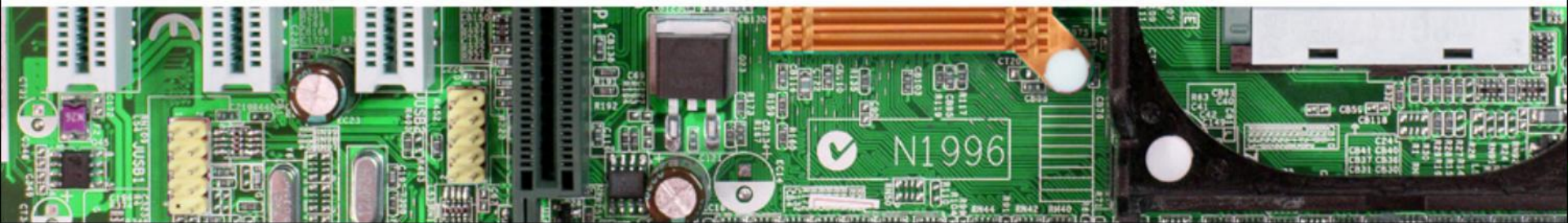
Как рассчитать окупаемость инвестиций для DLP-системы

Александр Астахов

Генеральный директор

Global Trust Solutions

Продукты и услуги в области информационной безопасности



Статистика утечек за 2015 (по данным Zecurion Analytics)

- Общий зарегистрированный ущерб - $29 млрд. (868 утечек)
- Средняя стоимость утечки ~ $33 млн.
- Россия на 4-м месте (после США, Великобритании и Канады) — 49 публичных инцидента (~ $1 617 млн.)
- Финансовые данные физлиц — один из самых востребованных киберпреступниками типов информации — 19.1% инцидентов
- Чаще всего утекает информация из госучреждений, розницы и банков
- Достоверных данных данных, особенно по России, нет

