ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

DLP : выбираем, внедряем, эксплуатируем

Луганцев Александр
lugantsev@vtbsd.ru

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

DLP (Data Loss Prevention) — это **программный продукт для предотвращения утечек конфиденциальных данных в корпоративной сети.**

А так ли это на самом деле?

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Утечки конфиденциальной информации в 2022 году

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Не была внедрена DLP?

Не правильно настроена?

А может не противодействует ?

А может не защищает?

Комплексные ошибки при принятии решении о внедрении

Не инфобезом единым

DLP – сложное комплексное решение

I. Принимаем решение о внедрении. Зачем?

У него то есть, а я чем хуже

Вы финансовая организация и обязаны это сделать ГОСТ 57580.1 - 2017)

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

У вас есть значимая информация, которую необходимо защитить (КТ, РИД)

Защита персональных данных

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Определяем цели использование DLP

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
Экономическая безопасность **Информационная безопасность** 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

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Использование DLP в процессе работы с сотрудниками

В процессе анализа информации	
Выявляемые признаки	Эффект
Экономическая и кадровая безопасность 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.
Кадровая безопасность 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.

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 (для отдела персонала и руководителей подразделений)	
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

Пред внедрением необходимо понять и учесть

DLP – имеет высокую стоимость проекта как по внедрению так и по владению.

Кто является инициатором внедрения: ТОП, ЭБ, кадры, ИБ

DLP не внедряется на «голую» инфраструктуру, нужна определенная зрелость бизнес-процессов

Главный вопрос: цель внедрения, каков будет результат внедрения, какие решения будут приниматься по результатам работы системы

Как будем внедрять?

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Определили цели использования - в зависимости от задач определяемся с необходимым набором функционала DLP выбираем продукт

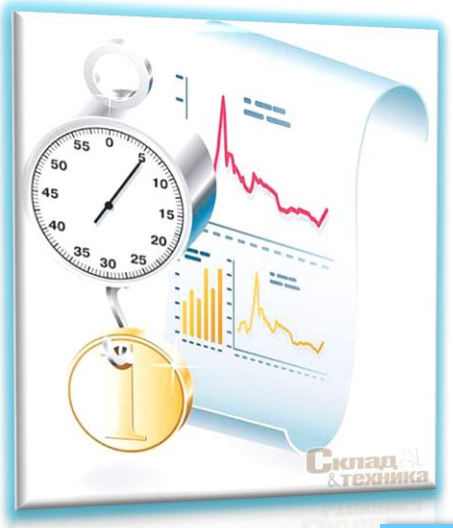
1. **Изучение и анализ рынка, функционал продуктов (референс, встречи, документация, стенды)**

2. Проведение пилотных проектов: этап тестирования DLP систем

3. Определение DLP отвечающей ТЗ (предъявляемым требованиям)

4. Принятие решения

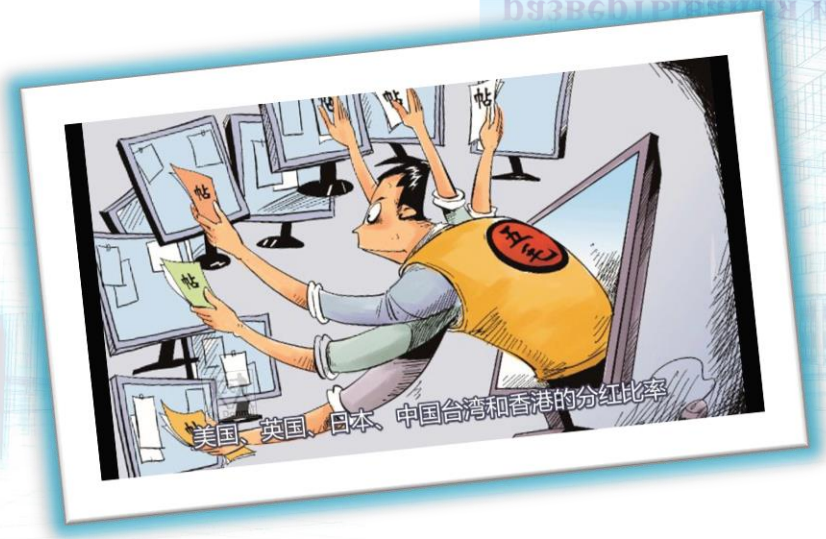
ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ



Так же необходимо учесть:

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

2. Технические возможности для развертывания и развития системы



3. Подготовленные специалисты для эксплуатации DLP

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Важный вопрос: режим работы системы

Blocking

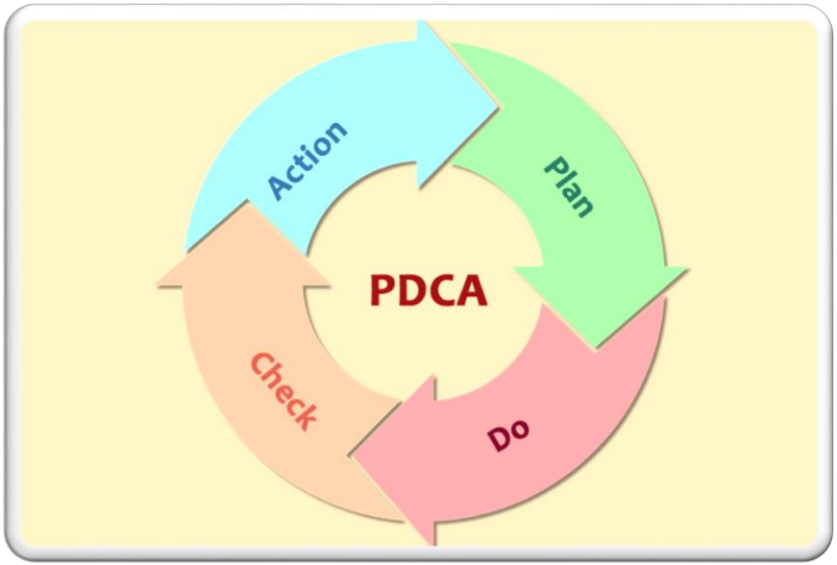
- ложные срабатывания;
- увеличение времени на обработку инцидентов;
-увеличение штата сотрудников.

Monitoring

Система не предотвращает угрозы, а информирует об их свершении

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Эксплуатируем



Планируем. Определяем цели системы, какую информацию будем защищать и как.
Реализуем. Реализуем политики и настройки DLP.
Анализируем. Эксплуатируем систему, анализируем получаемые результаты;
Корректируем. Изменяем политики с учетом результатов анализа.
Планируем. Новый цикл планирования. Учитываем изменившиеся цели, актуализируем информацию, применяем новые подходы. и т.д.

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

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

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).

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

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;

ВТБ СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ

Спасибо за внимание

Луганцев А.А.
05.04.2023