

# Переход от «бумажной» безопасности и требований регуляторов по ИБ к практической

**Анастасия Ситская**

*Менеджер по развитию бизнеса  
Группа развития решений по ИБ*

# «Бумажная безопасность»



Федеральный закон от 26.07.2017 № 187-ФЗ  
«О безопасности критической информационной  
инфраструктуры Российской Федерации»

- Акты критических процессов
- Акты категорирования ОКИИ
- Методика обследования;
- Отчет об обследовании ОКИИ
- Частные модели угроз,
- ОРД регламентирующее организацию ИБ
- Частные ТЗ на разработку подсистем безопасности ЗОКИИ

**ПП РФ №1119**

**ПП РФ №687**

**ПП РФ №127**

**Приказ ФСБ России №378**

**Приказ ФСБ России №524**

**Приказ ФСТЭК России №21**

**Приказ ФСТЭК России №239**

**И т.д. и т.п.**

Федеральный закон от 27.07.2006 №152-ФЗ  
«О персональных данных»

- Порядка 46 различных Актов, форм, журналов, инструкции для легализации ПДн
- Аттестационные документы
- Частные модели угроз,
- ОРД регламентирующее организацию ИБ
- Частные ТЗ на разработку систем безопасности

# «Бумажная безопасность»

## Ответственность

КоАП РФ  
Статья 13.11



Ответственность возлагается на должностных лиц и юридических лиц

₽

₽

₽

₽

Дл: 10 000 – 20 000  
Юл: 60 000 – 100 000

Дл: 20 000 – 40 000  
Юл: 30 000 – 150 000

Дл: 6 000 – 12 000  
Юл: 30 000 – 60 000

Дл: 8 000 – 20 000  
Юл: 50 000 – 100 000

Обработка ПДн в случаях, непредусмотренных законодательством, или несовместимая с целями сбора ПДн

Обработка ПДн без письменного согласия субъекта обработки ПДн

Невыполнение оператором обязанности по опубликованию политики оператора в отношении обработки ПДн

Несоблюдение условий, обеспечивающих сохранность ПДн при хранении материальных носителей ПДн и исключающих несанкционированный к ним доступ

Проект Минцифры предполагает введение оборотных штрафов за утечку персональных данных до 3% от оборота компании (от 5 до 500 млн. рублей).

# «Бумажная безопасность»

## Ответственность

УК РФ

Ст. 274.1. Неправомерное воздействие на КИИ РФ

КоАП РФ

Ст. 19.5.



**до 10 лет  
лишения свободы**

Невыполнение требований по безопасности КИИ, в случае наступления инцидента с тяжкими последствиями или их угрозой



**до 6 лет  
лишения свободы**

Невыполнение требований по безопасности КИИ, нарушение правил эксплуатации



**до 5 лет лишением  
права занимать  
определенные  
должности**

ч. 3,4,5 ст. 274.1 УК  
РФ



**до 20 000  
административный  
штраф**

Невыполнение предписания регулятора об устранении нарушения законодательства

+ Проект ФЗ «О внесении изменений в КоАП РФ»



Ответственность возлагается на должностных лиц субъекта КИИ:

- Руководитель субъекта КИИ
- Уполномоченное лицо
- Лица, эксплуатирующие значимые объекты
- Лица, обеспечивающие функционирование значимых объектов
- Лица, обеспечивающие безопасность значимых объектов

# Б - безопасность

## Защита конечных точек

- Антивирусные программы
- Средства от несанкционированного доступа
- Средства доверенной загрузки
- Средства контроля за съемными носителями

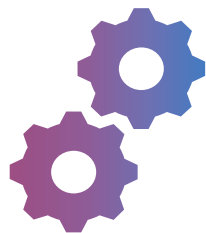


## Периметровая защита

- Межсетевой экран
- Криптошлюзы
- Сканер уязвимостей сети
- Система обнаружения вторжений