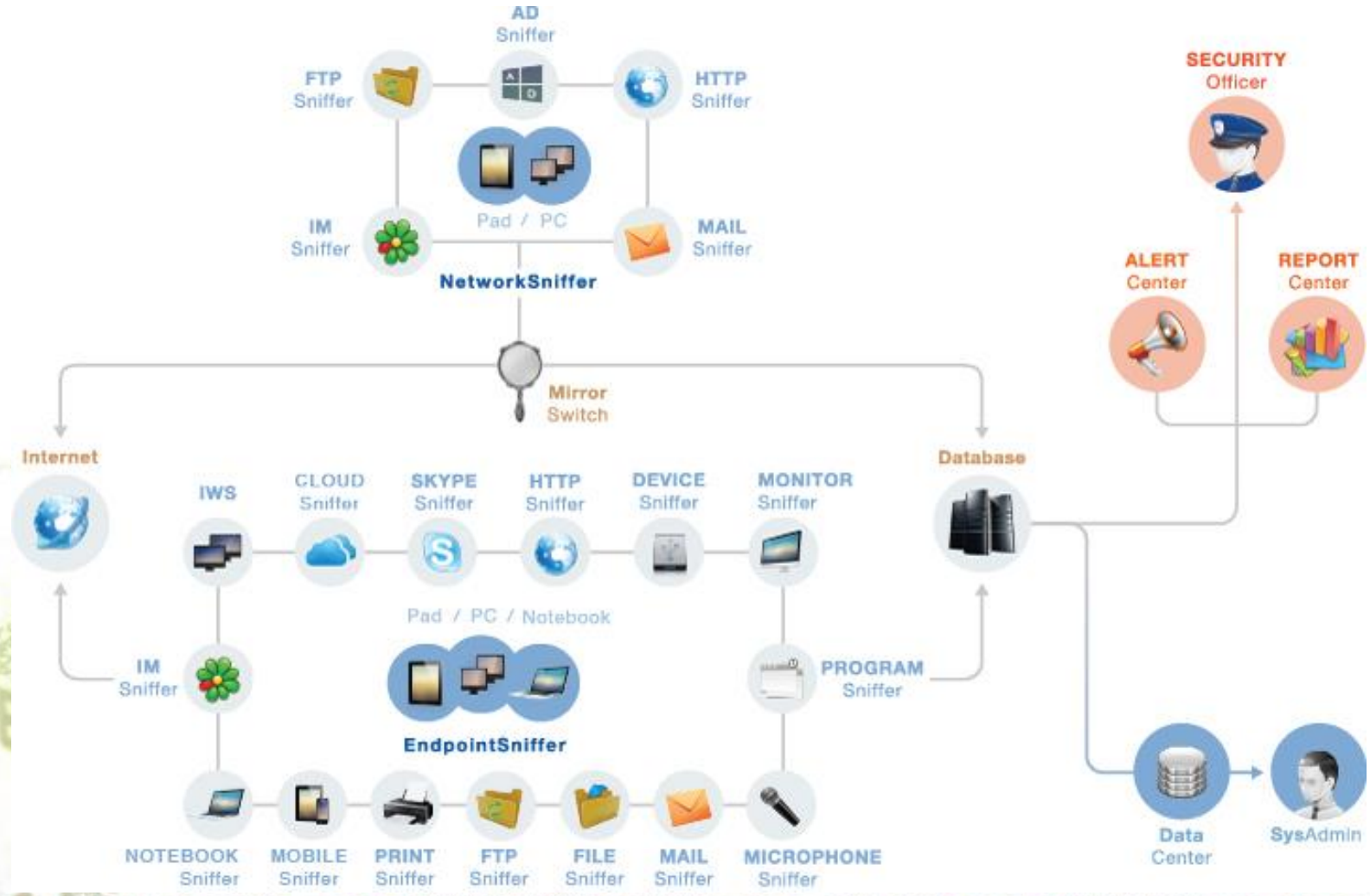
Global Trust Solutions

Громкие утечки из российских компаний

- **Mail.ru и Яндекс** в один день анонсировали запуск двухфакторной аутентификации для доступа к аккаунтам.
- **Яндекс** . Инсайдеру удалось успешно скопировать на флешку и вынести исходники и алгоритмы работы поисковика.
- **Ижевский автозавод.** Инсайдеры сделали «секретные» снимки нового серийного автомобиля Лада Веста и продали их интернет-блогеру.
- **Банк «Санкт-Петербург».** По данным представителей банка в руки злоумышленников попали имена, номера счетов, номера карт и ИНН нескольких тысяч клиентов. Перевыпуск карт и репутационный ущерб. Банк заявил об отсутствии ущерба.
- **Topface**. На одном из форумов для киберпреступников обнаружили базу пользователей российского сервиса знакомств Topface (только адреса и никнеймы).
- **На портале госзакупок** обнаружили паспортные данные членов Совета Федерации.

Global Trust Solutions

Архитектура DLP-системы КИБ SearchInform



Ограничения DLP-систем

DLP система позволяет:

- Выявлять, блокировать, расследовать утечки информации из корпоративной сети, осуществляемые сотрудниками организации при помощи штатных средств
- Осуществлять мониторинг действий пользователей корпоративной сети и контролировать производительность труда

