ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Противодействие утечкам информации с использованием DLP систем: кейсы и экономика

Развитие систем DLP

Специализированные технические средства для защиты от внутренних угроз стали массово выпускаться только после 2000 года.

1. Технологии сетевого мониторинга - без возможности блокировки утечки через сетевые протоколы (HTTP, SMTP…)

2. Добавлена функция блокировки информации при передаче через сеть.

3. Появляется возможность контроля рабочих станций за счет внедрения программных «агентов», что позволило:
- контролировать функции «copy/paste»;
- снимать скриншоты;
- осуществлять контроль передачи информации на уровне приложений.

4. Разработаны технологии поиска конфиденциальной информации на сетевых ресурсах и ее защиты, если информация обнаружена в тех местах, где ее не должно быть

АО ВТБ Специализированный депозитарий

Смена характера угроз и расширение конечных потребителей DLP систем предъявило к ним новые требования:

- **поддержка нескольких способов обнаружения утечки данных;**
- **поддержка всех популярных сетевых протоколов передачи данных;**
- **поддержка туннелирующих протоколов;**
- **прозрачный контроль защищенных SSL/TLS протоколов;**
- **поддержки нескольких методов распознавания ценной информации;**
- **избирательного блокирования передачи критически важной информации по любому контролируемому каналу;**
- **распознавания графики (OCR) и анализа содержимого;**
- **построение отчетности и т.д.,**

АО ВТБ Специализированный депозитарий

DLP в настоящее время

Работа с информацией (предотвращение утечки)

Контроль и предотвращение утечки информации:

- **конфиденциальная информация;**
- **информация относящаяся к интеллектуальной собственности (РИД), коммерческая тайна;**
- **персональные данные;**
- **информация ограниченного распространения**

Работа с персоналом (контроль сотрудников)

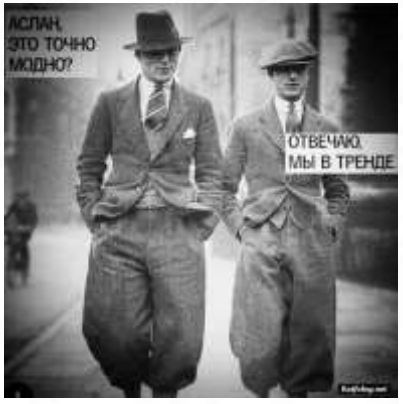
Контроль (борьба) за действием персонала:

- **рациональное использование служебного времени;**
- **легитимное использование ресурсов Компании;**
- **выявление действий криминальной/террористической направленности;**
- **не лояльные сотрудники/теневые лидеры**

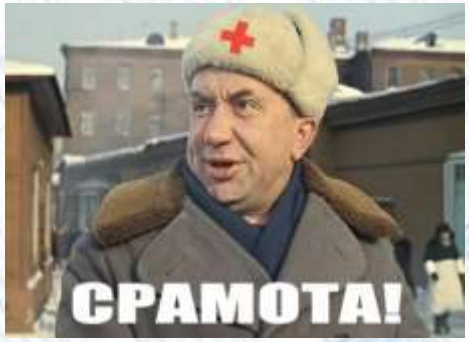
Приступаем к внедрению

А нужно ли?

I. Ищем ответ на вопрос: а зачем нам это нужно?



1. Это ооооооочень модно

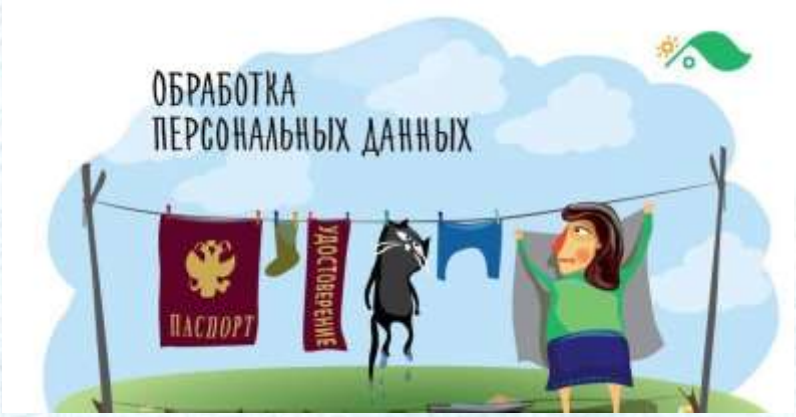


2. У него то есть, а я чем хуже

3. Вы финансовая организация и обязаны это сделать
683-П, 684-П (ГОСТ 57580.1 -2017)