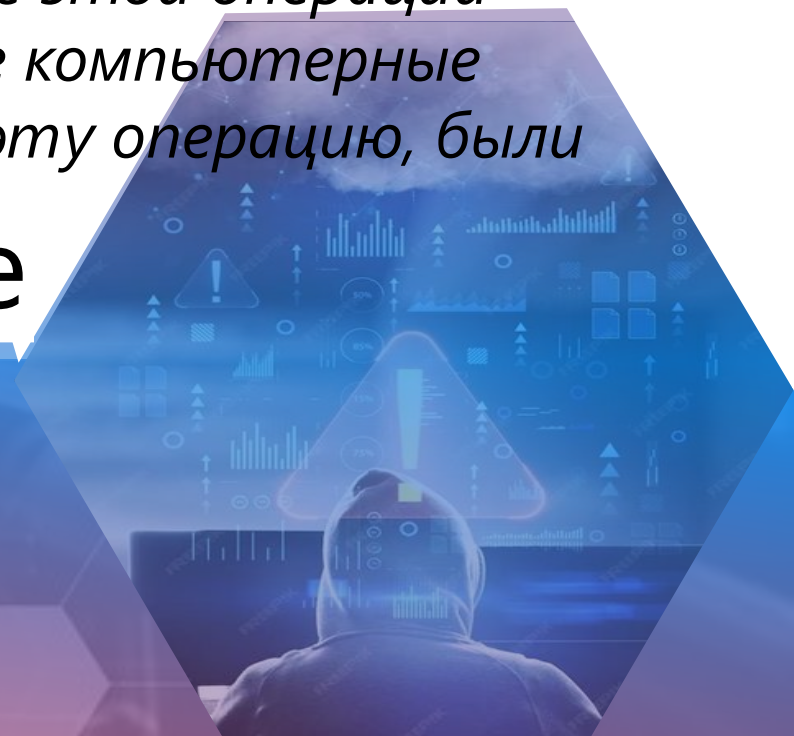


# Хакеры тоже задумались о здоровье



**Ученые из Дрездена**  
**Нейрохирурги**  
**Операция на**  
**ГОЛОВНОМ МОЗГЕ**

*«Главвраг больницы сделал очень сложную операцию на головном мозге тринадцатилетней девочке. В середине этой операции клинический центр подвергся кибератаке, и все компьютерные системы, все приборы, которые поддерживали эту операцию, были отключены», – рассказал Г-н Греб*



Трансформация.  
Успешная. Цифровая. Защищенная.