DLP-система не позволяет:

- Противодействовать утечкам информации, происходящим в результате краж или утраты оборудования и носителей информации, внешних взломов сетей и прочих действий, не охваченных политикой DLP-системы

DLP-система имеет ограничения:

- Эффективна только в сочетании с организационными, юридическими и техническими мерами защиты
- Может ухудшать моральный климат в коллективе и вступать в противоречие с законодательством

Global Trust Solutions

Оценка возврата инвестиций в информационную безопасность

- **[Коэффициент возврата инвестиций (ROI)] = ([Уменьшение среднегодовых потерь] – [Стоимость защитных мер]) / [Стоимость защитных мер]**
- Коэффициент возврата инвестиций (ROI) определяется как отношение величины сокращения ожидаемых среднегодовых потерь (величины уменьшения риска) к стоимости реализации контрмер.
- ROI показывает насколько величина ущерба превышает расходы на его предотвращение.

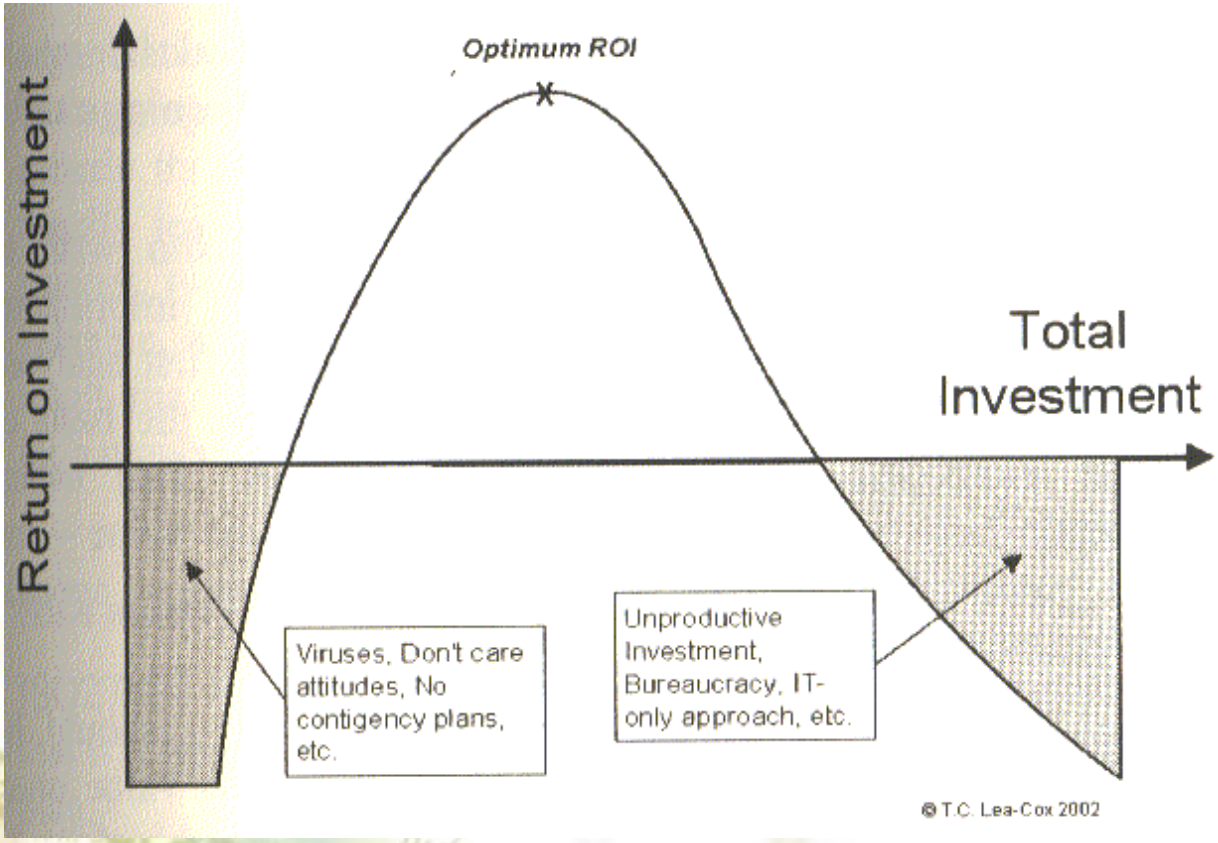
Global Trust Solutions

Коэффициент возврата инвестиций

ROI = ALE / TCO

Global Trust Solutions

Оптимальный уровень возврата инвестиций в безопасность



Методы оценки рисков используются для определения и обоснования оптимального уровня возврата инвестиций в механизмы контроля.

