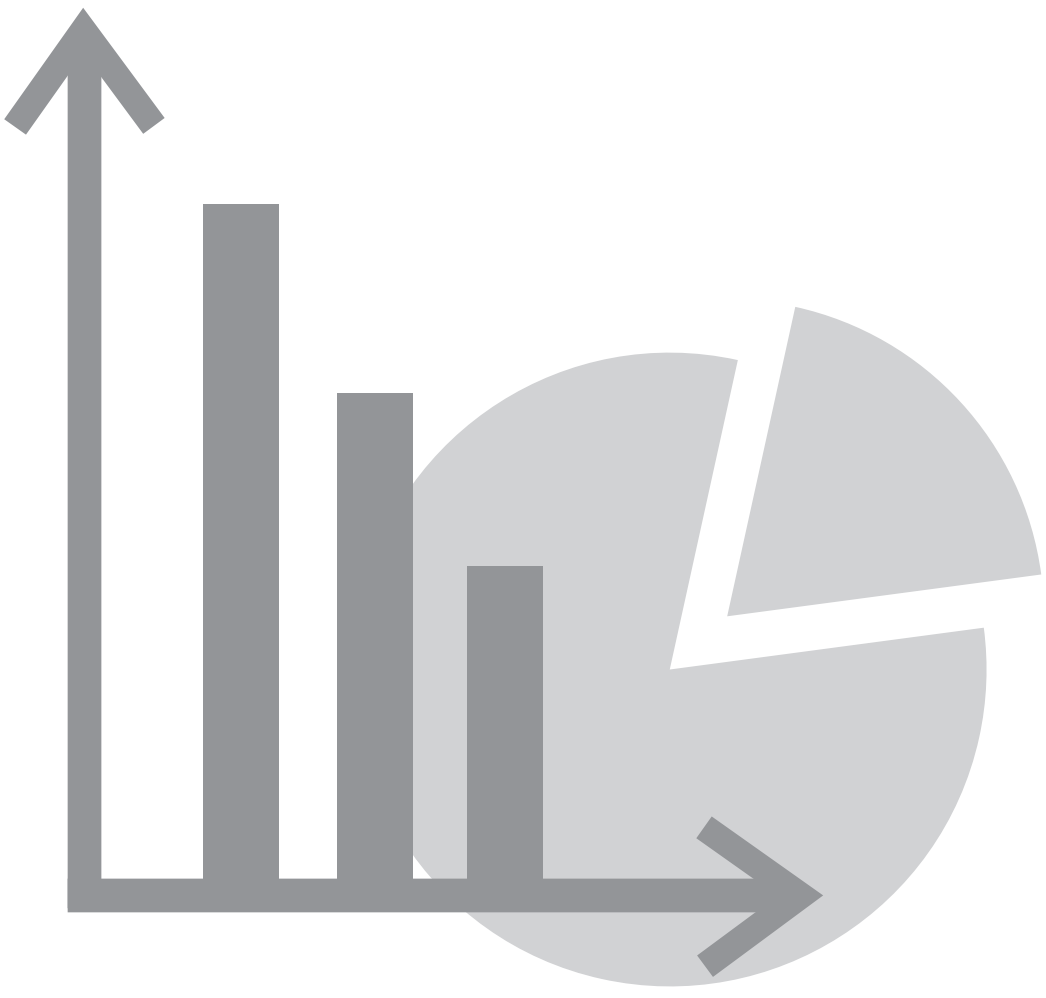
ISSP | Information Systems Security Partners

Аналитика

Количественный просчет рентабельности инвестиций от внедрения системы DLP



Проблематика

Деятельность современных организаций неотделима от обработки электронных данных, которые содержат не только открытую информацию, но и информацию с ограниченным доступом (данные о клиентах, финансовые отчеты, планы развития, проектная документация, интеллектуальная собственность и т.д.)

По режиму доступа информация делится на открытую и информацию с ограниченным доступом, которая, в свою очередь, по своему правовому режиму делится на тайную и конфиденциальную.

