на доходы и прибыль (Forrester Research)

	Year 1	Year 2	Year 3	Year 4	Year 5
Annual Revenue (assuming 8% growth)	$1,000,000,000	$1,080,000,000	$1,166,400,000	$1,259,712,000	$1,360,488,960
Annual Net Profit (assuming 20% margins)	$200,000,000	$216,000,000	$233,280,000	$251,942,400	$272,097,792
Annual Leak Remediation Cost	$12,220,000	$8,450,000	$5,770,000	$4,680,000	$4,680,000
Lost Business Costs	$120,000,000	$129,600,000	$139,968,000	$151,165,440	$163,258,675
Total Leak-Related Losses	**$132,220,000**	**$138,050,000**	**$145,738,000**	**$155,845,440**	**$167,938,675**
Resulting Annual Net Profit	$67,780,000	$77,950,000	$87,542,000	$96,096,960	$104,159,117
Decline in Profitability Due to Leak	***66%***	***64%***	***62%***	***62%***	***62%***

Figure 6: Estimated Revenue Impact of a Leak Over 5 Years

Далее прямые и косвенные последствия утечки суммируются. Получаем цифры по недополученной прибыли на периоде 5 лет.

Пример: Влияние утечки на прибыль (Forrester Research)

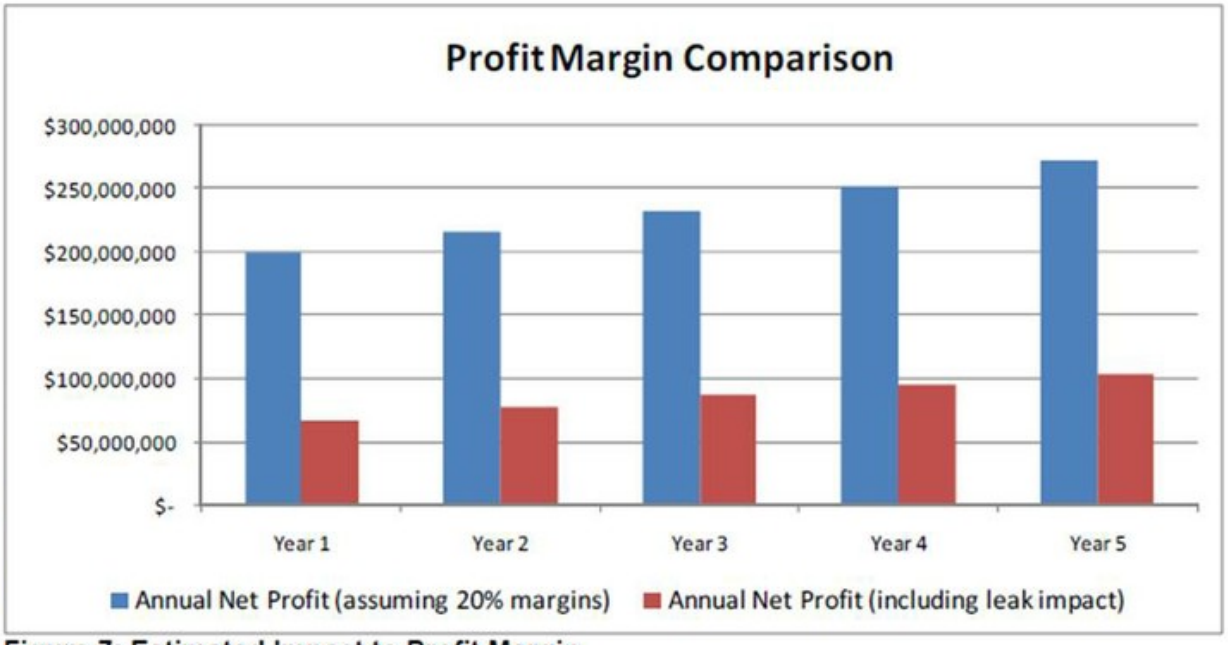


Figure 7: Estimated Impact to Profit Margin

На графике показана прибыль компании до и после инцидента.