Global Trust Solutions

Стоимость владения (TCO)

Инвестиции в DLP

=

Единовременные затраты

(обследование, проектирование, закупка ПО и оборудования, внедрение, обучение, консалтинг, разработка ОРД, приемочные испытания)

+

Постоянные затраты

(техническая поддержка, продление подписок, администрирование и эксплуатация)

Global Trust Solutions

Стоимость лицензии на DLP-систему

Полная комплектация (включая 1 год тех. поддержки и обучение специалистов):

- 100 машин ~ 2,3 млн. рублей
- 500 машин ~ 8,5 млн. рублей
- 1000 машин ~ 14 млн. рублей

Цена за 1 модуль на 1 компьютер:

~ 900 до 3900 рублей

Global Trust Solutions

Стоимость оборудования и системного ПО

Конфигурации серверов (для 1000 агентов):

- CPU от 2x2.0 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

~ 760 000 руб.

ОС и СУБД:

- Windows 2008R2
- Microsoft SQL Server 2008R2 Standard

~ 30000 руб. + 70000 руб.

Итого:

- Для 1000 агентов ~ 860 000 руб.

Global Trust Solutions

Стоимость технической поддержки DLP-системы

Состав услуг технической поддержки:

- обновление софта (выпуск новых версий, расширение функционала, оптимизация работы, исправление багов и т.д.)
- обслуживание по инженерной части (если клиент 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

Итого 30% от стоимости лицензии:

- 1000 машин ~ 4 200 000 руб.

Global Trust Solutions

Стоимость внедрения DLP-системы

Состав работ по внедрению DLP-системы:

- Заполнение анкеты (для определения состава оборудования, ПО и планирования работ)
- Подготовка к тестовому внедрению
- Тестовое внедрение (может включать сравнительные испытания, нагрузочное тестирование и т.п.)
- Развертывание (установка) DLP-системы
- Первичное обучение
- Настройка политик безопасности
- Анализ перехваченной информации и формирование отчётов

Стоимость внедрения ~ 10% от стоимости лицензии

(для КИБ SearchInform – включена в стоимость лицензии)

Global Trust Solutions

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**

Стоимость владения для DLP-системы (на 5-летнем периоде для 1000 машин)

Статья расходов	Сумма, тыс. руб.
Лицензия на DLP-систему	14 000
Серверное оборудование и системное ПО	860
Техническая поддержка DLP-системы (на 4 года)	16 800
Внедрение DLP-системы (включено в стоимость лицензии)	0
Разработка ОРД для DLP-системы	1 460
Обучение администраторов (2 специалиста, 7 дней)	230
Обслуживание DLP-системы (1 специалист, 5 лет)	12 000
Итого:	**45 350**

Global Trust Solutions

Количественная оценка риска

Величина риска

=

Вероятность угрозы

x

Величина уязвимости

x

Размер ущерба

Global Trust Solutions

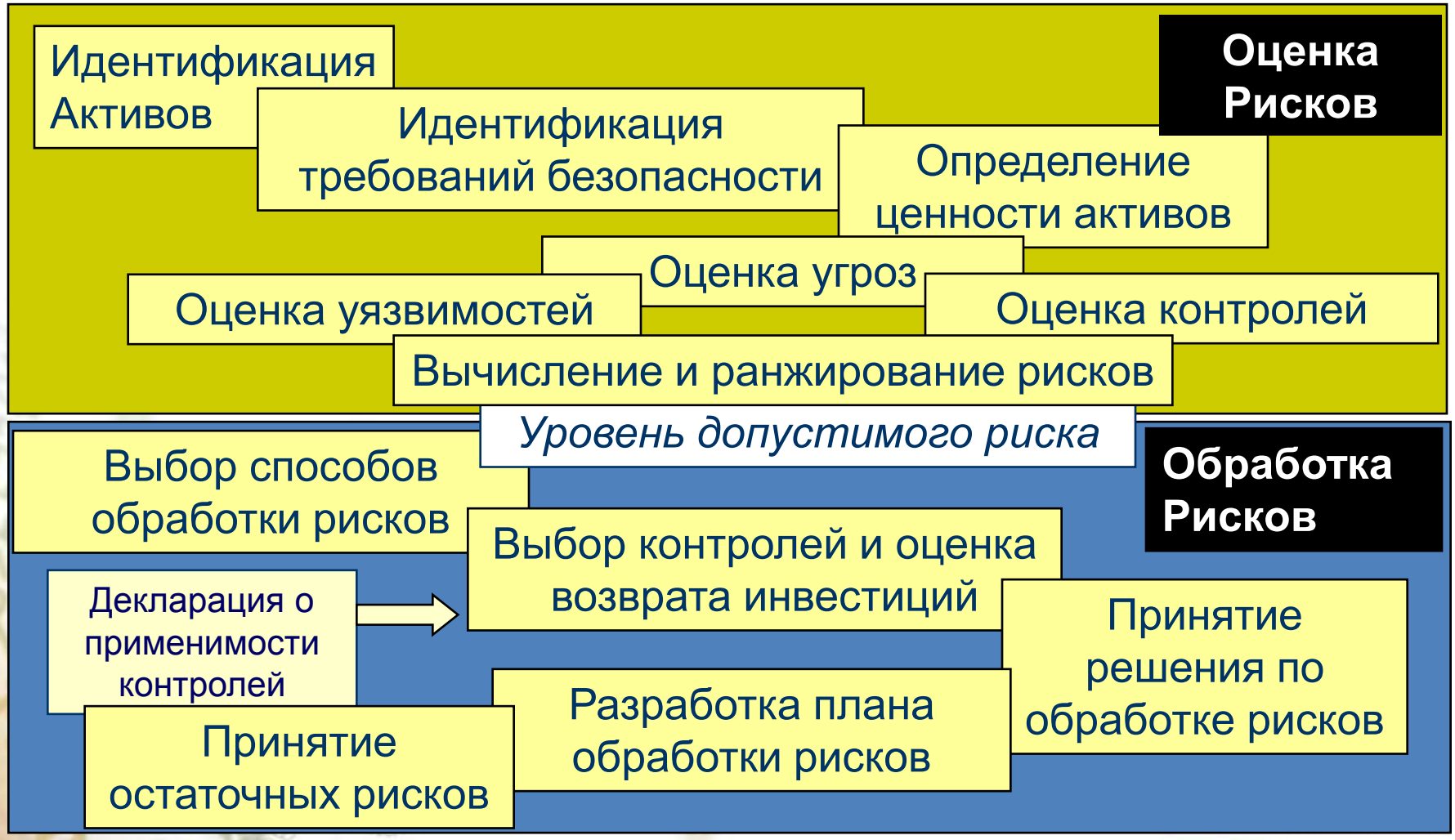
Оценка среднегодовых потерь (ALE)