Конфиденциальная информация *- сведения, которые находятся во владении, пользовании или распоряжении отдельных физических и юридических лиц и распространяются по их желанию в соответствии с предусмотренными ими условиями. Лица, которые владеют конфиденциальной информацией, самостоятельно определяют режим доступа к ней, включая отнесение ее к категории конфиденциальной, и устанавливают для нее систему (способы) защиты.*

Доступ к информации с ограниченным доступом предоставляется авторизованным сотрудникам в рамках утвержденных полномочий. При этом, доступ к такой информации не дает сотрудникам права на ее распространение как внутри организации, так и за ее пределами среди неавторизованных получателей. Несанкционированное распространение сотрудниками информации с ограниченным доступом представляет серьезную угрозу для бизнеса, так как может привести к негативным юридическим и финансовым последствиям, а также нанести ущерб деловой репутации компании.

Тем не менее, утечки корпоративных данных происходят постоянно. Исследования западных аналитиков показывают, что более 98% инцидентов происходит не по злому умыслу сотрудников, а в процессе выполнения ими текущих бизнес-процессов.

Стандартные бизнес-процессы организации часто вступают в противоречие с требованиями политики информационной безопасности (ИБ). В отсутствие инструментальных средств контроля утечек формальные запреты не дают ожидаемого эффекта. Корпоративная политика ИБ на практике не ограничивает сотрудников в их стремлении поделиться внутренней информацией — как со своими коллегами, так и с сотрудниками других организации.

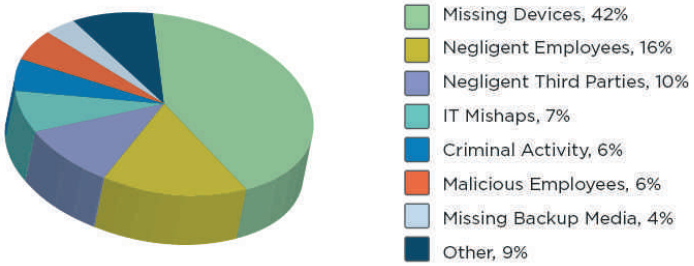
*Более **98%** инцидентов по утечке информации происходит в процессе выполнения сотрудниками текущих бизнес-процессов.*

Организации, продажи которых связаны с объектами интеллектуальной собственности, несут еще более ощутимые потери от утечки корпоративной информации. Вынос конфиденциальной информации для них может иметь сильное влияния на процесс исследования и разработки R&D (Research and development), на ожидаемый доход и на жизненный цикл активов в общем.

Таким образом, утечка информации – это не оперативный убыток. Она может иметь серьезные последствия в перспективе. Во многих случаях компании теряют свои конкурентные преимущества на рынке, а в некоторых случаях, вынос информации из компании приносит настолько серьезные последствия для бизнеса, что он уже никогда не вернется в нормальное состояние.

Более того, многие управляющие менеджеры не знают, что у них в компаниях происходит постоянная утечка информации, создающая бизнесу непрекращающиеся дополнительные барьеры, статьи расходов и более жесткую конкурентную среду на рынке. Иногда проходят годы, пока такой инцидент становится явным.

Затраты на нейтрализацию последствий в случае утечки информации и восстановление бизнеса высоки и могут возрастать со временем. По сравнению с этими цифрами, стоимость владения (TCO) системы предотвращения утечки информации , имеющей правовой режим информации с ограниченным доступом, отражает существенную экономию финансовых средств в краткосрочной перспективе и очевидные конкурентные преимущества компании в течение всего срока эксплуатации системы.



Исследования института Ponemon определили, что 85% опрошенных компаний имели подтвержденный инцидент утечки информации за последние 24 месяца.
Учитывая корпоративную бизнес-культуру западных компаний и законодательные регулятивные нормы, только 6% всех инцидентов произошли от преднамеренного выноса информации сотрудниками (умышленные инсайдеры), при этом, аж 42% инцидентов произошло из-за общего использования и утери USB-носителей с информацией.

Причем, эти 6% относятся к установленному факту кражи информации.