# DLP

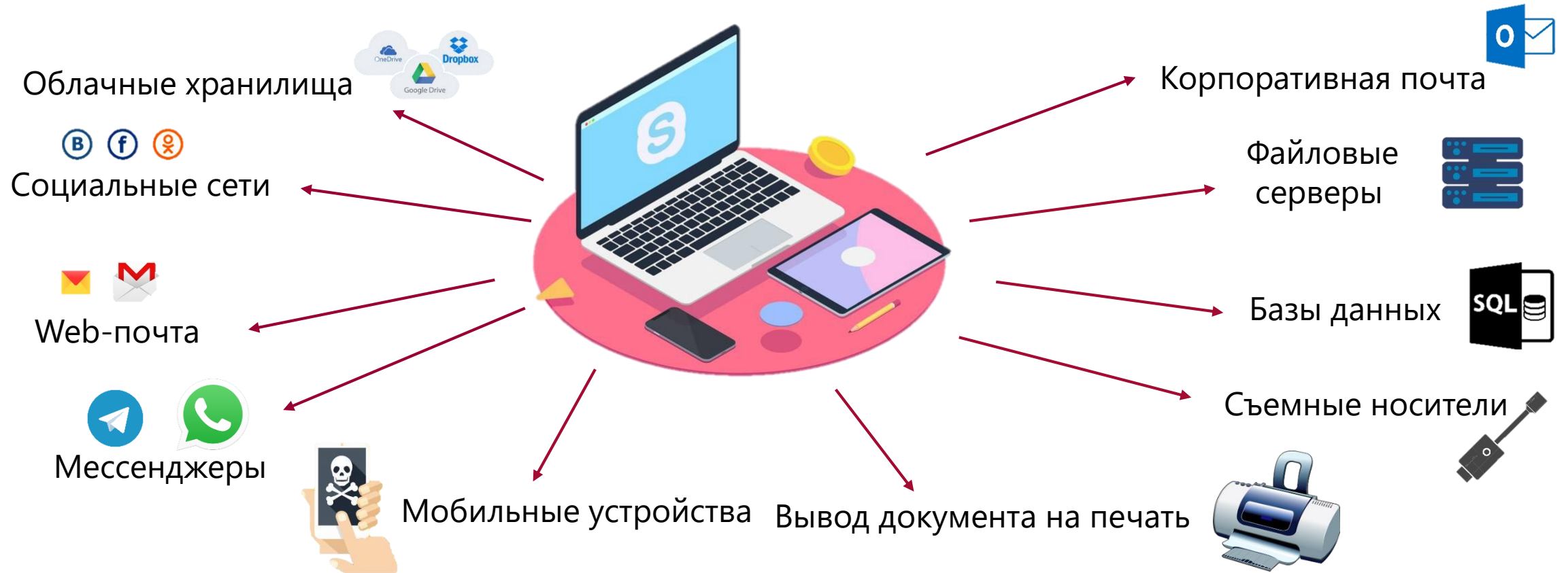
Мы всё сможем

softline® 30  
лет в ИТ

# ЧТО ТАКОЕ DLP СИСТЕМА?

**DLP-система** — специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. Эта аббревиатура на английском расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных).

# Каналы, которые контролирует DLP система



# ЧТО ПРЕДЛАГАЕМ МЫ?



## РАЗОВЫЕ УСЛУГИ

- Проанализируем потребности и поможем подобрать оптимальное решение
- Поставим софт на лучших условиях
- Внедрим систему, подключим источники данных
- Соберем перечень критичных документов в вашей организации
- Настроим индивидуальные правила так, как удобно вам
- Подготовим сопроводительную документацию или доработаем вашу



## СОПРОВОЖДЕНИЕ



### АНАЛИТИКА

- Оперативно проинформируем о потенциальных инцидентах
- Соберем всю информацию из архива по вашему запросу
- Актуализируем настройки при изменениях в компании
- Поможем выстроить процессы реагирования
- Обеспечим детальный контроль критичных элементов



### ТЕХПОДДЕРЖКА

- Выявим проблему, проведём диагностику, устраним проблему
- В сложных кейсах решим проблему совместно с вендором, соберем для него диагностическую информацию
- Оптимизируем процессы обработки и хранения данных
- Проведем обновление системы

# DRP - сервис(ETHIC)

DRP-сервис помогает бизнесам сохранить ресурсы и быстро адаптироваться в кризисных ситуациях. Этот сервис лицензирован и разработан компанией Softline, реализуется под названием «ETHIC». Мы можем предоставить возможность выбора только необходимого функционала ETHIC.

# Что такое «Этик» и как он работает?

**DRP (Digital Risk Protection)** - сервис позволяет детектировать *потенциально опасные действия и события* на ранних стадиях, благодаря чему можно своевременно реагировать на угрозы, не допуская наступления негативных последствий.



**ETHIC** - External Threats & Human Intelligence Center

- Миллионы площадок, в том числе закрытых (DarkNet)
- Мониторинг и анализ контента всех популярных цифровых угроз
- Поддержка опытных аналитиков

## 01

### Выявляет

Круглосуточно отслеживается несколько миллионов информационных ресурсов и фиксируются события, связанные с компанией.

## 02

### Классифицирует

Выявленные события классифицируются по типам и степени угрозы и верифицируются командой аналитиков.

## 03

### Оповещает

События, прошедшие верификацию, попадают в личный кабинет сервиса, а ответственный сотрудник оповещается о событиях.

# Какие задачи решает ETNISC?



Снижение рисков информационной, экономической безопасности и репутационных потерь



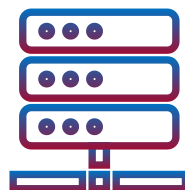
Выявление фактов неправомерного использования товарного знака



Защита от фишинга и социальной инженерии



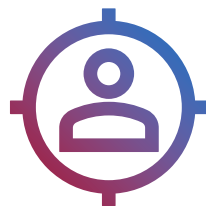
Выявление утечек информации и случаев компрометации учетных записей



Выявление утечек БД и их фрагментов



Обнаружение информационных атак



Проверка физических лиц и их контактных данных



Анализ трендов черного рынка

# Как попробовать?

## 1 Выберите необходимый функционал

Определите, какие модули и функции ETNICS вам нужны для оценки рисков ИБ

## 2 Получите пробную версию

Оставьте заявку на получение пробной версии сервиса и оцените его возможности

## 3 Обратитесь к нашим специалистам

Проконсультируйтесь с нашими экспертами по применению ETNICS в вашей организации



Трансформация.  
Успешная. Цифровая. Защищенная.

