

Выбираем DLP систему правильно

Станислав Якунин

Руководитель группы поддержки продаж
решений кибербезопасности
stanislav.yakunin@softline.com



Data Loss Prevention



Мониторинг
движения
информации и
действий
сотрудников



Контроль
хранения,
перемещения,
изменения
информации и
труда
сотрудников



Предотвращение
утечек
информации,
устранение
рисков связанных
с инсайдерами,
повышение
эффективности
труда.

Почему?

Почему стоит рассматривать DLP к приобретению?



- A. Защита критической для бизнеса информации
- B. Соответствие требованиям регуляторов
- C. Мониторинг и контроль движения информации внутри периметра компании
- D. Мониторинг и контроль действий пользователей

Как выбрать?



Предложения рынка

Далеко не полный перечень того, что сейчас
есть рынке



Infowatch Traffic Monitor

Solar Dozor

Falcongaze Secure Tower

Smartline DeviceLock DLP

McAfee DLP

Symantec DLP

Forcepoint DLP

Trend Micro DLP

Zecurion DLP

Eset Safetica DLP

Стахановец

Функциональность

Возможности контроля

Возможности блокировок

Автоматизация и фильтрация

Мониторинг персонала

Построение отчетов

Граф связи

БЛОКИРОВАТЬ

НЕЛЬЗЯ

ПРОПУСТИТЬ

Технические особенности

Модульный подход

Ресурсоемкость

Интеграция

Эксплуатация

User-friendly

Поддержка производителя

```
void main(InputArrayOfArrays _in_src, InputArray _in_labels, bool processData) {
    if(_in_src.kind() != _InputArray::STD_VECTOR_MAT || _in_src.kind() != _InputArray::STD_VECTOR_SEQ) {
        string error_message = "The images are expected as InputArray::STD_VECTOR_MAT or InputArray::STD_VECTOR_SEQ";
        CV_Error(CV_StsBadArg, error_message);
    }
    if(_in_src.total() == 0) {
        string error_message = format("Empty training data was given. You'll need more than one sample to train a model.");
        CV_Error(CV_StsUnsupportedFormat, error_message);
    } else if(_in_labels.getMat().type() != CV_32SC1) {
        string error_message = format("Labels must be given as integer (CV_32SC1). Expected %d, but got %d.", CV_32SC1, _in_labels.getMat().type());
        CV_Error(CV_StsUnsupportedFormat, error_message);
    }
    // get the vector of matrices
    vector<Mat> src;
    _in_src.getMatVector(src);
    // get the label matrix
    Mat labels = _in_labels.getMat();
    // check if data is well-aligned
    if(labels.total() != src.size()) {
        string error_message = format("The number of samples (src) must equal the number of labels (labels). The dimensions of src: %d, %d, %d, %d.", src[0].rows, src[0].cols, labels.rows, labels.cols);
        CV_Error(CV_StsBadArg, error_message);
    }
}
```

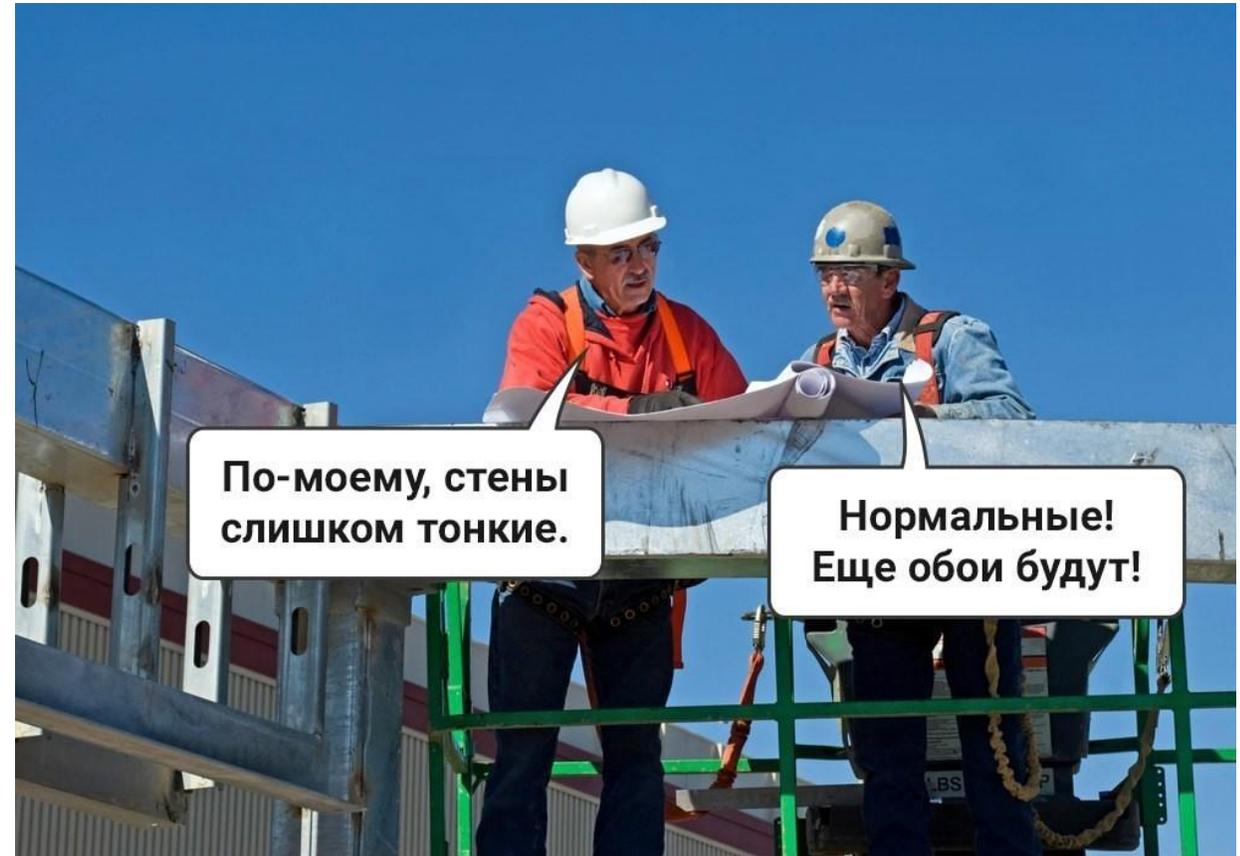
Применимость

Пилотирование или тестирование

Кастомизация под нужды организации

Соответствие требованиям

Юридические особенности



Стоимость

Понимание цели

+

Нужный функционал

+

Тестирование

+

Интеграция

+

Эксплуатация

- Стоимость ущерба



Почему Softline?

У нас лучшая команда

200+ инженеров и экспертов ИБ

100+ проектов по защите от утечек данных в 2018 году

Softline стратегический партнер ТОП-3 вендоров DLP в РФ

Опыт реализации SOC DLP



BONUS

DAG (Data Access Governance) -

комплексные решения по управлению доступом к неструктурированным данным и контролю за активностями с этими данными.

netwrix

VERITAS

VARONIS

IRM (Information Rights Management) –

класс систем, которые позволяют не терять контроль над документами после их публикации.

 **Microsoft**

ORACLE

Кому?

Тысячи сотрудников (от 100 и более)

Сложная структура документооборота

Большие объемы информации

Периметр компании размыт

Вопросы и ответы



GO GLOBAL



GO CLOUD



GO INNOVATIVE