Многие же сотрудники попросту забирают всю информацию, с которой они работают, домой. Далее, она оседает у них на компьютерах, флешках, плеерах, и прочих устройствах, затем свободно распространяется среди друзей, знакомых (которые зачастую находятся в смежной бизнес-сфере), вследствие чего происходит утечка и свободное распространение конфиденциальной информации компании.

Определение убытков от утечки информации

Утечка информации, о разработках, проектах, объектах интеллектуальной собственности, приносит наибольший вред компании-владельцу такой информации, будь то производитель компьютерных процессоров нового поколения, или венчурная инвестиционная компания, готовившая инвест-пакет для прибыльного проекта.

Еще более тяжкий случай – это утечка конфиденциальной информации о клиентах, в том числе персональных данных, в компании, у которой такая информация находится во владении, пользовании и распоряжении (например, данные страховой компании о своих клиентах и т.д).

Затраты

- *Затраты на юридический иск (установление факта утечки информации, причинения ущерба и виновных лиц).*
- *Краткосрочное влияние на стоимость восстановления R&D.* Ключевые переменные здесь – этапы жизненного цикла R&D
- *Долгосрочные последствия на прибыльность и прогнозирование доходов.* Ключевые переменные здесь – этапы жизненного цикла, воспроизводимость, рыночный спрос
- *Системный аудит и аудит процессов для определения источника утечки*

Исследования Forrester (Trends: Calculating the Cost of a Security Breach. Forrester Research, Inc. April 10, 2007.) показывают, что в среднем утечка информации обходится в $1,5 миллиона экономического урона, в то же время исследования Ponemon Institute показывают $4,8 миллиона.

Убытки

- *Возмещение убытков третьих лиц*
- *Убытки организации, в том числе утрата деловой репутации (снижение гудвила как денежного эквивалента деловой репутации).*

Согласно исследованиям Forrester, составляющие прямых затрат на ликвидацию ущерба от утечки информации выглядят так:

Категория затрат	Описание	Затраты на 1 запись
Определение, реагирование и уведомление	Юридические затраты, уведомление клиентов, увеличение нагрузки на call center, маркетинг и PR, занижение стоимости предложения	$50
Потеря продуктивности работы сотрудников	Сотрудники отвлекаются от обыденного порядка работ, наем подрядчиков	$30
Реституция*	Компенсация ущерба пострадавших клиентов	$30
Отстроченный Ущерб	Потеря будущих возможностей бизнеса (потеря клиентов)	$98
Общая стоимость утери единицы записи		*$218*

На самом деле, каждый конкретный случай определяется размерами и природой организации, критичностью информации, которая была вынесена, и продолжительностью самого инцидента утечки.

В Украине под реституцией понимают возврат сторон в первоначальное положение, в частности, в случае признания сделки недействительной. Учитывая, что приведена западная практика, допустимо употребить и термин «реституция».

Таким образом, утечка 100 000 клиентских записей вырастает в $21,8 миллионов прямых и немедленных затрат. Чтоб отобразить это число в перспективе, сотруднику, который приносит $1000 прибыли для компании в час, пришлось бы работать 109 лет для возмещения этого ущерба.

Например, в середине 2005-го года, из компании ChoisePoint (риск-менеджмент) было похищено 145 тысяч записей об американских гражданах. Эти записи содержали адреса, имена, отчеты по операциям с кредитными картами, номера соц. страхования и прочую информацию, которую собирала компания.

Вследствие этого инцидента компания понесла более 45млн убытков, 2млн из которых компания потратила лишь на уведомление своих клиентов об инциденте – утечке информации. 5млн – был размер фонда выплаты пострадавшим
Снижение прибыли компании вследствие потери репутации составляло $20 – $25млн. Это, не учитывая непрямые затраты, например 10-ти миллионного штрафа, назначенного компании ChoisePoint Федеральной торговой Комиссией США.

Расширенные экономические последствия

Аналитики из Forrester and Ponemon определяют стоимость утечки записи определяется из прямых, непрямых затрат и потери возможностей: потеря доли рынка, невозможность вернуть утраченных клиентов, невозможность приобрести новых клиентов. Во многих случаях, список последствий продолжается, исходя из специфики определенного бизнеса, и стратегии компании, например, бизнес может потерять потенциальных инвесторов, или партнеров.