В качестве отрезка времени, для которого считаются вероятности берется 1 год. В этом случае: **Величина риска = Среднегодовые потери организации в результате успешного осуществления конкретной угрозы (группы угроз) в отношении конкретного актива (группы активов) с использованием уязвимостей данного актива.**

ALE (Annual Loss Expectancy)

Global Trust Solutions

Методика управления рисками BSI/ISO/GTS



Профиль риска

Введение

Контекст управления рисками

- Цели управления рисками
- Критерии оценки ущерба
- Критерии оценки рисков
- Критерии принятия остаточных рисков
- Область и границы оценки рисков
- Организационная структура управления рисками

Активы

- Бизнес-процессы
- Информационные активы
- Ценность активов

Угрозы

- Модель нарушителя
- Модель угроз
- Профили и жизненные циклы угроз
- Оценка вероятности угроз

Уязвимости

- Организационные уязвимости
- Технические уязвимости
- Оценка уровня уязвимостей

Контрмеры

- Организационные контрмеры
- Технические контрмеры
- Оценка эффективности контрмер

Риски

- Матрица оценки риска
- Шкала оценки риска
- Реестр информационных рисков
- План обработки рисков

Оценка возврата инвестиций

- Стоимость контрмер
- Экономический эффект
- Коэффициент возврата инвестиций

Указания по применению

Последствия утечек

1. Утрата конкурентных преимуществ, недополученная прибыль (утечка ноу-хау или клиентской базы)
2. Ущерб репутации (утечка ПДн клиентов, банковской тайны, внутренней финансовой отчетности)
3. Прямой финансовый ущерб: судебные издержки, штрафы со стороны регуляторов, компенсации пострадавшим, затраты на ликвидацию последствий инцидента (утечка данных третьих лиц, физ. лиц, клиентов, партнеров, контрагентов)

Средняя стоимость утечки: от $1.5 (Forrester Research) до $4.8 млн. (Ponemon Institute) или среднемесячный оборот организации

Global Trust Solutions

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

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

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

Пример: Влияние утечки на прибыль (Forrester Research)

