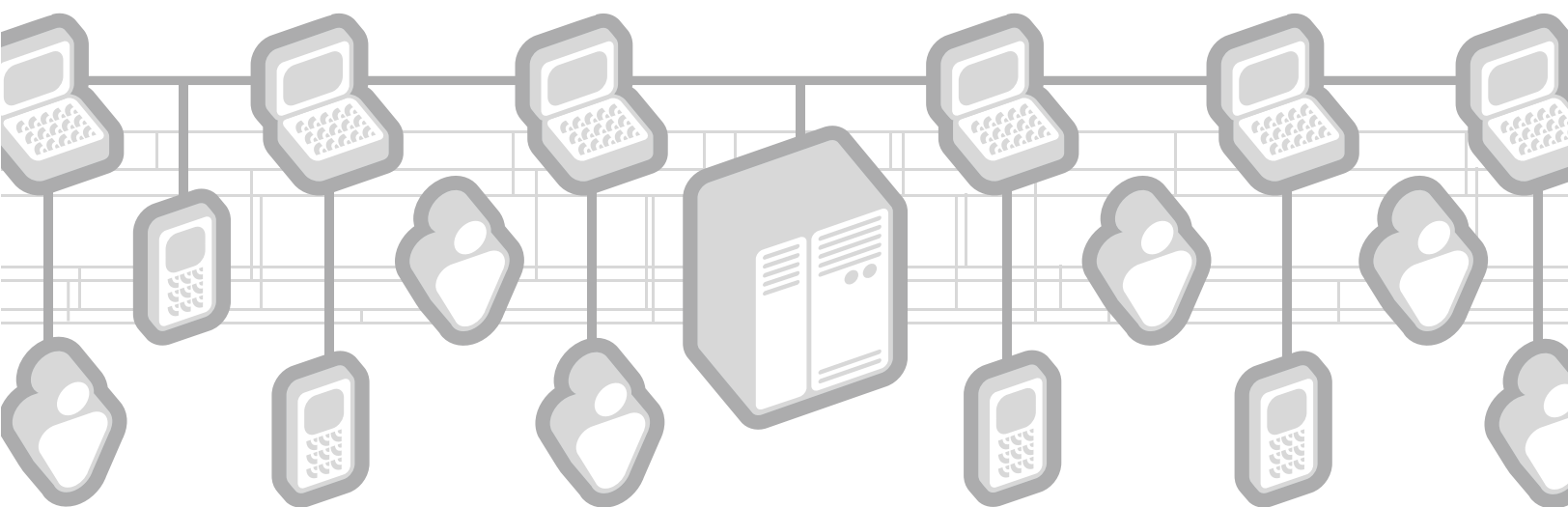
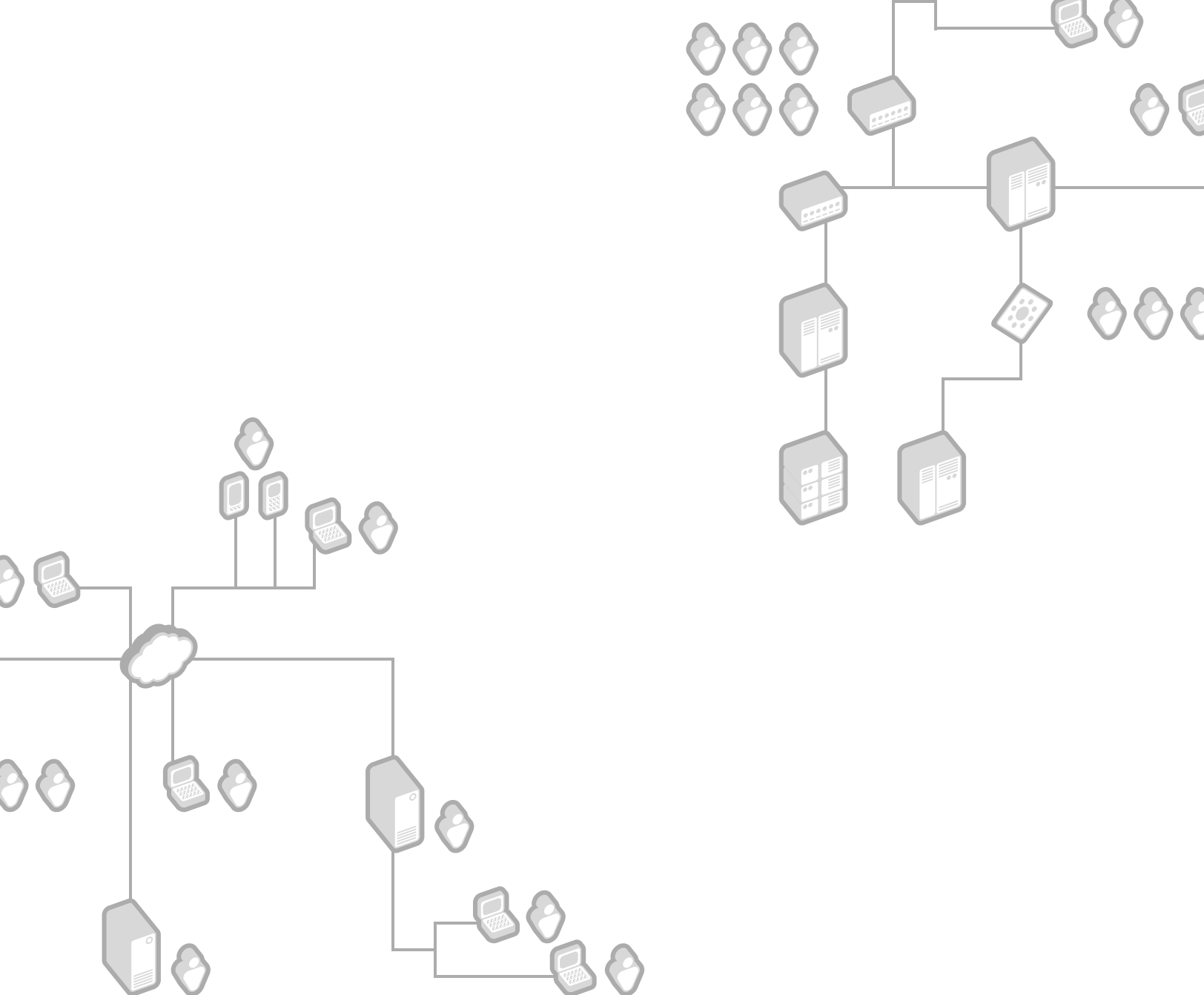