Исследования Forrester показывают приблизительную потерю около 20% клиентов при публикации факта утечки конфиденциальной информации. Если бизнес получает 80% прибыли от продаж своим постоянным клиентам, и вследствие утечки информации потерял 10% постоянных клиентов и зафиксировал 20% спад в приобретении новых клиентов – эти последствия будут являться катастрофическими.

Экономический эффект от утечки 100 000 клиентских конфиденциальных записей из компании с 100 миллионным годовым оборотом:

	Постоянные клиенты	Новые клиенты	Всего
Общий годовой доход	$80 миллионов	$20 миллиона	$100 миллионов
Потери бизнеса как процент от доходов	10%	20%	12%
Абсолютные потери бизнеса, в долларах	8$миллионов	4миллиона	$12 миллионов

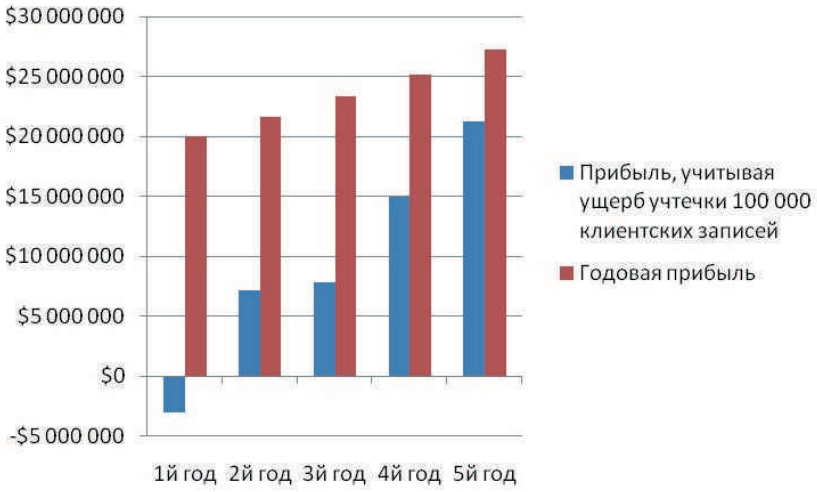
Экономический эффект от утечки *100 000 клиентских конфиденциальных записей из компании с 100 миллионным годовым оборотом равен 12-ти миллионам или* ***12% от прибыли компании*** *за первый год после инцидента*

Итак, общий экономический эффект равен 12-ти миллионам, или 12% от прибыли компании за 1й год после инцидента. Дополнительно, надо учитывать затраты (прямые и непрямые) на предотвращение последствий, которые существенно влияют на маржу, процент-операционную маржу и стоимость акций компании (EPS)
Давайте предположим, что бизнес (гипотетическая компания) имеет рентабельность в 20%, что отражает разумный показатель её операционной деятельности. После потери бизнес возможностей, из $20милионной годовой прибыли, останется только $8 миллионов на предотвращение последствий инцидента информационной утечки в первый год.
Если не брать в расчет статью «отсроченный ущерб», так как она почти целиком входит в просчитанные нами потери рынка, на 1й год возмещение ущерба обойдется компании в 11 млн долларов только прямых расходов!

	1й год	2й год	3й год	4й год	5й год
Годовой вал (предполагающий 8% роста)	$100 000 000	$108 000 000	$116 640 000	$125 971 200	$136 048 896
Годовая нетто-прибыль, (учитывая 20% рентабельность)	$20 000 000	$21 600 000	$23 328 000	$25 194 240	$27 209 779
Ежегодное возмещение ущерба из-за утечки информации	$11 000 000	$1 500 000	$1 500 000	$100 000	$500 000
Ущерб бизнесу из-за, сокращения клиентов	$12 000 000	$12 960 000	$13 996 800	$10 077 696	$5 441 956
Результирующее годовое сальдо	-$3 000 000	$7 140 000	$7 831 200	$15 016 544	$21 267 823

Из непрямых расходов, давайте только учтем ежегодные аудиты – для возврата лояльности клиентов.