4. У вас есть чувствительная информация, которую необходимо защитить (КТ, РИД)

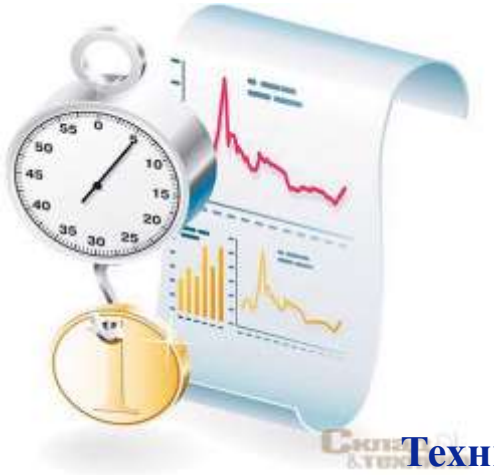
5. Защита от утечки персональных данных



6. Защищать то особо нечего, но хочу все знать

АО ВТБ Специализированный депозитарий

Так же необходимо учесть:



Стоимость и сроки внедрения, а затем и владения (техническая поддержка)

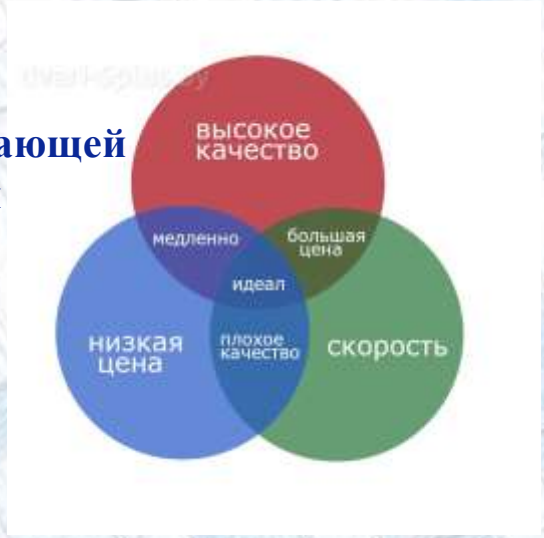
Технические возможности для разворачивания системы

Подготовленные специалисты для эксплуатации DLP

II. В зависимости от задач определяемся с необходимым набором функционала DLP

1. Проведение пилотных проектов: этап тестирования DLP систем

2. Определение DLP отвечающей ТЗ (предъявляемым требованиям)



3. Принятие решения

Юридические аспекты внедрения DLP

Внесение в трудовой договор информации:

Об осведомлённости и согласии работника:

- об использованием систем видеонаблюдения в служебных кабинетах;
- о том, что выданные материальные средства должны использоваться только для целей предусмотренных договорными отношениями, о запрете использования устройств в личных целях;
- что работодатель имеет право на получение доступа к информации о просмотренных работником веб-страницах в сети Интернет, содержанию отправленных и полученных по каналу корпоративной электронной почты сообщениях (электронных письмах), осуществлять мониторинг использования служебной телефонной связи;
- при работе в информационных системах работодателя ему не гарантируется конфиденциальность информационного обмена

Дополнительно, вышеуказанная информация может вносится в Инструкцию Пользователя по обеспечению информационной безопасности

АО ВТБ Специализированный депозитарий

Необходимо разработать:

1. Регламент/инструкцию по использованию DLP:
- **цели, которые достигаются и решаемые задачи в процессе эксплуатации DLP;**
- **роли и участники процесса эксплуатации (администратор ИБ, администраторы ИТ, офицер безопасности), зоны ответственности;**
- **порядок определения контролируемых параметров;**
- **порядок определения лиц подлежащих контролю;**
- **порядок предоставления/доступа к выходной информации;**
- **порядок и сроки хранения информации;**
- **порядок использования информации.**

2. Инструкцию Пользователям по требованиям информационной безопасности, с отражением вопросов касающихся эксплуатации DLP (определение что такое хорошо и что такое плохо, что можно делать, а что делать запрещено).