БОРЬБА С УТЕЧКАМИ ДАННЫХ





Этот документ был подготовлен LETA IT-company исключительно в целях информации. Содержащаяся в настоящем документе информация была получена из источников, которые, по мнению LETA IT-company являются надежными, однако LETA IT-company не гарантирует точности и полноты информации для любых целей. Информация, представленная в этом документе, не должна быть истолкована, прямо или косвенно, как информация, содержащая рекомендации по инвестициям. Все мнения и оценки, содержащиеся в настоящем материале, отражают мнение авторов на день публикации и подлежат изменению без предупреждения. LETA IT-company не несет ответственность за какие-либо убытки или ущерб, возникшие в результате использования любой третьей стороной информации, содержащейся в настоящем документе, включая опубликованные мнения или заключения, а также последствия, вызванные неполнотой представленной информации. Информация, представленная в настоящем документе, получена из открытых источников либо предоставлена упомянутыми в документе компаниями. Дополнительная информация предоставляется по запросу. Этот документ или любая его часть не может распространяться без письменного разрешения LETA IT-company либо тиражироваться любыми способами. Copyright © LETA IT-company





О проблеме инсайдеров

Защита от инсайдеров – одна из первоочередных задач, стоящих перед руководством предприятия/компании/бизнеса, желающим предотвратить финансовое мошенничество, кражу конфиденциальной информации или ее искажение, аппаратные и программные сбои, халатность сотрудников.

Так как инсайдеры – сотрудники компании, которые находятся внутри самой организации и наделены вполне легальными полномочиями, им гораздо проще получить доступ к интересующей их информации, чем любому злоумышленнику со стороны.

Действия инсайдеров зачастую приводят к серьезным негативным последствиям для бизнеса, таким как: финансовые убытки, потеря клиентов/партнеров, потеря авторитета и даже банкротство.

Кроме того, вступление в силу новых федеральных законов, в первую очередь, о коммерческой тайне и персональных данных, требует принятия эффективных мер по контролю над доступом к защищаемой информации и ее использованием.



Понятие внутренних угроз

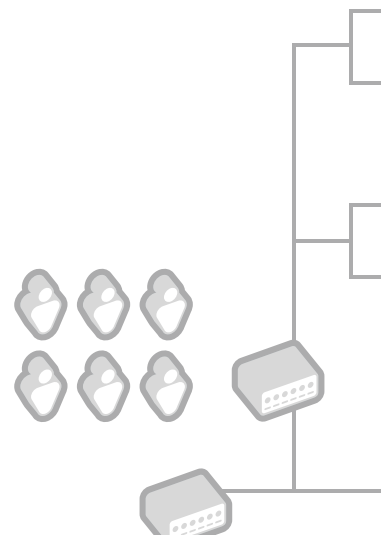
Всё многообразие угроз ИБ по одной из классификаций принято делить на внешние и внутренние.

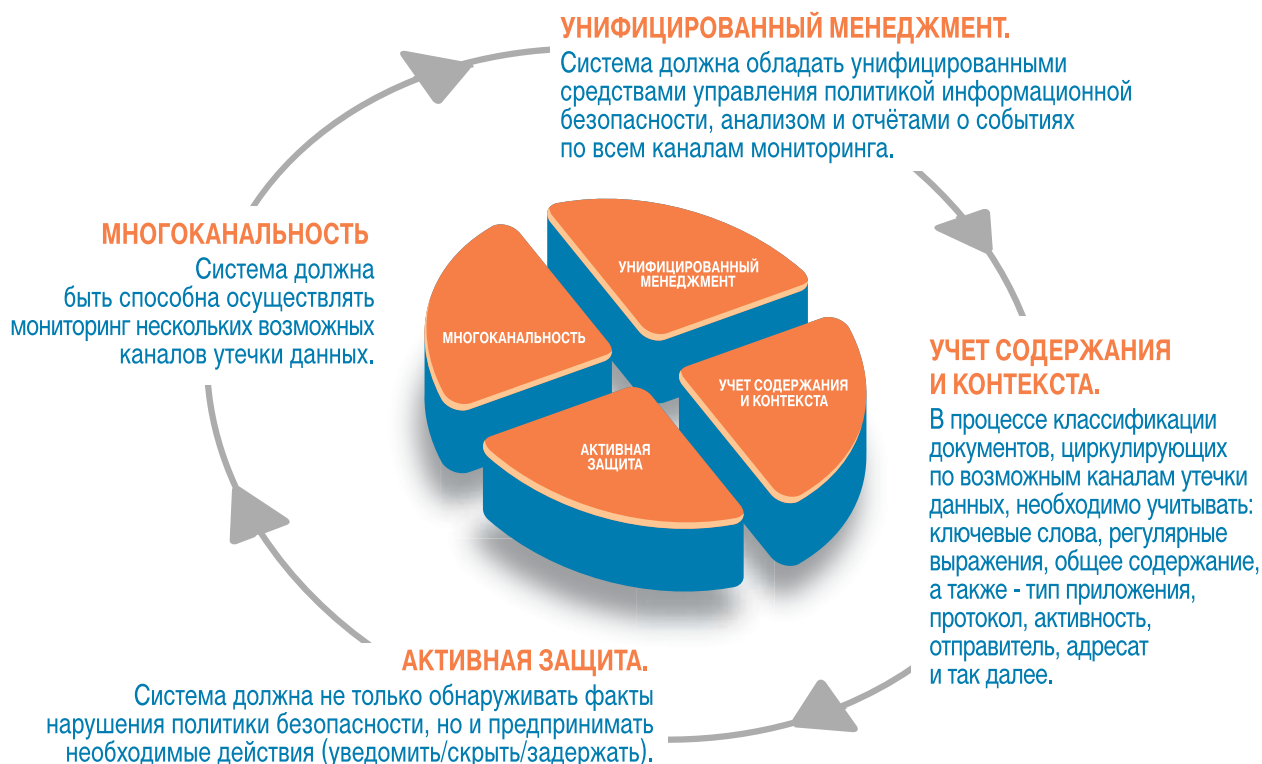
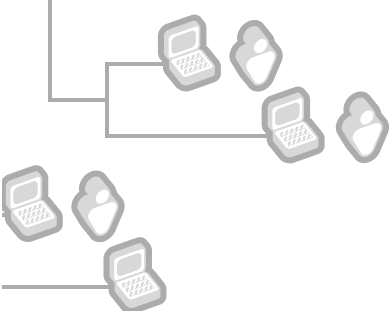
Под внутренними угрозами принято понимать любые инциденты утечки, блокирования или искажения конфиденциальной информации, возникающие в результате преднамеренных действий или небрежности собственных сотрудников компании. В данном случае исключениями будут являться разного рода техногенные катастрофы (пожары, террористические акты), происшествия природного характера (наводнения, ураганы), а также другие форс-мажорные обстоятельства, ущерб от которых был получен по вине сотрудников компании. Данный каталог будет рассматривать внутренние угрозы именно как манипуляционные действия с информацией, выраженной в цифровом виде (данными).

