Опыт повышения осведомленности не ИТ-персонала, по вопросам информационной безопасности

Источники утечек, Обучение. Контроль

Основные источники утечки информации

Ценные данные :

- Соц, сети
- Мессенджеры
- Файлообмен
- Почта
- Бумаги

- Данные о сотрудниках
- Учетные данные
- Коммерческая информация
- Фотографии
- Скриншоты

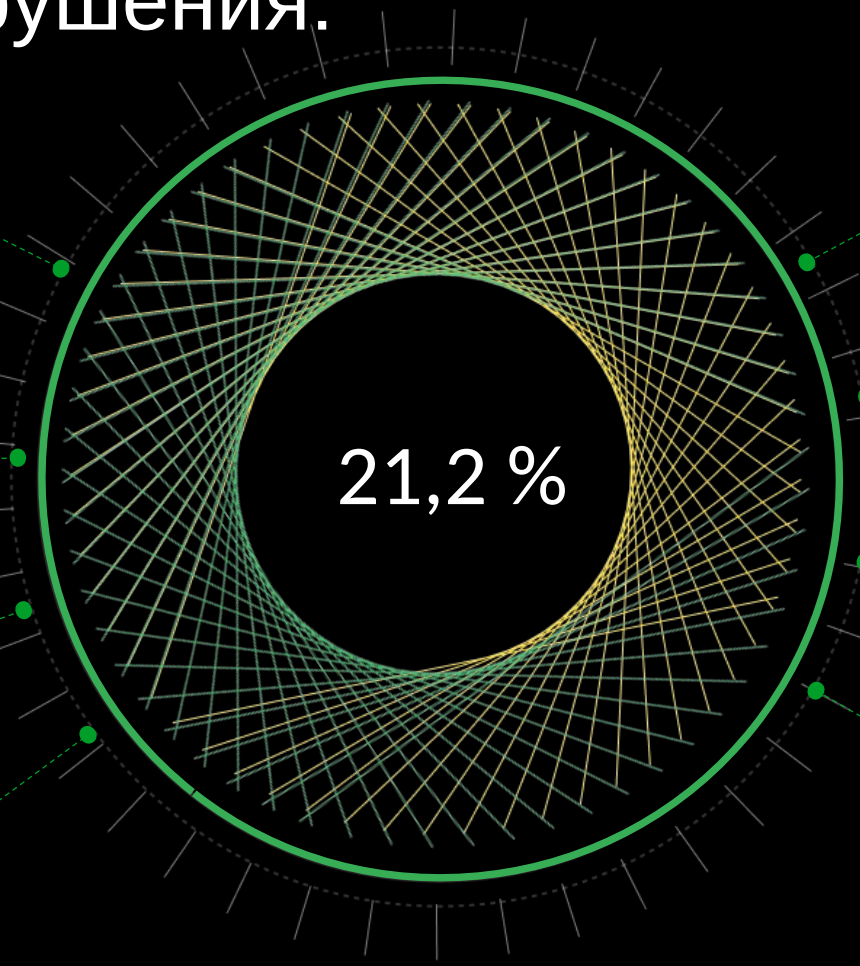
Умышленные нарушения:

Умышленные нарушения
Составляют 98 %

Случайные нарушения
снизились с 21 % до 1,6%

Умышленные нарушения
персонала,
рост 25% до 75%

Защита репутации
Утечки признают 42%



Рост
8,8 % до 21,2%

Рост
7% до 21,2 %

Кибератаки 2021
87,5%

Кибератаки 2023
57,6%

Учить

Лечить

Продают действующие сотрудники

Звонки сотрудникам от мошенников

Уволенный обиженный сотрудник

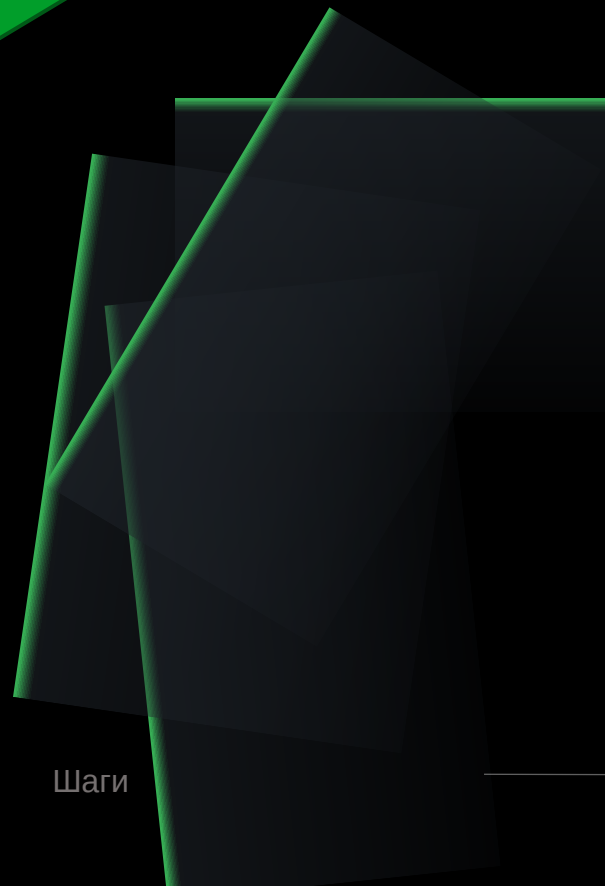
ИТ действующий/ уволенный

Повышение осведомленности:

Цифровая гигиена

Распознавание злоумышленника

Снижение риска утечки данных

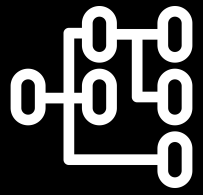


Минимальный набор уроков:

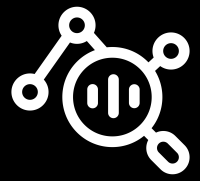
Без существенных финансовых вложений

Социальная инженерия

Пароли, авторизация



Фишинг, электронная почта



Средства криптографи-ческой защиты

DEERAY
MACHINES CAN UNDERSTAND

Шаг 1:

Организовать обучение

Если позволяет бюджет – создать интерактивный курс

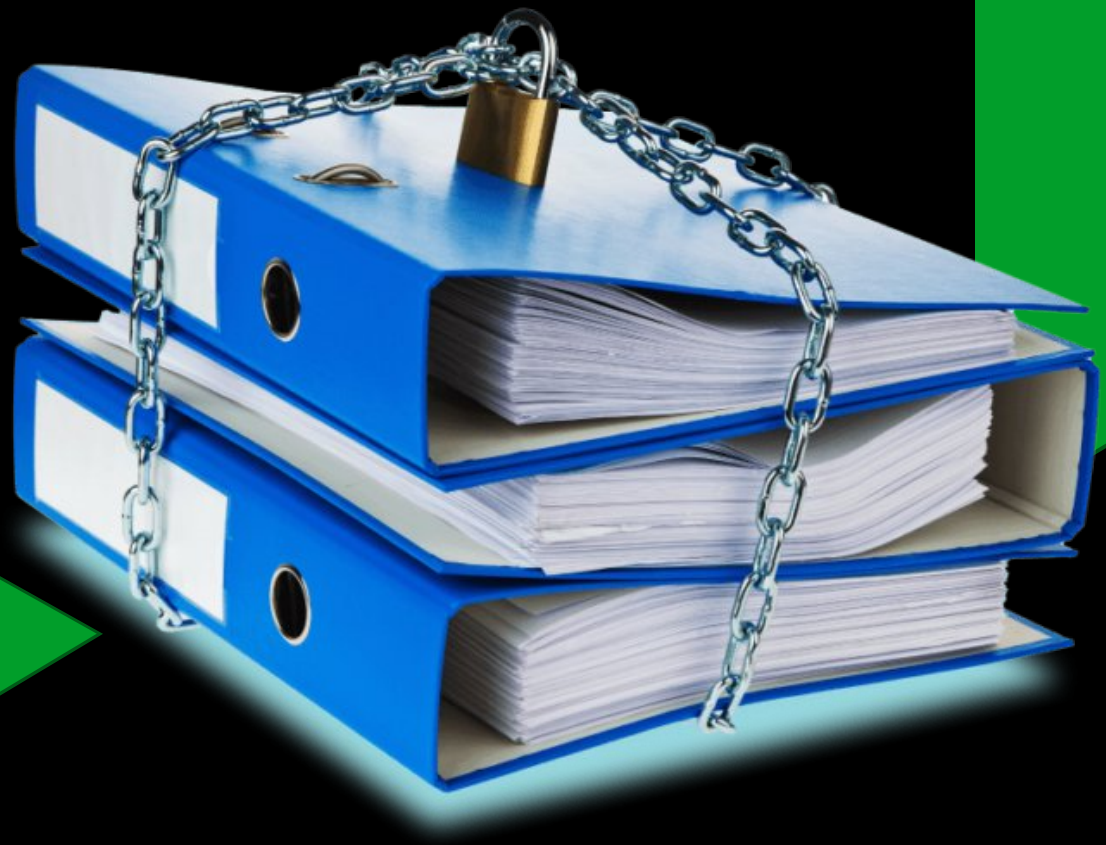
DEERAY
MACHINES CAN UNDERSTAND

Шаг 2: Рассылки новостей

DEERAY
MACHINES CAN UNDERSTAND

Шаг 3:

Регулярная актуализация документов.



Шаг 4:

Разносторонний контроль.

Применение программных средств контролирующих обмен информацией.

- Анализ сообщений электронной почты
- Анализ общения в социальных сетях
- Анализ передачи данных
- Контроль записи на переносные устройства

Меры ИБ

Наиболее эффективные.

Внедрение систем защиты от вторжений
33%

Внедрение DLP систем
25%

Upgrade
33%

Проведение обучающих мероприятий
58%

Благодарю за внимание:

" Надежно защищен только выключенный компьютер.

© Евгений Касперский

Безопасность это процесс, а не результат.

© Брюс Шнейер

ПЁТР ФЕДОСЕЕВ

+7 (902) 9292 333
@PeterFedoseev