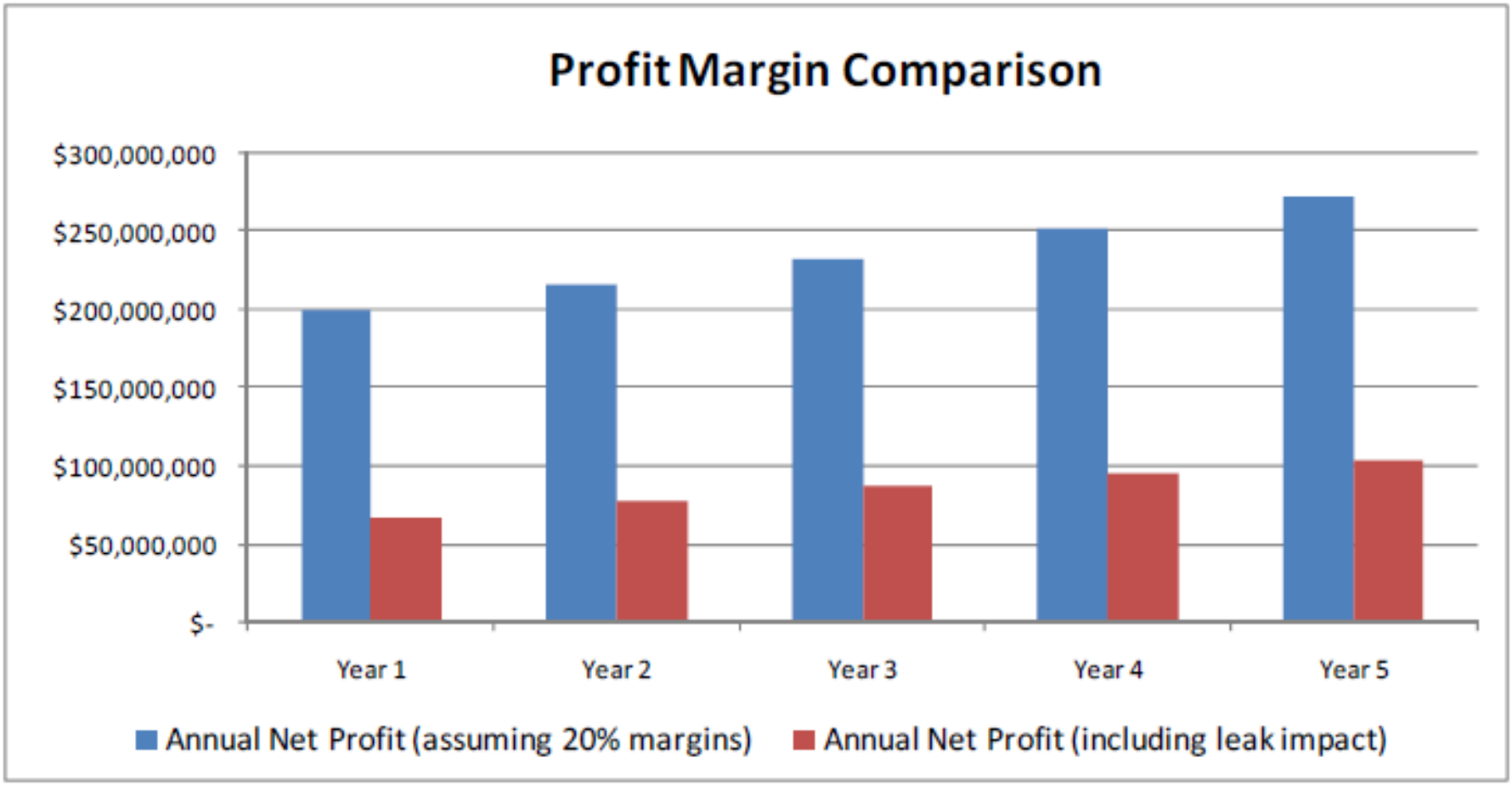


Figure 7: Estimated Impact to Profit Margin

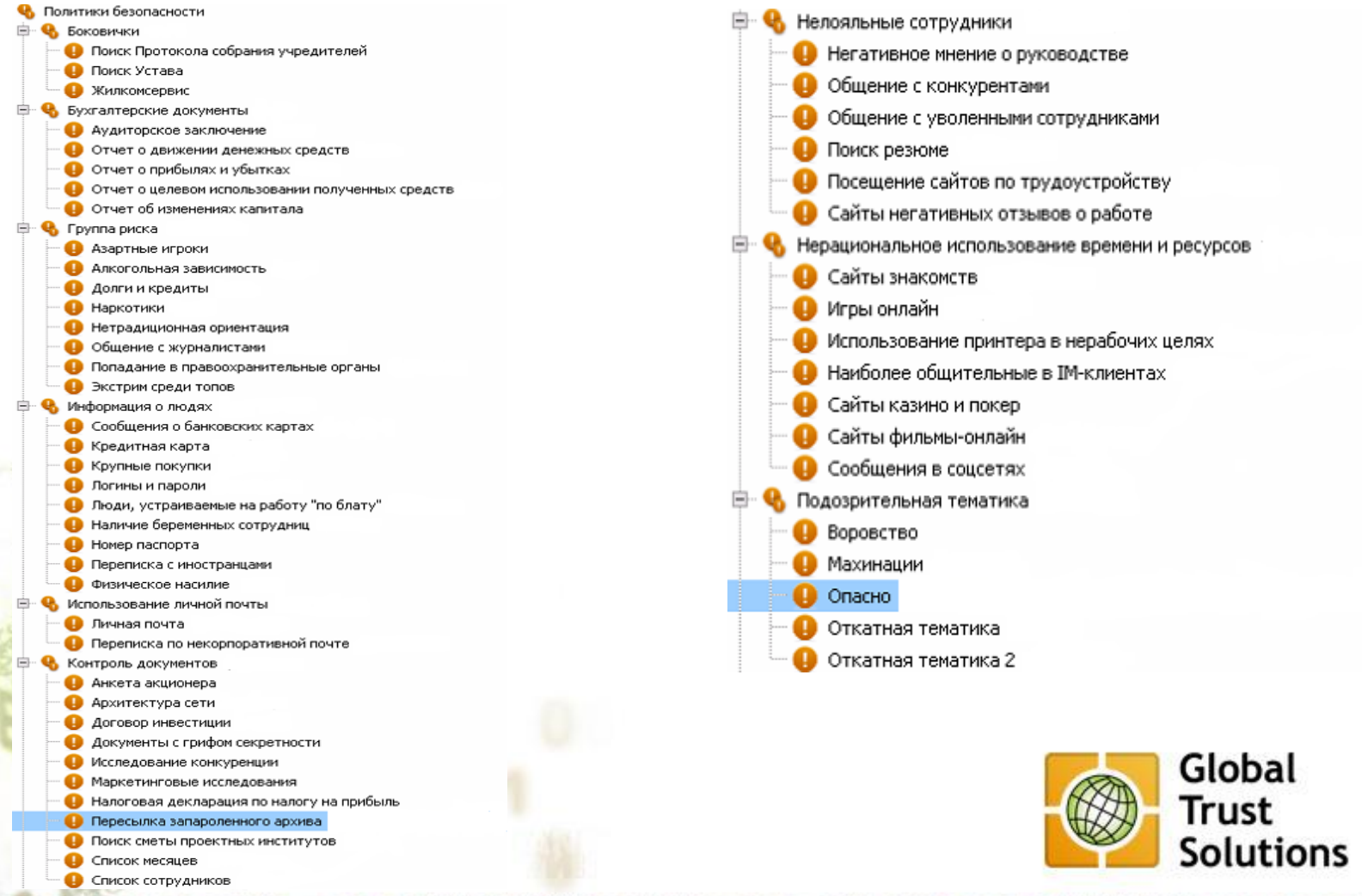
Пример: Сравнение стоимости DLP-системы и ущерба от утечки (Forrester Research)