Что мы понимаем под DLP-системой и что она должна уметь делать

Обычно под системой предотвращения утечек данных (от английского Data Loss Prevention, DLP) понимается программное решение, которое строится на анализе потоков данных, пересекающих периметр защищаемой информационной системы, и контролю действий на конечных рабочих станциях. Цель DLP-системы в том, чтобы обнаружить в потоке исходящей информации – конфиденциальную и активно отреагировать на предполагаемую попытку утечки.

Наиболее стройные и непротиворечивые критерии принадлежности к DLP системам были выдвинуты исследовательским агентством Forrester Research в ходе их очередного исследования данного рынка. Они предложили четыре критерия, в соответствии с которыми систему можно отнести к классу DLP.





Системы защиты от утечек данных

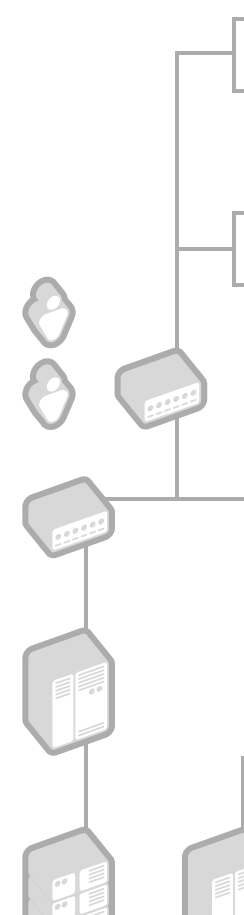
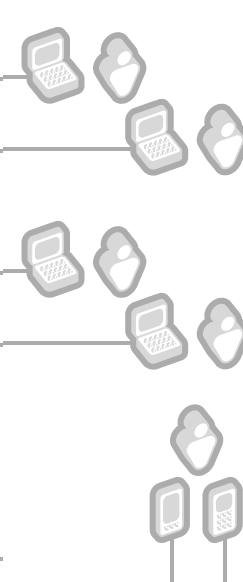
Это автоматизированное средство, позволяющее распознавать и/или блокировать перемещение конфиденциальных данных за пределы защищаемой информационной системы по всем каналам, используемым в повседневной работе.

Другие системы контроля за внешними устройствами

Кроме полнофункциональных программно-аппаратных DLP-решений существует также целый ряд разнотипных систем по защите данных в отдельных каналах утечки.

Наиболее распространенным является класс решений по контролю операций с внешними устройствами, ярким примером которых является съемный USB-накопитель. Такие системы не чувствительны по отношению к содержанию передаваемых (записываемых) данных. Вы сможете заблокировать попытки записи файлов определенного объема или заданного формата, но не сможете заблокировать запись файлов, содержащих защищаемые данные.

Тем не менее, в отдельных ситуациях подобные системы необходимы и достаточны для защиты корпоративной информации.





Опыт и компетенции LETA IT-company

LETA IT-company имеет одну из лучших экспертных компетенций в области DLP-решений на российском рынке информационной безопасности.

Наш опыт – это участие более чем в 20 проектах по внедрению DLP-решений и около 50 проектов по защите отдельных каналов утечки данных.

Наша компетенция подтверждается высокими партнёрскими статусами у ведущих российских и зарубежных вендоров DLP-решений.

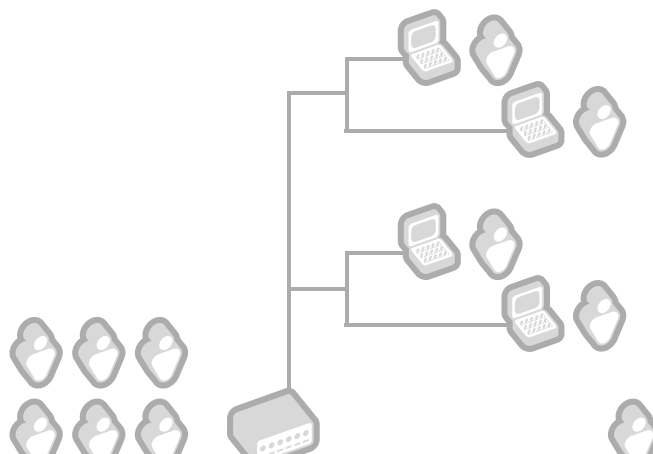
Подход LETA IT-company к внедрению DLP-решений

Главная особенность проектов по внедрению систем борьбы с утечками информации – все они уникальны. Существует несколько базовых подходов к внедрению DLP-систем, которые отличаются по:

- степени воздействия на существующие бизнес-процессы;
- охвату базы конфиденциальной информации;
- покрытию сценариев утечки информации;
- механизмам реакции на обнаруженные инциденты и т.д.