Учитываем также дополнительные ежегодные бюджеты на PR $1 000 000 и реконструкцию процессов ИТ $500 000. Также учтем сокращение процента потери бизнеса до 8% в 4м году и до 4% в пятом, благодаря инвестициям в PR.



Внедрение DLP решения

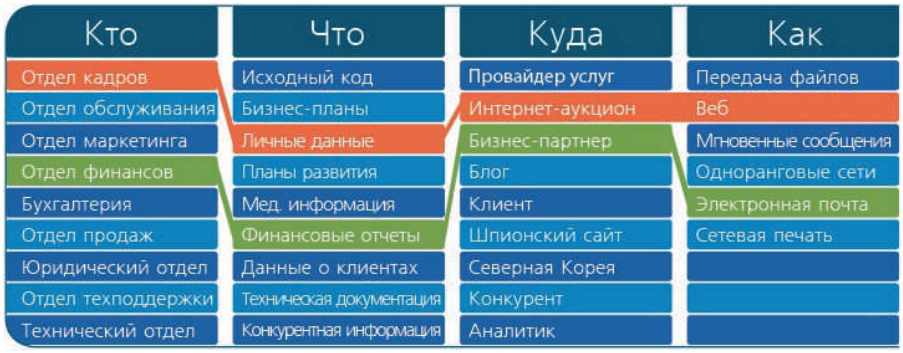
DLP (Data Leak Prevention) – это автоматизированная ИТ система, препятствующая утечкам или краже информации из организации.

DLP внедряется в существующую ИТ систему на предприятии и контролирует все информационные потоки, происходящие в компьютерной сети и на компьютерах сотрудников, выявляя инциденты несанкционированной передачи информации.

За счет оперативного анализа данных и автоматического применения политик безопасности, независимо от того, работают пользователи в корпоративной сети или вне ее, DLP система предотвращает вынос информации за пределы контролируемой ИТ системы.

Для того, чтобы DLP решение выявляло конфиденциальный контент в сессии, ему необходимо указать все информационные активы организации: базы данных, документы, архивы с указанием критичности содержащейся там информации. Далее, система осуществляет автоматическое обнаружение и классификацию данных, хранящихся в сети организации

DLP решение анализирует содержание, контекст и направление передачи данных, позволяя управлять тем, кто может пересылать информацию, какую информацию разрешено пересылать, кому она может быть адресована и какими способами осуществляется пересылка.



Возврат инвестиций от внедрения DLP системы:

Инвестиции в DLP систему можно разбить на 3 категории:
- стоимость программного обеспечения
- стоимость внедрения и настройки
- стоимость сопровождения системы

Стоимость программного обеспечения – те инвестиции которые необходимы для приобретения лицензий программного продукта. Количество лицензий напрямую зависит от количества сотрудников в организации. Например, организация, имеющая 1200 сотрудников инвестирует порядка $75 на лицензию на одного сотрудника в год. Итоговая инвестиция в программное обеспечение и аппаратное обеспечение обойдется приблизительно в $100 000. Для сравнения, лицензия на 10 000 пользователей обойдется в $175 000 в год.

Внедрение и настройка системы происходит профессиональными, сертифицированными инженерами, и также зависит от масштабов организации, политик и количества информационных активов, измеряется в человеко-часах.

Объем нашей гипотетической организации потребует на установку, настройку и обучение персонала порядка $15 000. Стоимость сопровождения и управления системы проводится внутренними ресурсами организации.

