



DLP и частная жизнь

Деликатный баланс

Денежкин Владимир,
Генеральный директор компании Трафика

Познакомимся

Компания **Трафика**, российская компания-разработчик технических решений для защиты конфиденциальной информации компаний различного масштаба

Трафика основана в конце 2008 года в Москве.

Среди наших партнеров: Актив-софт, АВВУУ, НИИ КСС, РКСС, МГУПИ.

Среди наших заказчиков как крупные компании: В2В банк, Росгосстах, так и небольшие туристические агентства, поставщики элитных автомобилей и многие другие.



АВВУУ



лига
безопасного
интернета



B2B Bank
БАНК БИЗНЕС ДЛЯ БИЗНЕСА



trafica
ADVANCED NETWORK
TECHNOLOGIES

Чем мы занимаемся

Компанией разработан программный продукт **Monitorium** - система мониторинга и фильтрации корпоративного сетевого трафика, предназначенная для предотвращения утечки и распространения конфиденциальной информации через Интернет.

- **Monitorium** в реальном времени осуществляет мониторинг и/или блокировку нежелательного исходящего трафика на основании правил политики безопасности компании

Впервые в России **monit****orium**

система защиты информации от утечек через Интернет адаптирована, в том числе и для «малых компаний» (SMB):

- *доступна по стоимости,*
- *проста в установке*
- *проста в использовании.*



Постановка задачи

**Защита интересов
бизнеса**

**Соблюдение
этических норм**



Большее количество утечек - неумышленные

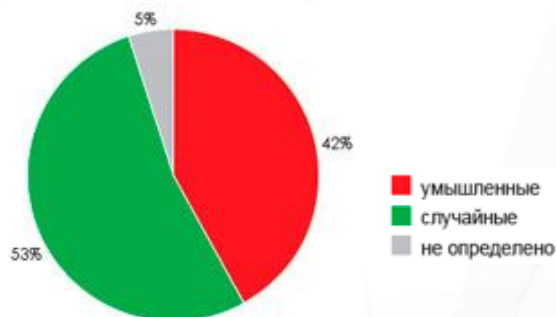
По опубликованным данным лидера российских DLP-систем InfoWatch:

Динамика роста утечек, 2006-2010 гг.



Динамика роста утечек в 2010 году по сравнению с предыдущим 2009 годом изменилась несущественно. Вместе с тем, аналитики отмечают существенный рост среднего размера ущерба от утечки.

Соотношение случайных и умышленных утечек, 2010 г.



В истекшем году случайные и намеренные утечки продолжали колебаться около соотношения 60/40.

Наиболее крупные утечки информации за 2011 год

- 26/10/2011. Персональные данные 1,6 млн абонентов **МТС** размещены в Интернете.
- 18/07/2011. В выдачу поисковых запросов Yandex попали СМС, отправленные с сайта сотового оператора **Мегафон**.
- 08/2011. Более 7 тыс. пенсионных накоплений граждан переведены из **ПФР** в **НПФ** без ведома пострадавших.

...От их всевидящего глаза,
От их всеслышающих ушей...



“Жизнь под контролем Google”

- СОРМ
- Google Analytics
- Яндекс Метрика
- Карты Visa, Mastercard
- Конкурентные разведчики с Avalanche
- Геолокационные данные мобильных телефонов



... анализируют, систематизируют, синхронизируют и строят прогнозы...

Определимся с терминами

Перлюстрация — просмотр личной пересылаемой корреспонденции, совершаемый **в тайне** от отправителя и получателя.

- В понятии негласного просмотра личных сообщений, не законна для несубъектов оперативно-розыскной деятельности (ОРД)
- Для субъектов ОРД применение перлюстрации регламентировано соответствующими законами



Легитимный контроль - **гласный** аудит электронных сообщений в компании, как контроль использования ресурсов компании.



Законодательная защита от нелегитимного контроля переписки

Статья 23 Конституции РФ

«п. 1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

п. 2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.»

Статья 138. УК РФ

«п. 1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.»



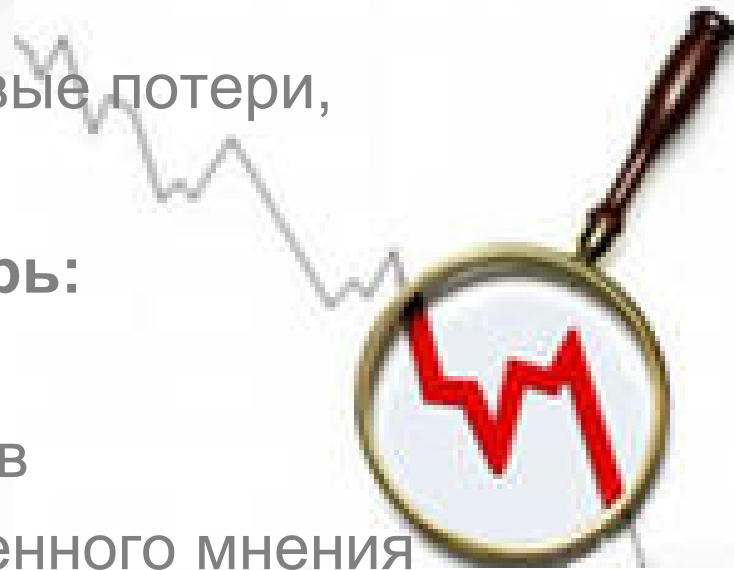
Последствия утечек информации для бизнеса