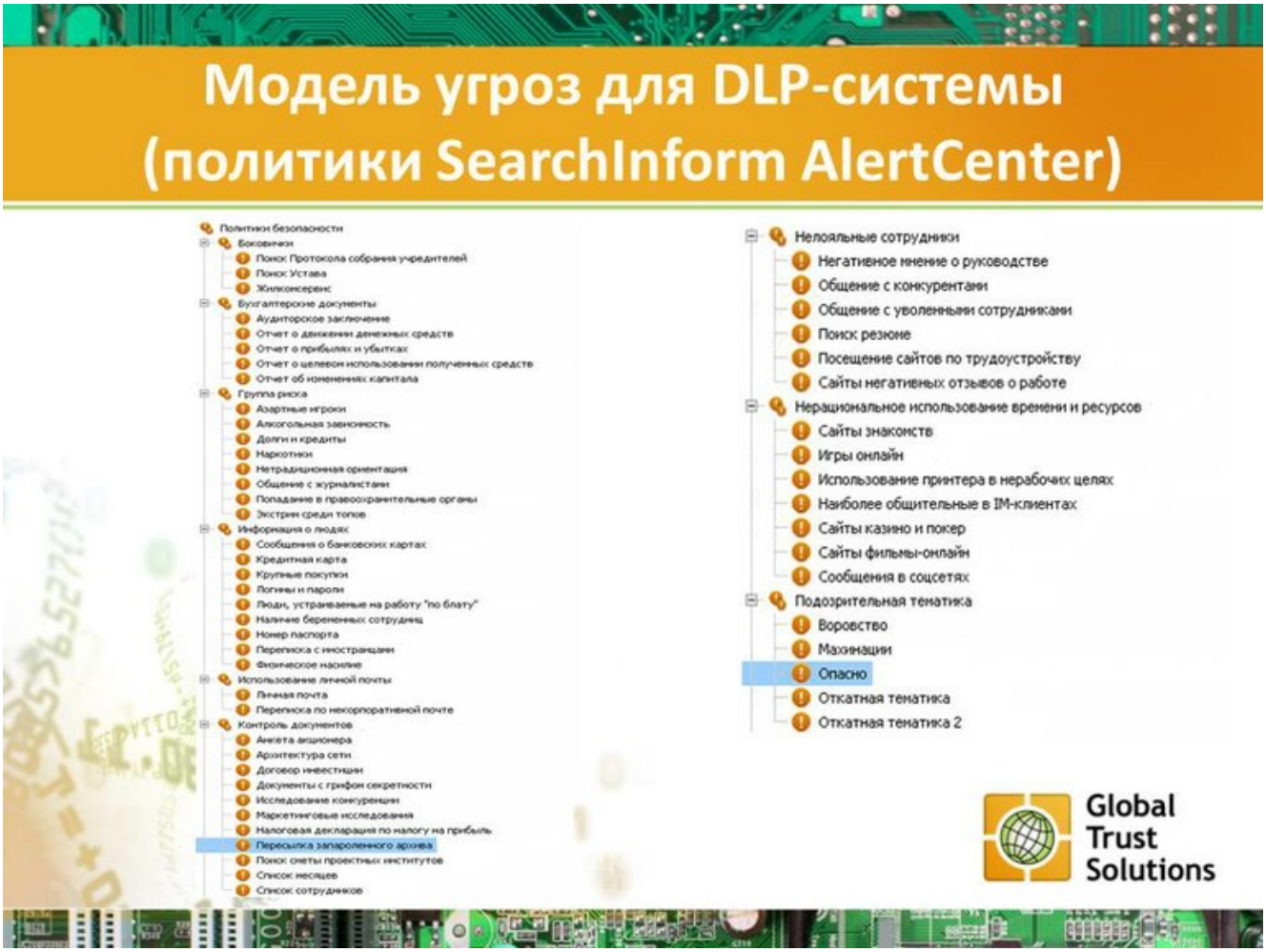
Пример: Сравнение стоимости DLP-системы и ущерба от утечки (Forrester Research)