	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

Модель угроз для DLP-системы (политики SearchInform AlertCenter)

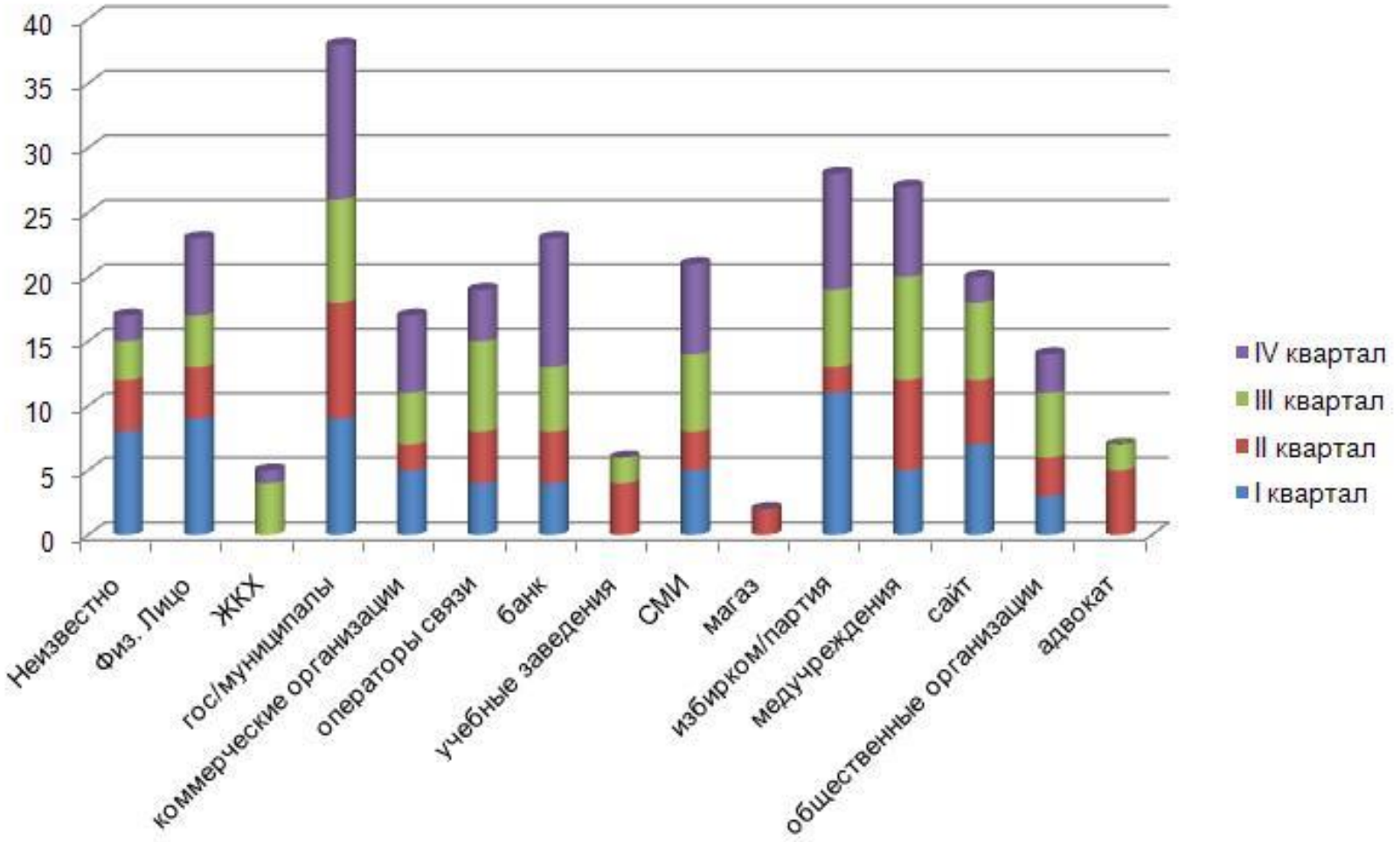


Global Trust Solutions

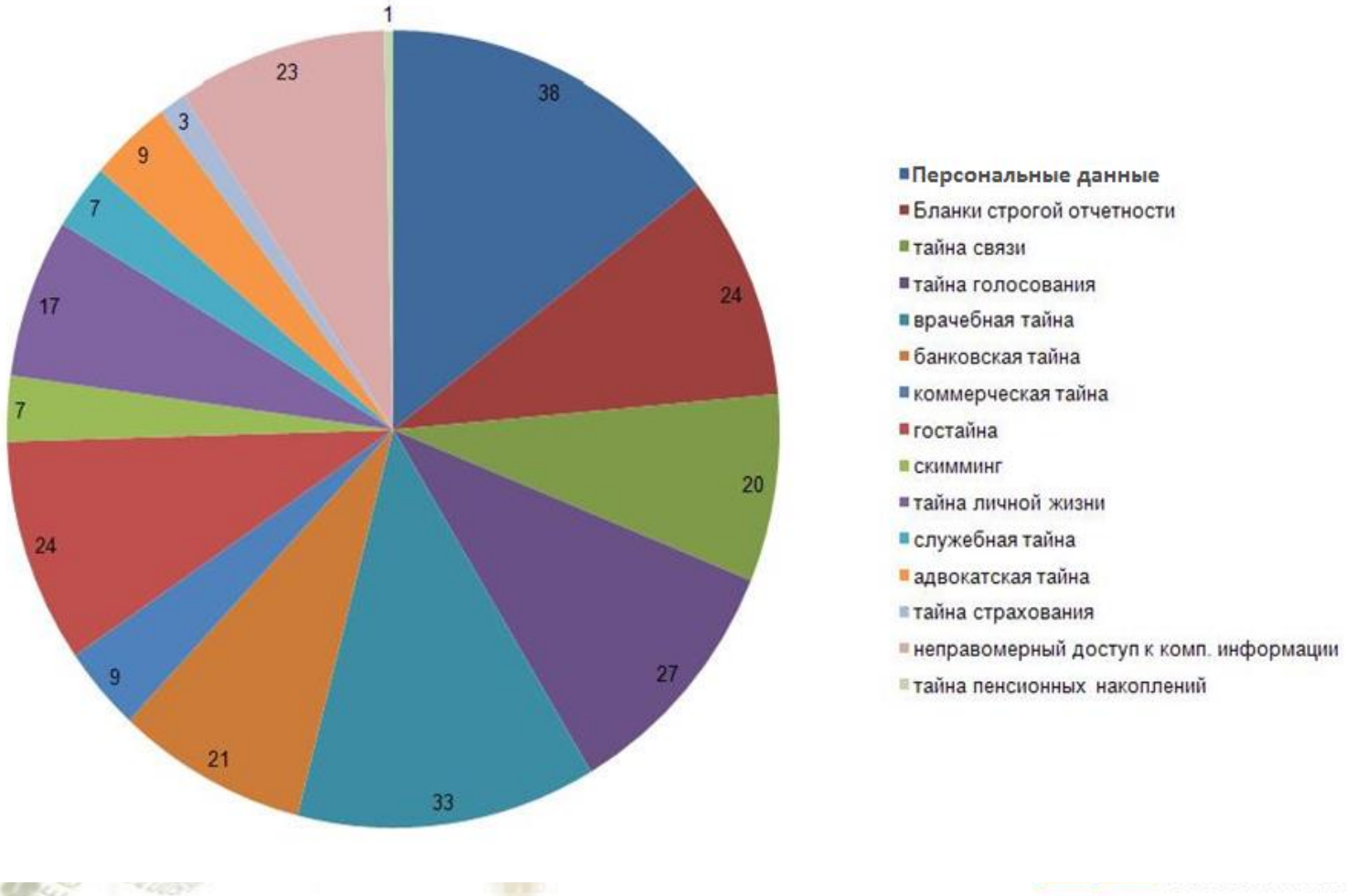
Частота реализации угроз (события ИБ SearchInform AlertCenter)

Логины и пароли (Информация о людях)	4816
Переписка по некорпоративной почте (Использование личной почты)	4150
Сайты фильмы-онлайн (Нерациональное использование времени и ресурсов)	2642
Личная почта (Использование личной почты)	1258
Сообщения о банковских картах (Информация о людях)	618
Посещение сайтов по трудоустройству (Нелояльные сотрудники)	389
Сайты знакомств (Нерациональное использование времени и ресурсов)	347
Опасно (Подозрительная тематика)	215
Поиск резюме (Нелояльные сотрудники)	193
Использование принтера в нерабочих целях (Нерациональное использование времени и ресурсов)	176
Махинации (Подозрительная тематика)	111
Откатная тематика 2 (Подозрительная тематика)	108
Сообщения в соцсетях (Нерациональное использование времени и ресурсов)	94
Кредитная карта (Информация о людях)	47
Список месяцев (Контроль документов)	44
Игры онлайн (Нерациональное использование времени и ресурсов)	37
Откатная тематика (Подозрительная тематика)	36

