DLP:
ПЕРСОНИФИЦИРОВАННАЯ ЗАЩИТА ОТ УТЕЧЕК

СТАТИСТИКА

213 СЛУЧАЕВ УТЕЧКИ ИНФОРМАЦИИ

из российских компаний и государственных органов было опубликовано в СМИ в 2016 году (14% от числа утечек по всему миру)

ТИП ИНФОРМАЦИИ

НАРУШИТЕЛИ

ПОХИЩЕННЫЕ ДАННЫЕ

ОСНОВНЫЕ УГРОЗЫ

Согласно данным статистики, большинство инцидентов информационной безопасности является результатом действий сотрудников компании.

ГРУППЫ ПОВЫШЕННОГО РИСКА

- Испытательный срок
- Увольнение
- Подозрение на алкогольную, наркотическую зависимость
- Подозрение на радикальные политические взгляды
- Подозрение на нарушения
- Участие в конфликтах
- Наличие расширенных прав в информационных системах
- Возможность распоряжаться средствами клиентов

ЦЕЛИ И ЗАДАЧИ

Снижение количества и тяжести последствий от утечки данных

Оценка продуктивности и лояльности сотрудников

Контроль всех потоков информации, пересекающих периметр

Выявление фактов хранения и передачи конфиденциальной информации вне бизнес-процессов

Проверка соблюдения регламентов и процедур

Разоблачение мошеннических схем

Расследование инцидентов

ЭТАПЫ

АНАЛИТИКА И КОНСАЛТИНГ

ВНЕДРЕНИЕ

СОПРОВОЖДЕНИЕ

АНАЛИТИКА И КОНСАЛТИНГ

СОСТАВ РАБОТ

Анализ нормативных документов клиента на соответствие законодательству о коммерческой тайне

Выбор контролируемых каналов передачи данных

Подготовка архитектуры решения и ТЗ для пилотного внедрения

РЕЗУЛЬТАТ

Рекомендации по разработке недостающих внутренних документов

Отчет с разработанной архитектурой решения

ТЗ для пилотного внедрения

ВНЕДРЕНИЕ

СОСТАВ РАБОТ

Подбор оптимального решения DLP, включая настройку политик и фильтров

Разработка недостающих внутренних документов, включая политики реагирования на инциденты и порядок проведения расследований

Пилотное и промышленное внедрение ПО

Обучение сотрудников клиента

РЕЗУЛЬТАТ

Полный комплект необходимых внутренних документов

Отчетность по результатам пилотного и промышленного внедрения

Система выявления и расследования инцидентов с настроенными политиками и фильтрами

Статистика обучения сотрудников

НАСТРОЙКА ПОЛИТИК И ФИЛЬТРОВ

Выявление проблемных зон (группы сотрудников, каналы передачи данных)

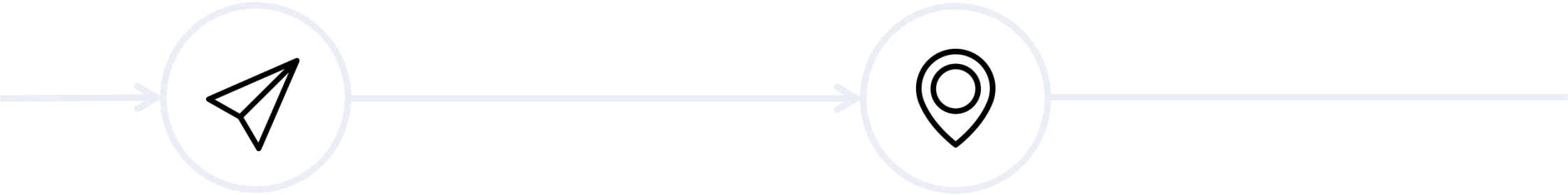
Выработка предложений по соблюдению баланса между информированием и предотвращением утечки данных

Согласование критериев критичности события

Доработка базовых политик с учетом специфики компании

Обогащение критериев контроля на базе имеющегося опыта

СОПРОВОЖДЕНИЕ



СОСТАВ РАБОТ

Анализ данных и выявление угроз в режиме реального времени

Мониторинг каналов передачи данных

Анализ активности сотрудников

Расследования по запросу клиента

Предоставление отчетности

РЕЗУЛЬТАТ

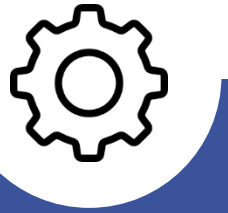
Персонифицированная система защиты данных

Статистика инцидентов ИБ по каналам передачи данных

Отчетность по результатам анализа активности сотрудников

Отчетность о работе сервиса

МОНИТОРИНГ КАНАЛОВ



Контроль обработки, передачи и хранения конфиденциальной информации

Вариативное автоматическое реагирование на факты копирования конфиденциальной информации

Анализ информации, передаваемой по разным каналам, с акцентом на группы повышенного риска

Выявление фактов неправомерного обращения с конфиденциальными данными

Подготовка справочной информации по нарушенным требованиям ИБ

ПРОФАЙЛИНГ

Анализ эффективности работы сотрудников и определение их лояльности к компании

Анализ данных о сотрудниках или событиях из внутренних и внешних источников (в том числе ретроспективный анализ)