	Year 1	Year 2	Year 3	Year 4	Year 5
Total Leak-Related Losses	$132,220,000	$138,050,000	$145,738,000	$155,845,440	$167,938,675
Total Cost of DLP	$385,000	$193,750	$192,813	$191,922	$191,076
DLP as a % of Total Risk	**0.29%**	**0.14%**	**0.13%**	**0.12%**	**0.11%**

Figure 11: DLP as a Percent of Total Risk

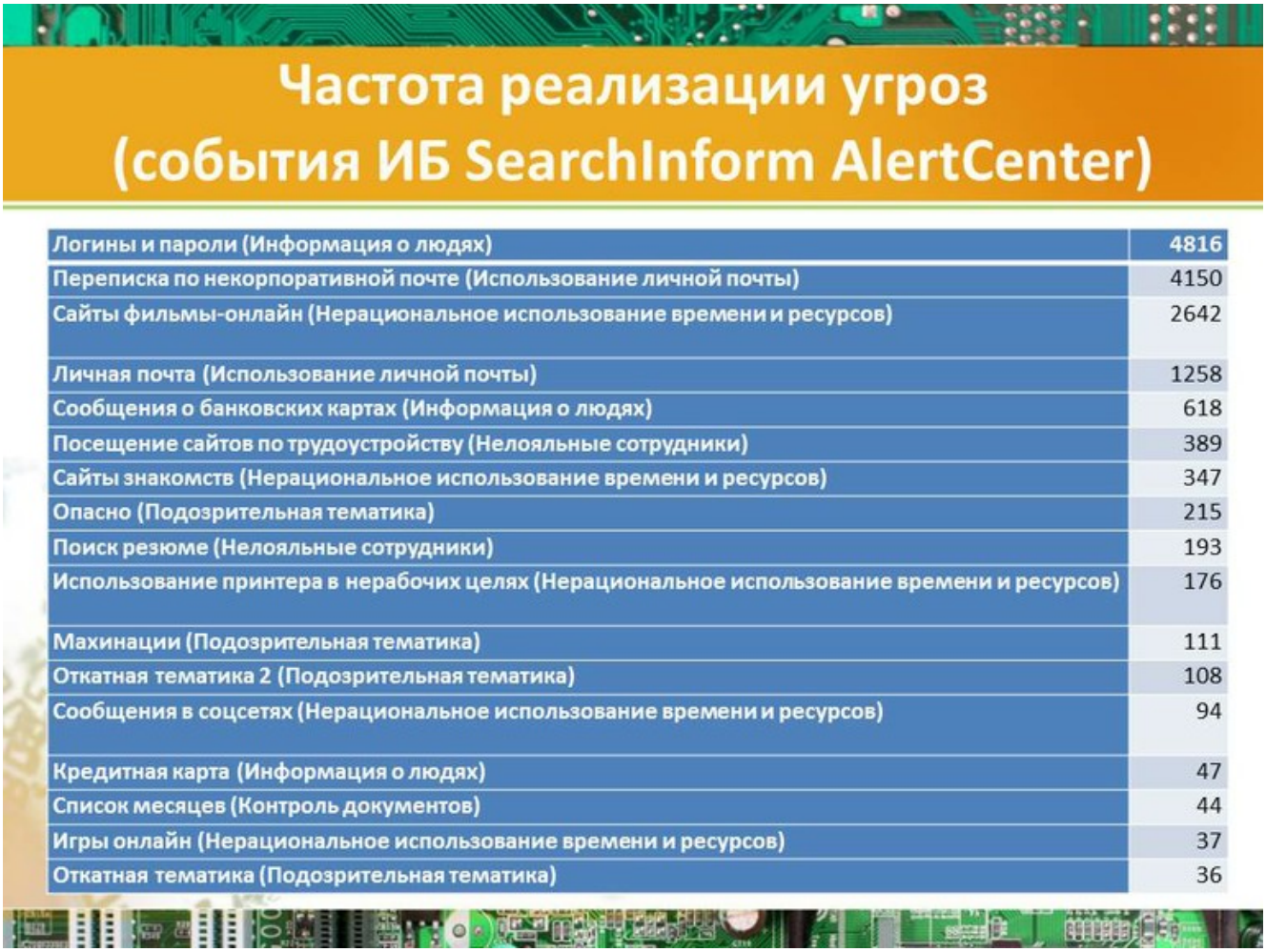
Global Trust Solutions

Теперь размер ущерба сопоставляется со стоимостью DLP. Вобщем-то страховка от угроз ИБ столько и должна стоить. Если учесть еще вероятность реализации рассматриваемого инцидента, то эти проценты