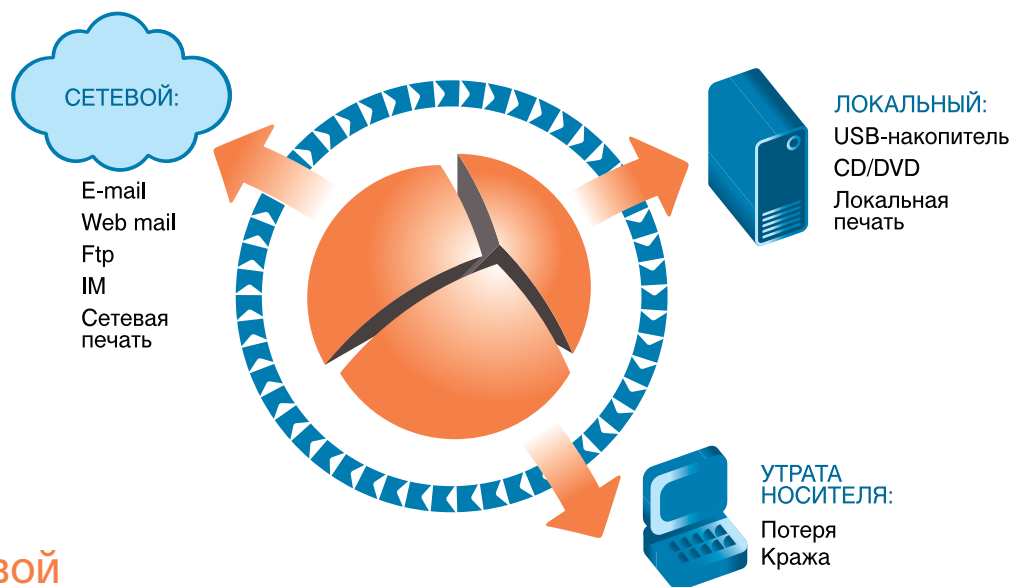
Кроме того, в каждой организации, в силу особенностей бизнес-процессов, всегда будет актуальна защита своей особенной группы каналов утечки: через корпоративную почту, через загрузку на внешние ftp-ресурсы, посредством мобильных устройств, внешних USB-накопителей, через печать на бумагу – список этот можно продолжать и продолжать.

Компания LETA старается делать все возможное, чтобы подобрать наиболее подходящее решение и оптимальный для каждого заказчика способ внедрения DLP-решения. Именно поэтому компания имеет в своем арсенале 4 различных вида полноценных DLP-решений – больше, чем кто бы то ни было на российском рынке. С учетом нашего опыта, накопленной компетенции и знания специфики конкретных продуктов, мы готовы предложить заказчику оптимальный вариант решения.



Основные каналы утечки

Принято выделять следующие основные каналы утечки конфиденциальной информации, защита которых возможна техническими средствами.



Сетевой

Предполагает отправку информации за «периметр» контролируемого информационного поля посредством:

- электронной почты;
- системы передачи мгновенных сообщений (ICQ, MSN, AOL);
- web-почты (mail.ru, gmail.com);
- ftp-соединения;
- печати документа на сетевом принтере;

Локальный

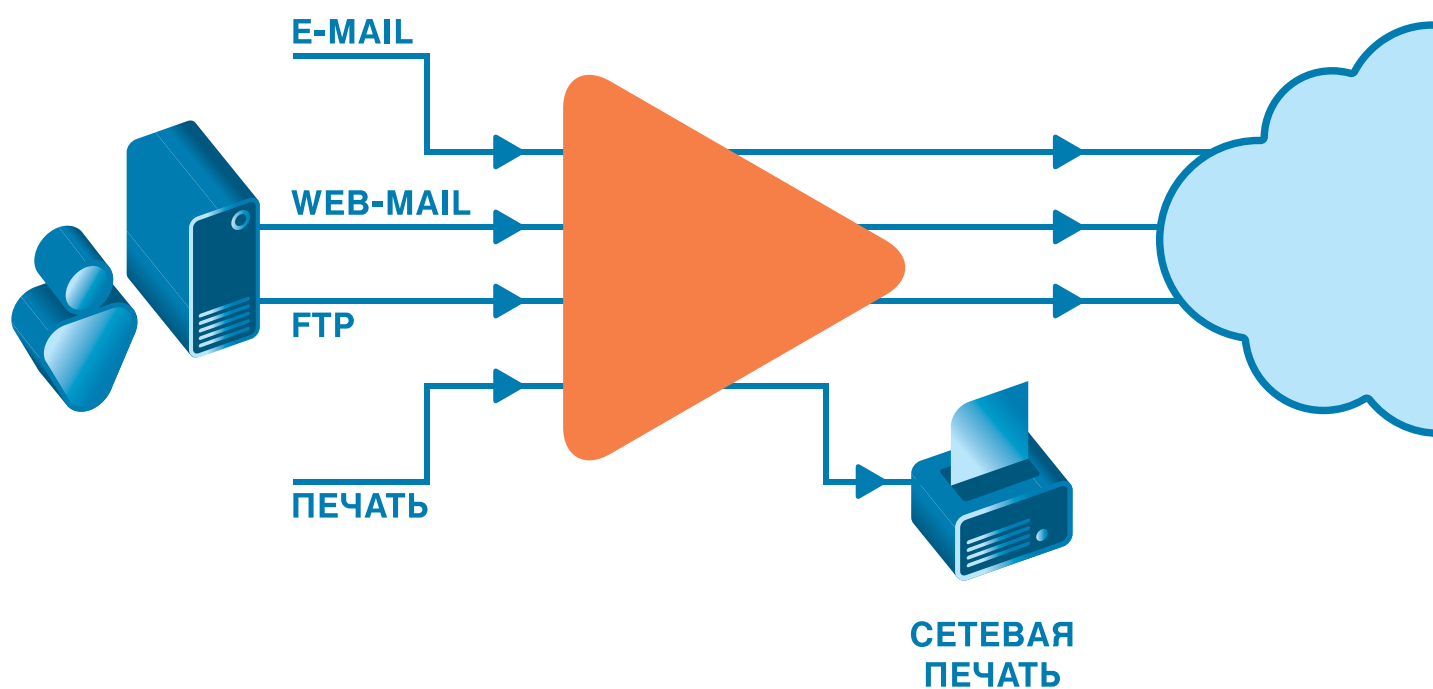
Предполагает использование локальных средств на конечной рабочей станции, таких как:

- внешние USB-накопители;
- съемные жесткие диски;
- запись на CD/DVD;
- локальная печать;
- создание локальных соединений WiFi, Bluetooth.

Утеря или кража носителя

В реальности является самым распространенным случаем, когда конфиденциальная информация становится доступной третьим лицам. Ноутбуки, смартфоны, USB-носители теряются или их воруют – почти каждая компания сталкивается с этим риском, и свести его к нулю невозможно.

Сетевой сценарий

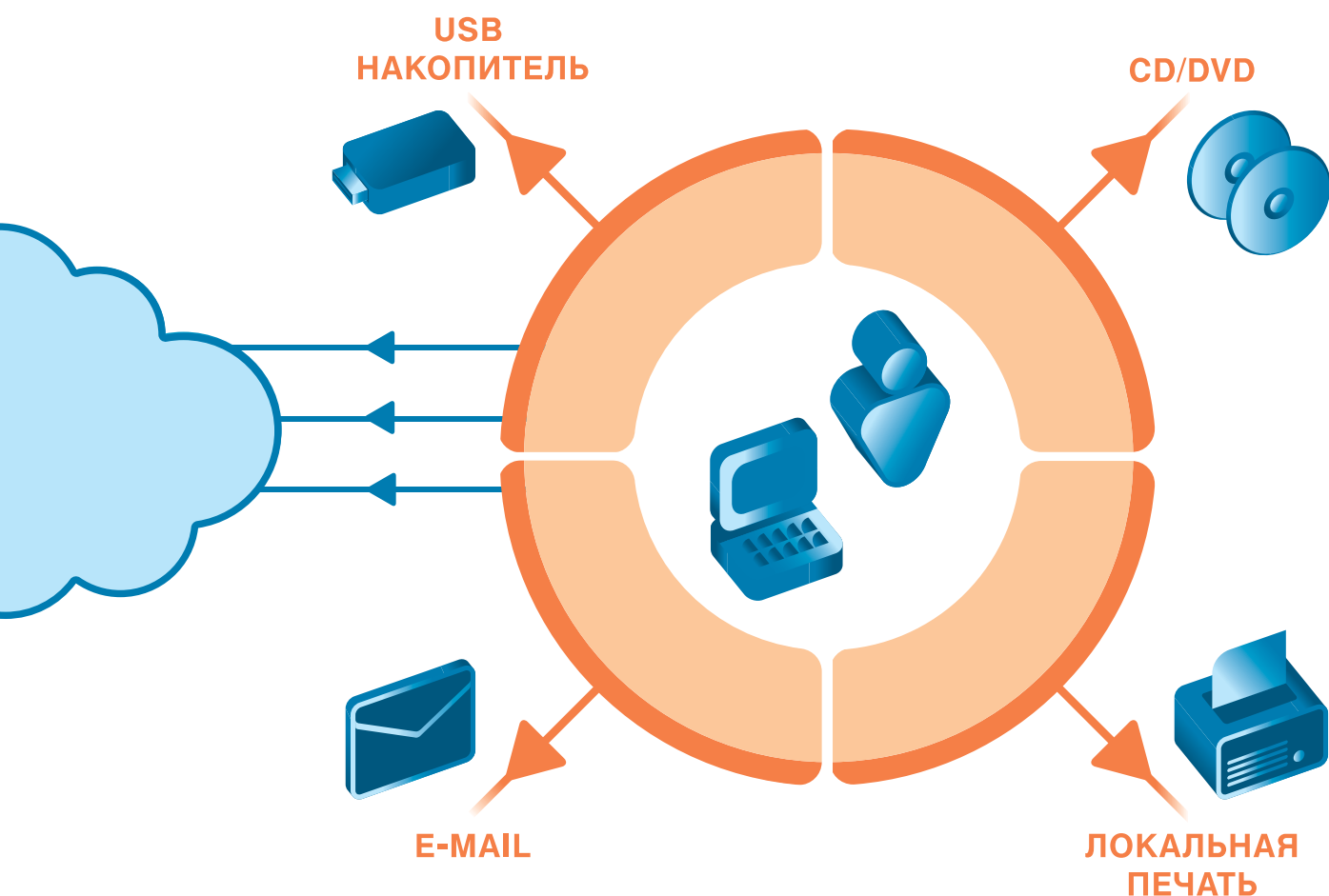


Аудит и блокирование подозрительных сообщений и пакетов

В случае противодействия утечкам с использованием сетевого сценария, DLP-система:

- осуществляет перехват сообщения;
- проводит анализ содержания отправки;
- информирует ответственного сотрудника (в случае обнаружения подозрительного содержания);
- применяет политики безопасности (приостанавливает отправку);
- вносит детали инцидента в журнал системы.