# Security Awareness

Облачный сервис по развитию навыков  
кибербезопасности

# Security Awareness

Облачный сервис по развитию навыков кибербезопасности

## Интерактивное обучение

Предлагаем разнообразные интерактивные курсы и тренинги для повышения кибербезопасности вашей команды

## Симуляция атак

Наши тренировки имитируют реальные кибератаки для развития навыков в обнаружении и предотвращении угроз

## Оценка результатов

Предоставляем детальный анализ прогресса участников и поддерживаем улучшение их навыков в кибербезопасности

# Как попробовать?

Организуем доступ и назначим интересующие курсы:

- длительность доступа до 2 недель
- до 2 сотрудников
- до 4 учебных курсов



Организуем учебную фишинговую рассылку:

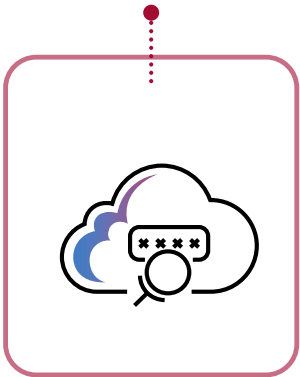
Предоставим вам аргументы  
для выделения ресурсов на обучение

# Тестирование на проникновение

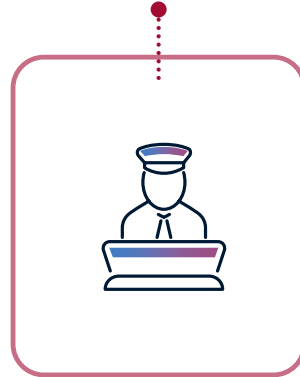
Softline предлагает услуги тестирования на проникновение для проверки безопасности вашей сети и приложений. Мы используем различные методы, включая взлом сети, симуляцию атак и анализ уязвимостей, чтобы помочь вам выявить и устранить слабые места в вашей защите.