возрастут на порядок и ROI DLP как раз попадет в интервал 10-100. Но как оценить эту вероятность угроз? Далее покажем как это можно сделать.



После того, как мы разобрались с активами и их ценностью, можно переходить к анализу угроз и уязвимостей для DLP. Модель угроз DLP в конечном счете находит отражение в политиках.

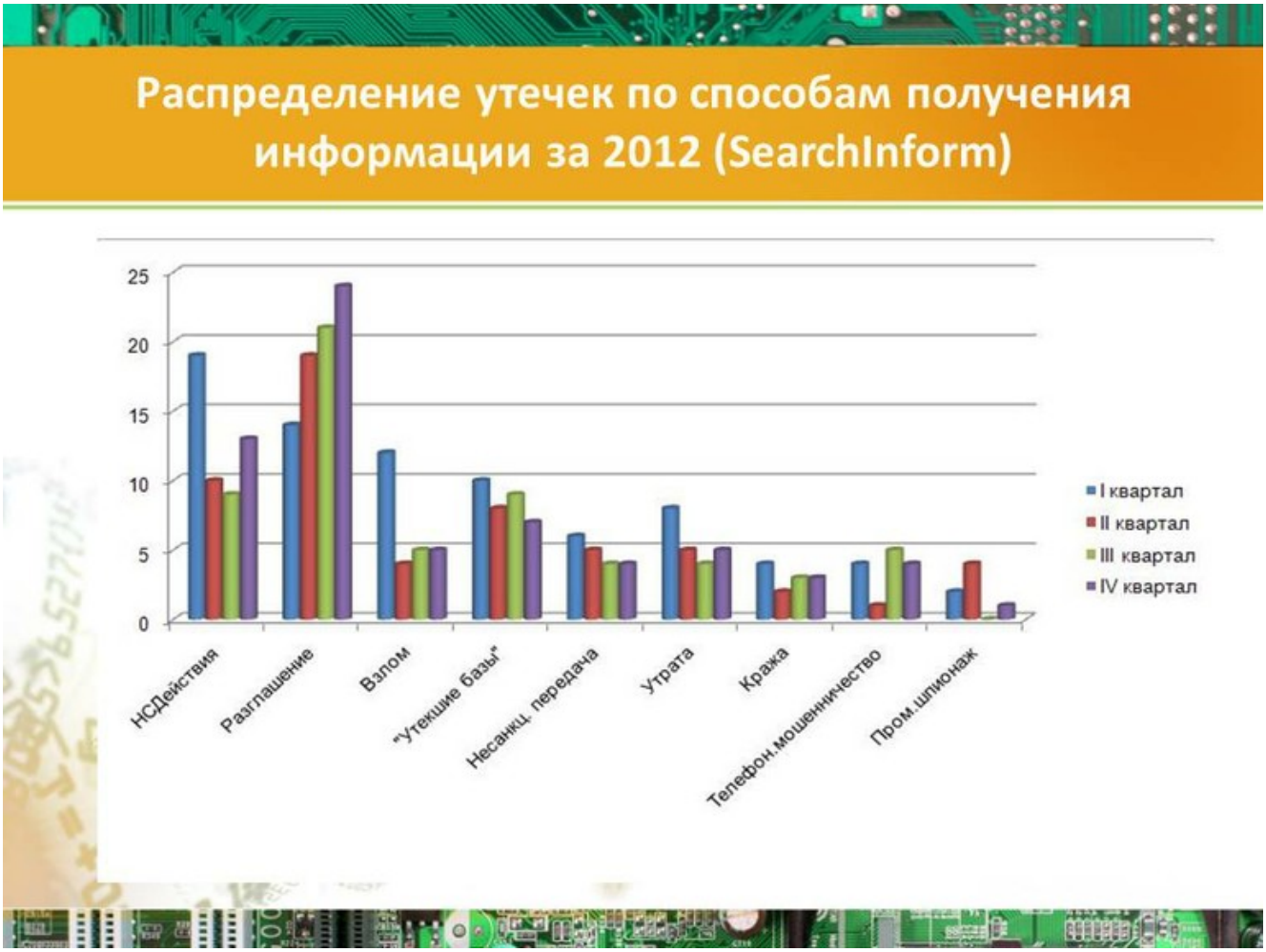
DLP-система ограничена своими политиками. Половина политик направлены не на выявление утечек, а на мониторинг действий сотрудников. Т.е. DLP обеспечивает значительный ROI не связанный с утечками.