Локальный сценарий



Аудит и блокирование подозрительных действий пользователя

DLP-система, контролирующая операции с данными на компьютере пользователя:

- отслеживает факт обращения к конфиденциальной информации;
- блокирует все запрещенные действия (print screen, печать, формирование отправки через коммуникационные каналы и т.д.);
- блокирует обращение к файлу через программы, не внесенные в число разрешенных для работы с данным файлом;
- формирует журнал событий, который при очередном сеансе связи передается в центральную базу инцидентов.

Точки контроля и принятия решения

DLP-решение: что подлежит контролю

Контролировать каналы утечки информации можно с помощью двух разноплановых подходов:

- контроль передачи данных по каналам связи (Шлюзовое решение);
- контроль действий каждого конкретного пользователя, работающего с этими данными (Агентское решение).

ПОДХОД	СИЛЬНЫЕ СТОРОНЫ	СЛАБЫЕ СТОРОНЫ
ШЛЮЗОВОЕ РЕШЕНИЕ	+ Централизованное внедрение системы и администрирование политиками безопасности + Невидимо для пользователей и не создает нагрузку на локальные рабочие станции + Не зависит от вида операционных систем и программ, установленных на рабочих местах	— Контролирует только подключенные к корпоративной сети рабочие станции — Возможна дополнительная нагрузка на сеть (например в случае проведения сканирования рабочих станций) — Требуется дополнительное серверное оборудование
АГЕНТСКОЕ РЕШЕНИЕ	+ Наиболее полный охват возможностей по контролю рабочих станций, в том числе отключенных от корпоративной сети + Неприхотливо к каналам связи + Минимальные технические требования к серверу управления агентами	— На каждую рабочую станцию пользователя необходимо устанавливать дополнительную программу-агента — Повышенные технические требования к рабочим станциям — Требуется регулярная связь с сервером управления для обновления политик безопасности

DLP-решение: кто вовлекается в работу системы

- **Потенциальный нарушитель** – пользователь защищаемой информационной системы, у которого существует потенциальная возможность совершения правонарушений.
- **Владелец ресурса** – топ-менеджер компании, который напрямую понесёт финансовые или репутационные потери в случае утечки.
- **Офицер безопасности** – сотрудник компании, отвечающий за информационную безопасность.
- **IT-менеджер** – специалист, который обеспечивает функционирование информационной системы организации.



Стадии внедрения решения по борьбе с утечками

По рекомендациям лучших мировых практик и опыта выполнения аналогичных проектов, компания LETA предлагает придерживаться нижеописанной схемы.

1 Предпроектное обследование

Предпроектное обследование, в ходе которого определяется начальное состояние (организационное и техническое) информационной системы компании, согласовываются ожидания от проекта и разрабатывается техническое задание.

2 Пилотное внедрение

Существует несколько форматов пилотного развертывания, вот некоторые из них:

- проверка исходящего потока информации без блокирования отправки;
- проверка действий персонала в режиме аудита или блокирования;
- поиск в сети содержания конфиденциальных документов;
- отслеживание ограниченного числа конфиденциальных документов в рабочей среде;
- развертывание полноценного решения в ограниченном сегменте рабочей среды.

3 Разработка частной политики

Разработка процедур, правил, «матрицы доступа», эксплуатационной документации и иных документов, составляющих частную политику обращения с конфиденциальной информацией в компании.

4 «Обучение системы»

Настройка системы для работы с выделенным множеством документов.

5 Развертывание

Развертывание системы в рабочей среде предприятия и ввод её в продуктивную эксплуатацию

6 Оказание сопутствующих услуг:

- обучение персонала (технических специалистов и офицеров безопасности);
- разработка системы отчетности;
- интеграция с существующими системами сбора и анализа инцидентов;
- расширенная техническая поддержка решения.

Продукты по борьбе с утечками данных

По состоянию на вторую половину 2008 года на российском рынке доступны 4 полноценных технологических решения по борьбе с утечками данных (DLP). Приведенная таблица содержит их названия, краткую информацию о каждом из них и соответствующий партнерский статус LETA IT-company¹.

КОМПАНИЯ	ПРОДУКТ	О РЕШЕНИИ	ПАРТНЕРСКИЙ СТАТУС LETA IT-COMPANY
Websense	Data Security Suite	Лидирующее DLP-решение согласно ² авторитетным исследованиям 2008 года. Система интегрирована с продуктами web-безопасности и web-фильтрации.	Gold ChannelConnect Partner
InfoWatch	Traffic Monitor	Самое распространенное в России ³ решение по борьбе с утечками на 2008 год. Единственный из перечисленных продуктов, имеющий русскоязычный интерфейс.	Security Integrator
Symantec	Vontu DLP	Признанное ведущими корпорациями ⁴ из списка Fortune 100 решение, имеющее крупнейшую в мире базу инсталляций.	Platinum Partner
McAfee	Total Protection for Data	Интегрированное в единую систему управления продуктами McAfee DLP-решение, осуществляющее анализ и блокирование запрещенных действий пользователя на конечной станции.	Premier Partner Solution Provider

Специалисты LETA IT-company готовы провести «живую» демонстрацию всех перечисленных продуктов, используя уникальный тестовый стенд, развернутый в офисе компании.

В процессе демонстрации есть возможность увидеть и оценить основной функционал решений, пройти по всем основным сценариям использования, а также получить ответы на возникающие вопросы у сертифицированных инженеров по DLP-решениям.

Примечания:

¹ Настоящая таблица не может восприниматься как полноценное сравнение систем. Информация, приведенная в таблице, имеет справочный характер и приводится для ознакомления с некоторыми особенностями приведенных решений.