Экономические:

- ✓ Прямые и косвенные финансовые потери,
- ✓ Упущенная выгода

Состав потерь:

- Затраты по судебным искам
- Штрафы регулирующих органов
- Ухудшение имиджа и общественного мнения
- Снижение конкурентоспособности за счет:
 - Потери лояльности клиентов
 - Репутационных издержек: потеря доверия со стороны партнеров, инвесторов, государства
 - Снижение лояльности сотрудников



Правовое обоснование легитимности контроля исходящего трафика



п. 3 Статьи 17 Конституции РФ :

«Осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц».

п. 1 Статьи 10 ГК РФ *Пределы осуществления гражданских прав.*

«Не допускаются действия граждан и юридических лиц, осуществляемые исключительно с намерением причинить вред другому лицу, а также злоупотребление правом в иных формах.»

Правовое обоснование легитимности контроля исходящего трафика

Статья 209 ГК РФ. Содержание права собственности

«п. 1. Собственнику принадлежат права владения, пользования и распоряжения своим имуществом.*

п. 2. Собственник вправе по своему усмотрению совершать в отношении принадлежащего ему имущества любые действия, не противоречащие закону и иным правовым актам и не нарушающие права и охраняемые законом интересы других лиц, в том числе отчуждать свое имущество в собственность другим лицам, передавать им, оставаясь собственником, права владения, пользования и распоряжения имуществом, отдавать имущество в залог и обременять его другими способами, распоряжаться им иным образом.»

**Адреса и ресурсы принадлежат работодателю на праве собственности или пользования, отсюда его гражданско-правовые полномочия (права) по их использованию (в том числе - просмотру). Право пользования ими у работника возникает лишь в силу прямого согласия работодателя в рамках исполнения им трудовых функций.*



Правовое обоснование легитимности контроля исходящего трафика

ТК РФ

«Статья 21. работник обязан:

- *добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором; соблюдать правила внутреннего трудового распорядка;*
- *бережно относиться к имуществу работодателя.*

Статья 22. работодатель имеет право:

- *требовать от работников исполнения ими трудовых обязанностей и бережного отношения к имуществу работодателя, соблюдения правил внутреннего трудового распорядка»*



Российская судебная практика

МОСКОВСКИЙ ГОРОДСКОЙ СУД

в своем Определении* признал законным расторжение трудового договора за разглашение охраняемой законом тайны, а именно коммерческой тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей



* Определение московского городского суда от 2 декабря 2010 г. по делу N 33-37435

Зарубежная судебная практика

Практика Европейского Суда По Правам Человека (ЕСПЧ) позволяет банкам и компаниям, при правильном документальном оформлении процесса, знакомиться с сообщениями, отправляемыми работником по корпоративной электронной почте.



Копланд против Соединенного Королевства (Copland v. United Kingdom) (N 62617/00). Европейский Суд присудил выплатить заявительнице 3000 евро в счет компенсации причиненного ей морального вреда.*

в своем решении ЕСПЧ основной акцент сделал не на незаконность мониторинга, как такового, а на **недопустимость его без ведома** контролируемого лица

* http://www.napka.ru/press_centre/Article2/?id=129

Зарубежная практика. Вывод



На чем акцентировал внимание ЕСПЧ (решения Европейского суда обязательны для России). Ключевые цитаты:

- « **Заявительница не была предупреждена** о том, что ее звонки могут подвергаться мониторингу, и, следовательно, **имела обоснованное ожидание в отношении тайны переговоров** по своему рабочему телефону. Те же ожидания должны распространяться на электронную почту и использование Интернета».
- «Сбор и хранение **без ведома заявительницы** персональной информации, относящейся к использованию телефона, электронной почты и Интернета, представляли собой вмешательство в ее право на уважение личной жизни и корреспонденции».

* http://www.napka.ru/press_centre/Article2/?id=129

Анализировать переписку сотрудников, не нарушая их права на частную жизнь

Привести **правила внутреннего трудового распорядка** в соответствие с действующим законодательством:

1. Доведение информации до сотрудников под роспись:
 - Наличие гласного аудита в компании.
 - Запрет обработки с помощью корпоративных ресурсов информации, составляющей тайну личной жизни сотрудников.
 - Запрет личной переписки в рабочее время.
2. В компании должны быть определены сотрудники, ответственные за аудит. Перечень сотрудников должен быть документально закреплён.



По материалам: Alex Toparenko <http://securitywiki.ru>
Черняева Д.В. Злоупотребление правом и зарубежное трудовое право «Справочник кадровика», 2010. № 10-11

Вопросы?

Буду рад ответить на Ваши вопросы и надеюсь на плодотворное и взаимовыгодное сотрудничество

Контактная информация:

- <http://trafica.ru>
- Тел. +7 495 956 8421
- [e-mail: info@trafica.ru](mailto:info@trafica.ru)

СПАСИБО ЗА ВНИМАНИЕ