DLP-система выявляет не инциденты, связанные с утечками, а события ИБ (десятки и сотни тысяч в месяц), которые могут потенциально быть инцидентами. Нет возможности заблокировать все обнаруженные события, а значит нет возможности и предотвратить возможные утечки.

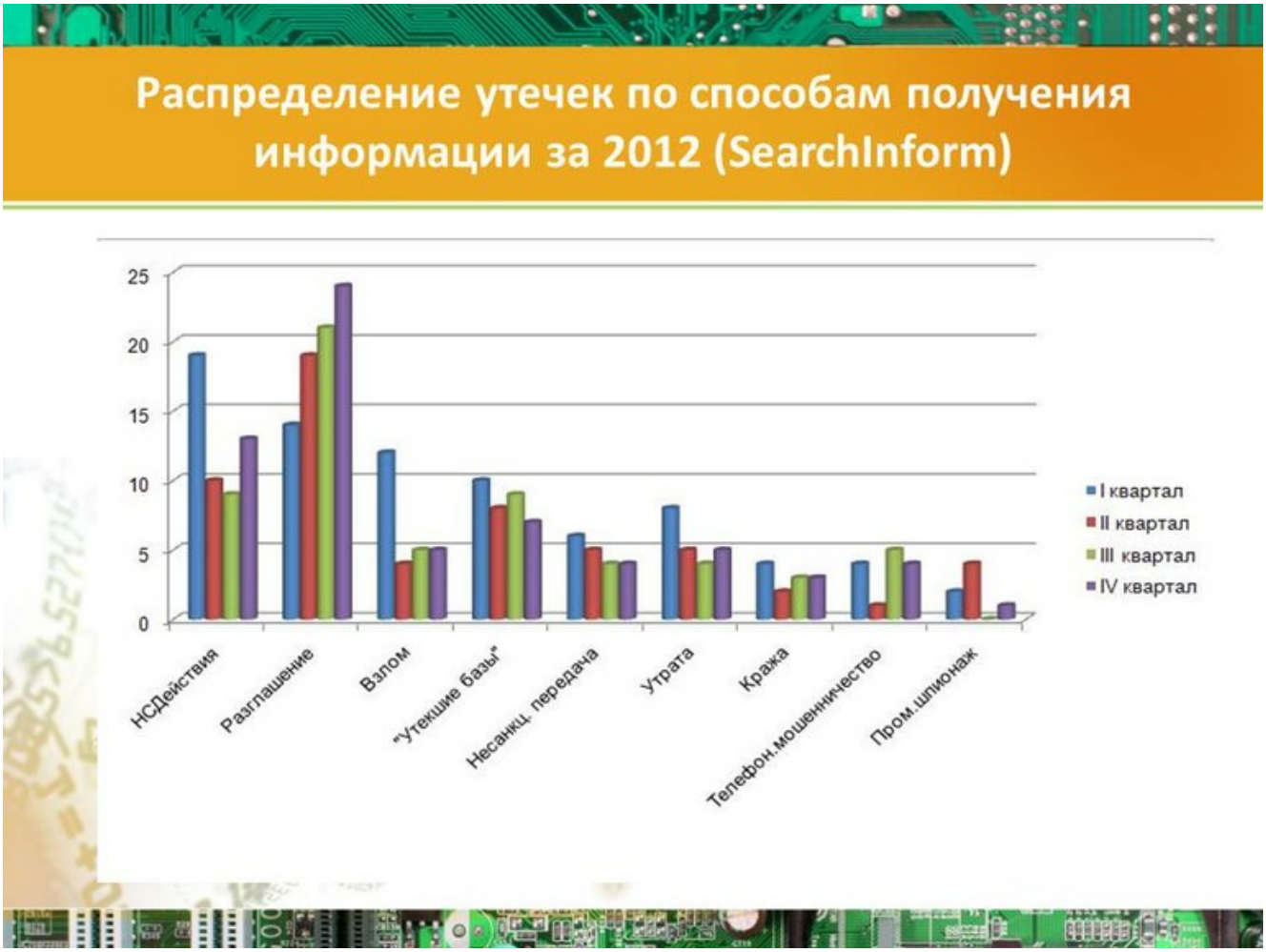
Нужна статистика по организации: сколько было инцидентов, сколько утечек предотвращено, как оценивается ущерб. Сопоставляя это с общей и отраслевой статистикой, можно достаточно точно оценивать вероятность угроз, потенциальный ущерб и ценность активов.