² The Forrester Wave: Data Leak Prevention, Q2 2008, Gartner Magic Quadrant for CMF and DLP Q2 2008

³ <http://www.infowatch.ru/customers>

⁴ <http://www.vontu.com/customers/>

Типизированная услуга – уникальное предложение компании LETA

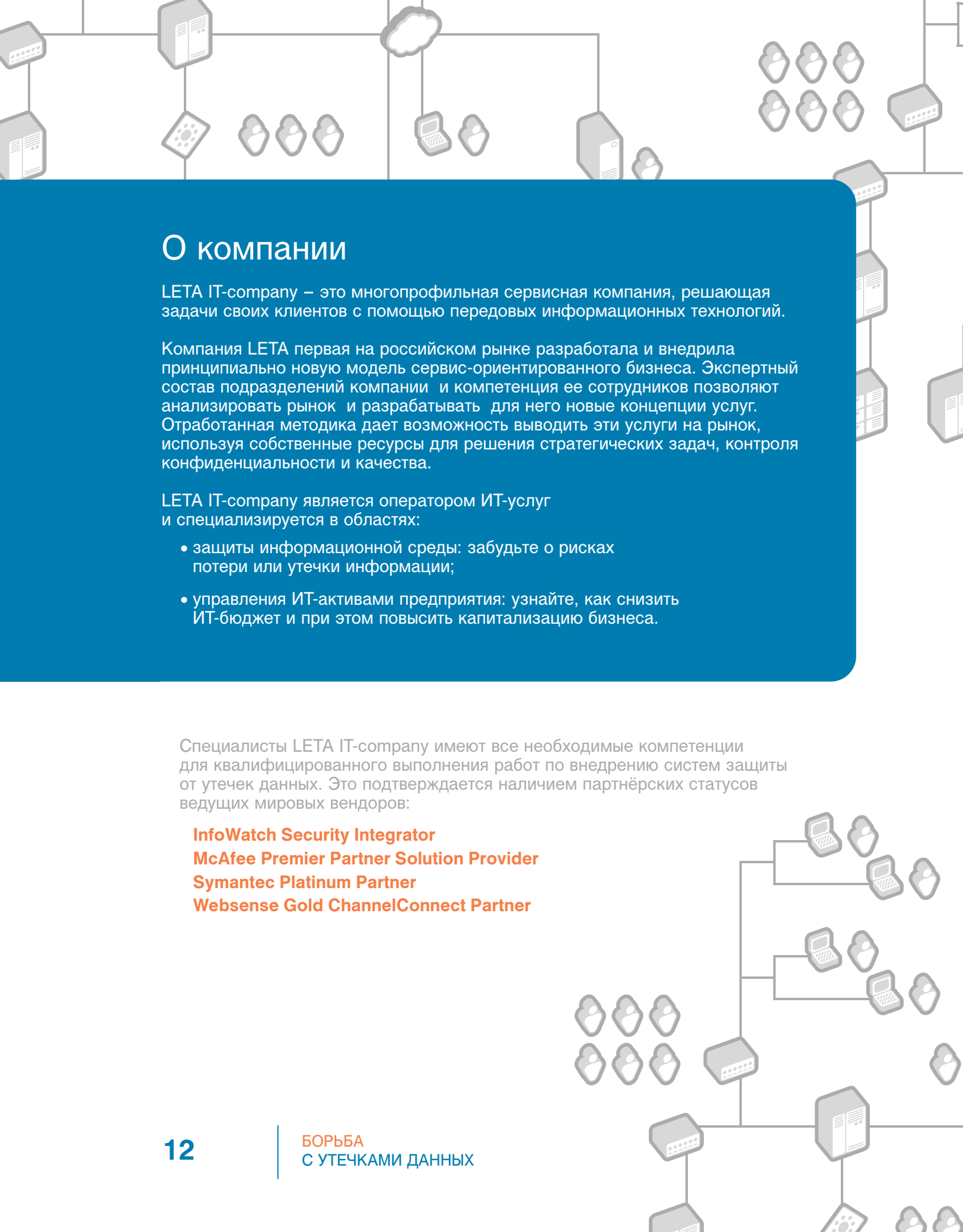
Задача борьбы с утечками стоит не только перед крупными корпорациями, которые сегодня являются «типичными» покупателями DLP-систем. Борьба с утечками приобретает актуальность и для относительно небольших компаний с парком от 100 компьютеров. Именно для нужд таких компаний в LETA IT-company разработана типизированная услуга «DLP-решение на 100 рабочих мест».

Типовой проект по внедрению McAfee DLP на 100 рабочих станций

№	ОСНОВНЫЕ ЭТАПЫ ПРОЕКТА	ДЛИТЕЛЬНОСТЬ В ЧЕЛОВЕКО-ДНЯХ
ЭТАП 0	Подготовка карты готовности заказчика	0,5
ЭТАП 1	Обследование Обследование информационной системы Разработка и согласование «Требований к решению»	3
ЭТАП 2	Внедрение решения Установка и настройка центрального сервера McAfee ePO Server Развертывание агентов McAfee ePO и DLP на рабочих станциях Настройка системы в соответствии с «Требованиями к решению»	2,5
ЭТАП 3	Разработка и согласование технического описания системы	2
ЭТАП 4	Обучение персонала заказчика Консультирование технического специалиста по настройке решения Консультирование бизнес-специалистов по использованию решения	2
	Общая длительность	10

Примечания

- Решение McAfee DLP входит в состав комплексного продукта McAfee Total Protection for Data, которое, кроме функционала по борьбе с утечками данных, включает шифрование дисков и контроль внешних устройств, в т.ч. USB.
- Решение McAfee DLP не поставляется без внедрения.
- Стоимость лицензий McAfee DLP на 100 узлов составит порядка 150 000 рублей.
- Стоимость сервисного предложения – 150 000 рублей с НДС (охватывает только развертывание McAfee Data Loss Prevention).
- Прочие сервисы, такие как полноценное внедрение системы защиты от утечек, развертывание других модулей в составе McAfee Total Protection for Data, подготовка инструкций, регламентов и политик – оказываются в рамках дополнительных соглашений.