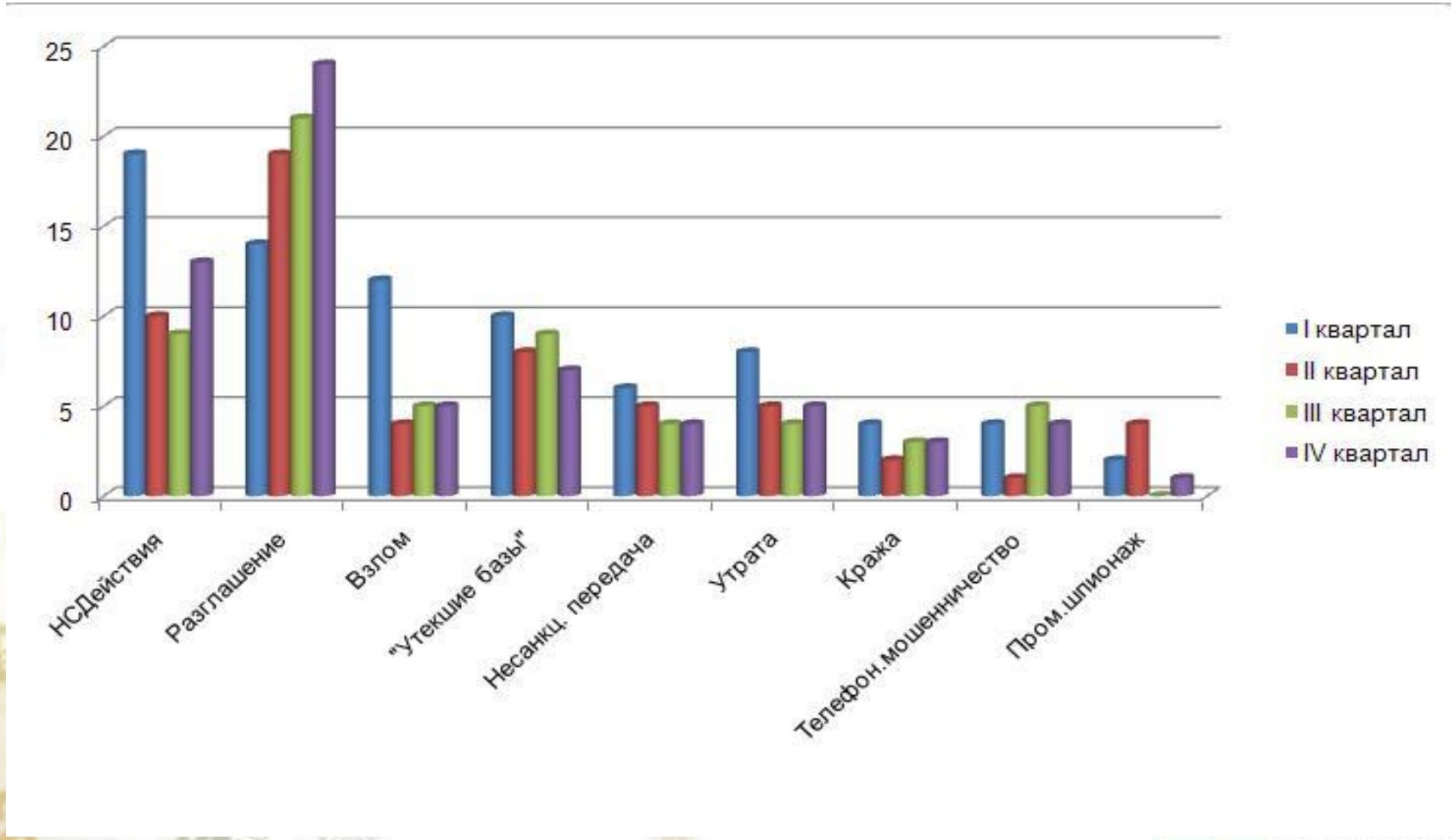
Распределение утечек по источникам за 2012 (263 инцидента по данным SearchInform)



Распределение утечек по типам информации (SearchInform)



Распределение утечек по способам получения информации за 2012 (SearchInform)



Эффект от внедрения DLP-системы (уменьшение среднегодовых потерь)

	До внедрения	**После внедрения**
Частота реализации угрозы (инцидентов за 1 год)	0,02	0,002
Величина уязвимости (% успешных попыток слива)	0.95	0,1
Размер ущерба (тыс. руб.)	2 145 000	2 145 000
Среднегодовой ущерб (ALE)	40 755	429

- Частота реализации угрозы = количество инцидентов в год / количество организаций
- Размер ущерба (ценность всех защищаемых DLP-системой активов) = среднестатистическая стоимость аналогичной утечки

Global Trust Solutions

Возврат инвестиций для DLP-системы

[Коэффициент возврата инвестиций (ROI)] = ([Уменьшение среднегодовых потерь] – [Стоимость защитных мер]) / [Стоимость защитных мер]

Уменьшение среднегодовых потерь (ALE)	201 630
Стоимость защитных мер (TCO)	45 350
Возврат инвестиций (ALE – TCO)	156 280
Коэффициент возврата инвестиций (ROI)	**3.5**

Global Trust Solutions

Выводы

Для оценки ROI DLP необходимо принимать во внимание:

1. Внутренняя и отраслевая статистика использования DLP-систем (результаты учета и анализа инцидентов).
2. Данные учета и классификации информационных активов.
3. Риски конфиденциальности носят спекулятивный характер. Одинаковые утечки могут иметь различные трудно-прогнозируемые последствия. Поэтому одной статистики для оценки ценности активов недостаточно, необходим анализ и прогнозирование с учетом особенностей конкретной ситуации.
4. Погрешность методов оценки (степени неопределенности результатов оценки).
5. Значение риска более точно выражается распределением вероятностей диапазона последствий, поэтому оценки ROI DLP – это распределение вероятностей.

Global Trust Solutions

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.

Global Trust Solutions

Библиография

1. The ROI of Data Loss Prevention (DLP), A Websense Whitepaper
2. Утечки конфиденциальной информации в России и в мире. Итоги 2015 года, ZECURION Analytics
3. ROI DLP. Можно ли посчитать?, Петр Сковордник, SearchInform
4. ИБ инциденты СНГ 2012, А. Бодрик, А. Токаренко, SearchInform

Global Trust Solutions

Спасибо за внимание!

Global
Trust
Solutions

ООО «ГлобалТраст Солюшинс»

Продукты и услуги в области
информационной безопасности

Астахов
Александр Михайлович

генеральный директор

123317, Россия, Москва,
Пресненская наб., 10, блок С,
Бизнес-центр «Регус»
www.globaltrust.ru

Тел.: +7 (495) 651-66-17
Моб.: +7 (495) 991-80-37
Факс: +7 (495) 967-76-00
E-mail: AlexAstahov@globaltrust.ru