Поскольку у нас нет сейчас такой статистики, воспользуемся очередным отчетом об утечках. Например, для банков имеем 21 зарегистрированный инцидент



Это подтверждается картиной распределения утечек по типам информации.

Примерно 20 инцидентов год связаны с утечкой банковской тайны, если эту цифру разделить на 1000 банков то получится 0,02 или 2% – вероятность инцидента в течение года. Ожидаемая частота угрозы – 1 раз в 50 лет.



Если посмотреть на распределение утечек по способам получения информации, то мы видим, что далеко не все утечки предотвращаются DLP системой, а только приблизительно 70% инцидентов (левая половина графика). Это надо учитывать в модели угроз. Банковских инцидентов, которые можно предотвратить при помощи DLP, будет не 21, а примерно 15.

Теперь рассчитаем ALE до и после внедрения DLP. В качестве среднего размера ущерба возьмем «среднее по больнице» из статистики инцидентов 2015 – $33 млн.

Величина уязвимости показывает эффективность DLP. Предположим, что сам факт использования DLP на порядок уменьшает количество инцидентов. А их тех, которые происходят, на порядок снижается количество успешных. Поэтому после частота угрозы и величина уязвимости у нас соответствующим образом уменьшаются.

В результате данных расчетов получаем ROI = 3.5. Это означает, что возврат инвестиций в DLP в данном случае в 3.5 раза превышает ее стоимость. Хороший результат для инвестиций, плохой – для страховки.

ALE и ROI носят вероятностный характер.

ROI = (-2 ; 50) слишком большая неопределенность метода оценки.

ROI = (2;5) – нормальная неопределенность. Например:

ROI = 3.5 с вероятностью 80%, =2 с вероятностью 4%, =5 с вероятностью 7% и т.п.

Эта презентация в формате pdf выложена на сайте GlobalTrust по адресу:

http://globaltrust.ru/ru/about/presscenter/informacionnye-materialy/prezentacii-reshenii-globaltrust/vebinar-kak-rasschitat-okupaemost-investicii-v-dlp-sistemy/view

Видеозапись вебинара выложена здесь:

http://iso27000.ru/video/video-s-seminarov-globaltrust/kak-rasschitat-okupaemost-investicii-dlya-dlp-sistemy