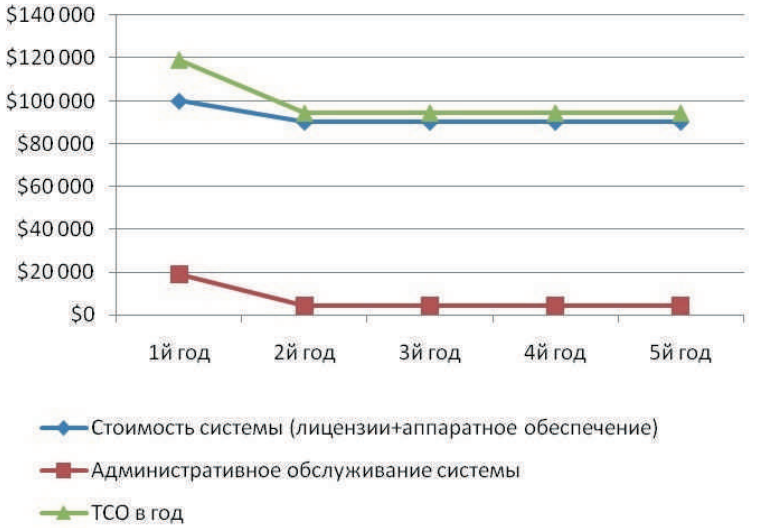
Категория затрат	CIO, Директор ИТ	Инженер информационной безопасности
Часов в неделю	1	6
Стоимость 1го часа	$25	$10
Стоимость в неделю	$25	$60
Стоимость в год (50 недель)	$1250	$3000
Суммарная стоимость администрирования системы	$4250	

Пока система производит автоматическую идентификацию и предотвращение потенциальных утечек информации, человеческие ресурсы компании будут вовлечены в:
- наблюдение и управление процессом
- применение и мониторинг соблюдаемости политик
- обработка исключений
- подача отчетностей руководству

Как правило, организации не требуется выделять специального человека для обслуживания DLP системы. Эти обязанности разделяются среди существующего штата ИТ специалистов и офицеров безопасности.

Итак, инвестиции в систему предотвращения утечек информации в организации с штатом сотрудников 1200 человек, следующие:

	1й год	2й год	3й год	4й год	5й год
Стоимость ПО, в год	$100 000	$90 000	$90 000	$90 000	$90 000
Инсталляция и настройка, обучение персонала	$15 000	$0	$0	$0	$0
Администрирование системы	$4 250	$4 250	$4 250	$4 250	$4 250
Суммарная стоимость владения (TCO)	$119 250	$94 250	$94 250	$94 250	$94 250



Процентное отношение инвестиций в DLP к рискам единой серьезной информационной утечки показывает экстремальную эффективность и выгодность решения. Из года в год компания не только ликвидирует риски информационной утечки, но и повышает эффективность операционных процессов.

	1й год	2й год	3й год	4й год	5й год
Суммарный ущерб от информационной утечки	$23 000 000	$14 460 000	$15 496 800	$10 177 696	$5 941 956
Стоимость владения системой DLP	$119 250	$94 250	$94 250	$94 250	$94 250
Инвестиции в систему DLP, как % от риска информационной утечки	0,5%	0,7%	0,6%	0,9%	1,6%

Способ сокращения рисковых фондов и предотвращения угрозы кражи информации очевиден. За полпроцента от величины риска компания может защитить себя от него.

Преимущества от внедрения системы DLP

Организации, которые внедрили DLP решение также получают дополнительную выгоду от ее использования. Они получили возможность усовершенствовать бизнес-процессы и увеличить операционную эффективность. Ключевая идея повышения доходности – это сфокусироваться на основных бизнес-процессах, определяя и исправляя поврежденные.

Многие организации имеют четко документированные политики информационного менеджмента, но они нуждаются в механизме мониторинга и регулирования этих политик. Без механизма контроля эффективный и действенный процесс может стать жертвой халатности сотрудника.

Фокусируясь на основных, критических бизнес-процессах, вы можете усиливать их DLP решением, которое помогает вам удостоверится, что процесс работает в наиболее эффективном русле, а организация показывает максимальную операционную действенность.

В дополнение ко всему, решение DLP дает ситуативную осведомленность в том, кто , куда и как отправляет какие данные, предоставляя прикладные знания для исправления некорректного процесса.

ООО “Информейшн Системс Секьюрити Партнерс”

03056, Киев, ул. Полевая 24
тел. +380 44 393 15 66
факс +380 44 393 15 67
e-mail info@issp.ua
web www.issp.ua