О компании

LETA IT-company – это многопрофильная сервисная компания, решающая задачи своих клиентов с помощью передовых информационных технологий.

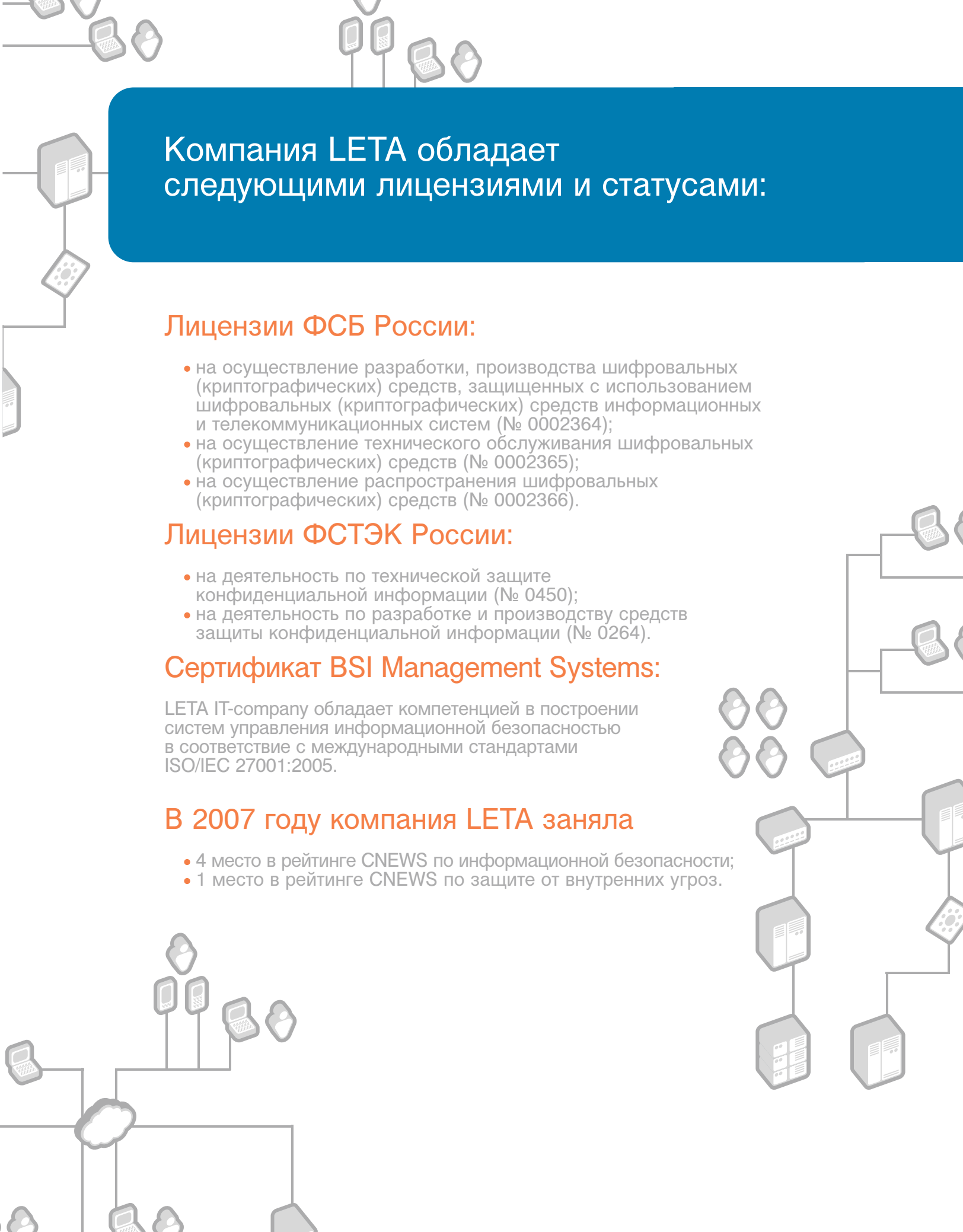
Компания LETA первая на российском рынке разработала и внедрила принципиально новую модель сервис-ориентированного бизнеса. Экспертный состав подразделений компании и компетенция ее сотрудников позволяют анализировать рынок и разрабатывать для него новые концепции услуг. Оработанная методика дает возможность выводить эти услуги на рынок, используя собственные ресурсы для решения стратегических задач, контроля конфиденциальности и качества.

LETA IT-company является оператором ИТ-услуг и специализируется в областях:

- защиты информационной среды: забудьте о рисках потери или утечки информации;
- управления ИТ-активами предприятия: узнайте, как снизить ИТ-бюджет и при этом повысить капитализацию бизнеса.

Специалисты LETA IT-company имеют все необходимые компетенции для квалифицированного выполнения работ по внедрению систем защиты от утечек данных. Это подтверждается наличием партнёрских статусов ведущих мировых вендоров:

InfoWatch Security Integrator
McAfee Premier Partner Solution Provider
Symantec Platinum Partner
Websense Gold ChannelConnect Partner



Компания LETA обладает следующими лицензиями и статусами:

Лицензии ФСБ России:

- на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем (№ 0002364);
- на осуществление технического обслуживания шифровальных (криптографических) средств (№ 0002365);
- на осуществление распространения шифровальных (криптографических) средств (№ 0002366).

Лицензии ФСТЭК России:

- на деятельность по технической защите конфиденциальной информации (№ 0450);
- на деятельность по разработке и производству средств защиты конфиденциальной информации (№ 0264).

Сертификат BSI Management Systems:

LETA IT-company обладает компетенцией в построении систем управления информационной безопасностью в соответствие с международными стандартами ISO/IEC 27001:2005.

В 2007 году компания LETA заняла

- 4 место в рейтинге CNEWS по информационной безопасности;
- 1 место в рейтинге CNEWS по защите от внутренних угроз.