# Виды пентеста, которые мы осуществляем

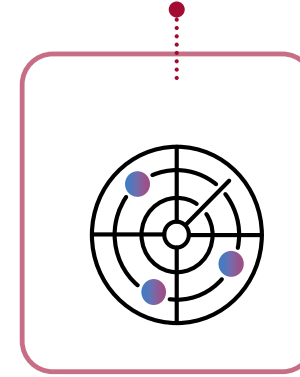
Пентест  
**web-приложений**



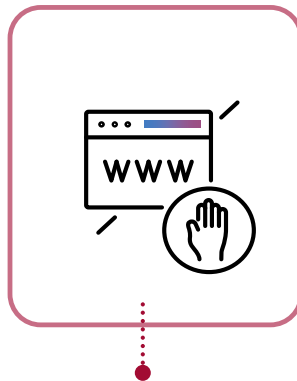
Пентест  
**внутреннего периметра**



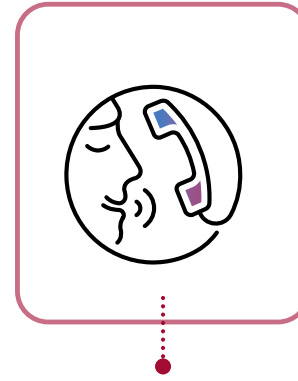
Пентест  
**Wi-Fi сетей**



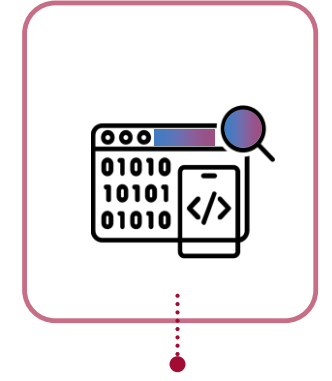
Пентест  
**внешнего периметра**



**Социотехнический**  
пентест



Пентест  
**мобильных приложений**



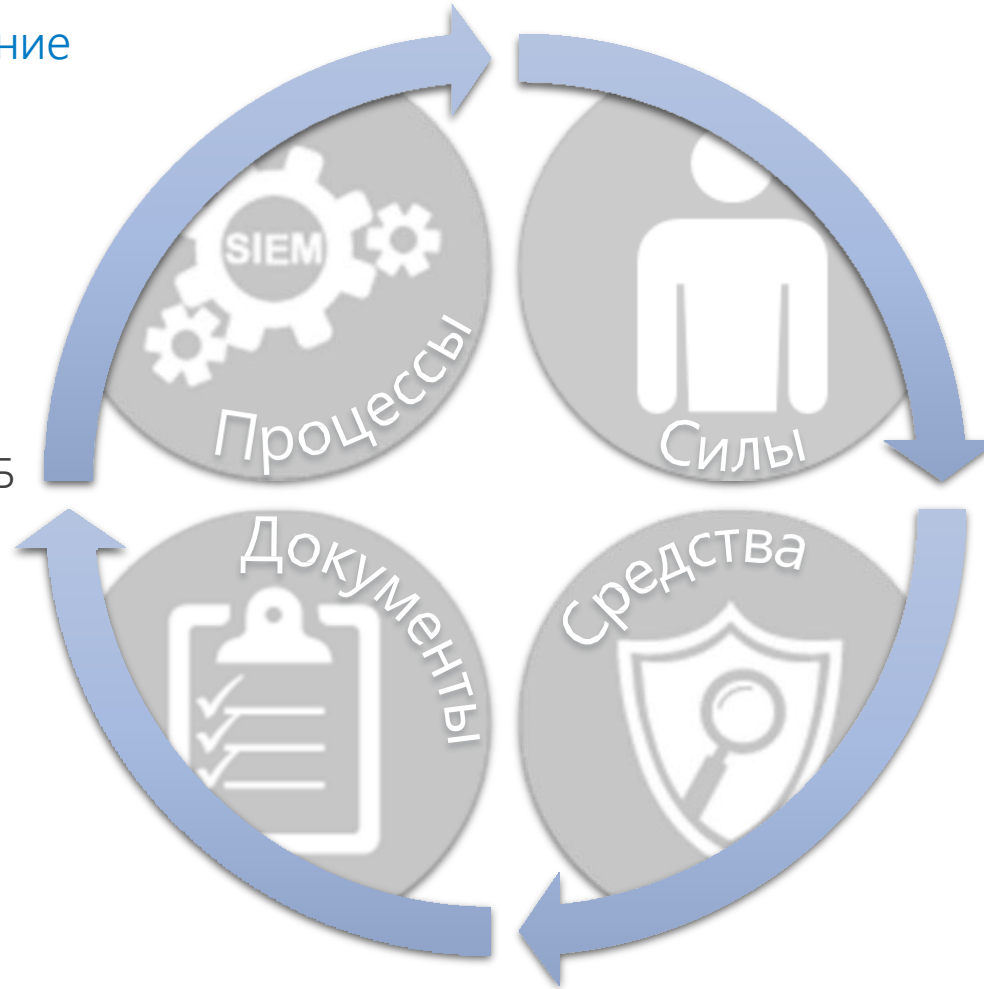
# Комплексный подход к безопасности

## Управление и планирование

- ✓ Построение СУИБ
- ✓ Ежегодный план
- ✓ Регулярный аудит

## Экспертиза

- ✓ Технический проект СОИБ
- ✓ Программа и методика
- ✓ Пакет ОРД по обеспечению ИБ
- ✓ pentest



## Учебный центр Softline

- ✓ Программа повышения квалификации

## Опыт реализации

- ✓ Реализация СОИБ
- ✓ Поддержка решений
- ✓ Поддержка производителей

**softline<sup>®</sup> 30**  
Мы всё сможем лет в ИТ

**Трансформация.**  
Успешная. Цифровая. Защищённая.