3. Инструкции по правилам настройки и эксплуатации:
- **Администратор ИБ;**
- **Администратор ИТ;**
- **Офицер безопасности (контролер).**

АО ВТБ Специализированный депозитарий

Возможные сценарии использования и измерение эффективности от использования

Ущерб, который можно измерить

Прямые финансовые потери:

- утрата важной информации;
- срыв распорядка рабочего дня;
- затраты на проведение расследования;
- потеря постоянных клиентов;
- Затраты на непланируемые мероприятия.

Потери не материального характера:

- ущерб репутации компании;
- снижение качества обслуживания;
- нарушение эмоционально-психологического состояния коллектива;
- снижение конкурентно способности на рынке

Не прямой ущерб:

- потеря потенциальных клиентов;
- материальный ущерб от разглашения КТ;
- моральный , физический или материальный ущерб от разглашения ПДн;

АО ВТБ Специализированный депозитарий

Использование DLP в процессе работы с информацией

Варианты использования	Что ищем/защищаем	Чего достигаем (каков эффект)
Поиск информации в локальных/закрытых ИС	Информацию, которая потенциально может быть отнесена к ГТ	Снижаем риск наступления уголовной ответственности, снижение репутационного ущерба
Противодействие утечки информации	Информация составляющая КТ, РИД	Предотвращение экономического ущерба в размере упущенной выгоды, в случае разглашения возможность взыскания /компенсации в судебном порядке
	Персональные данные сотрудников/клиентов	Предотвращение экономического ущерба в сумме возможного наложенного штрафа, компенсации за моральный ущерб в судебном порядке. Предотвращение репутационного риска связанного с уходом клиентов (упущенная выручка), не приходом новых клиентов
	Конфиденциальная информация	Возможность применение дисциплинарной ответственности к нарушителям, снижение репутационного риска
	Аутентификационная информация (логин пароль)	Позволило своевременно предотвратить НСД к критически важным ИС в целях их компрометации и вывода из строя
	Информация о выпущенных кредитных картах	Предотвращение судебных исков, экономического ущерба, защита ПДн

Использование DLP в процессе работы с сотрудниками

В процессе анализа информации	
Выявляемые признаки	**Эффект**
Выявление лиц из групп риска: - **азартные игры;** - **алкоголь, наркотики;** - **долги, кредиты;** - **крупные покупки.**	**Возможность предотвращения экономического и репутационного ущерба в виду попадания сотрудника в зону риска, возможность свершения противоправных действий направленных на извлечение незаконной выгоды, деструктивное воздействие на коллектив, снижение качества выполняемой работы, возможность ухода/недовольства клиентов.** **Возможное свершение противоправных действий: сопоставление значимых покупок и реальных доходов.** **Финансовые затраты на локализацию негативных последствий.**
Выявление лиц стремящихся сменить работу	**Внезапное увольнение сотрудников может привести к незапланированным затратам по:** - **поиску нового сотрудника;** - **Обучению и вводу в коллектив нового сотрудника;** **Невыполнение обязанностей по должности до ввода сотрудника в должность.** **Возрастание нагрузок на остальных сотрудников.**

АО ВТБ Специализированный депозитарий

В процессе анализа перехватываемой информации	
Выявляемые признаки	**Эффект**
Выявление неформальных деструктивных лидеров:	**Внесение разобщенности и смуты в коллектив. Срыв выполнения постеленных задач. Сопротивление инновациям. Экономический ущерб от деструктивной деятельности.**
Выявление неформальных лидеров:	**Использование для выполнения поставленных задач, вовлечение сотрудников и т.д.**

В процессе использования дополнительных функций	
Анализируемая информация	**Эффект**
Активность пользователей	**Рациональное и качественное использование рабочего времени (актуально на удаленке), оптимальное задействование сотрудников, перераспределение обязанностей**
Табель учета рабочего времени	
Активность процессов	
Эффективность работы сотрудников	

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Спасибо за внимание

Луганцев А.А.
18.02.2021