Анализ коммуникаций сотрудника (корпоративный email, мессенджеры)

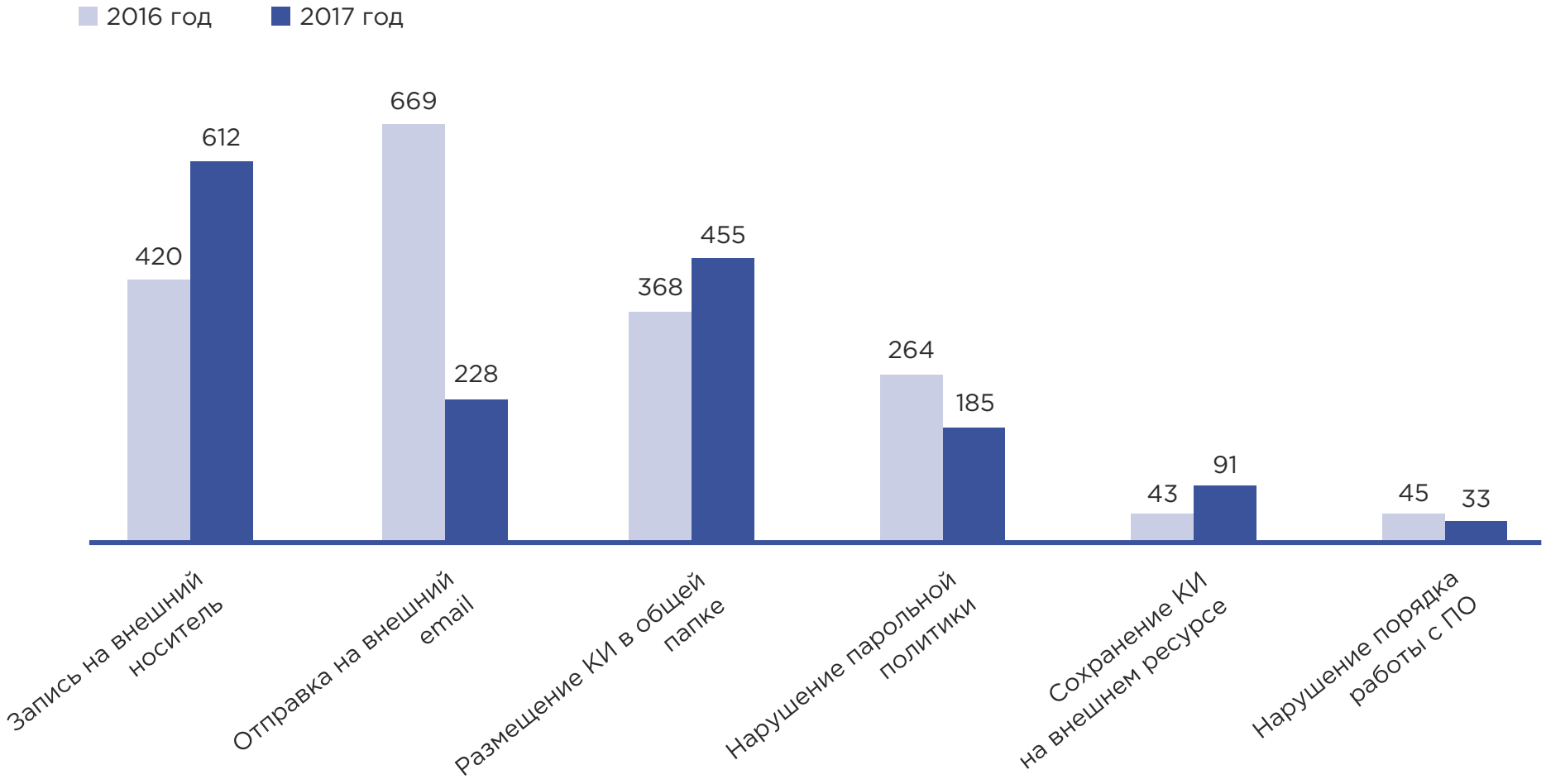
Создание индивидуального профиля сотрудника

Построение графа связей по сотрудникам/клиентам

ОТЧЕТ ПО ИНЦИДЕНТАМ

КОМПАНИЯ: Компания А

ВСЕГО ИНЦИДЕНТОВ В 2016 ГОДУ: 1809 **ВСЕГО ИНЦИДЕНТОВ В 2017 ГОДУ:** 1604



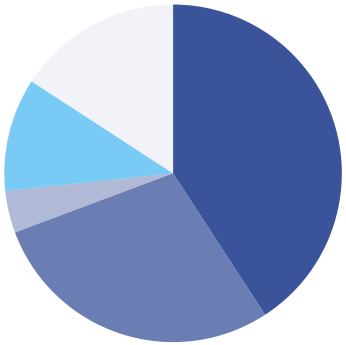
ОТЧЕТ ПО ЭФФЕКТИВНОСТИ

ПОЛЬЗОВАТЕЛЬ: Иванов Иван Иванович

ПЕРИОД: 09.01.18 – 31.01.18 (17 раб. дней)

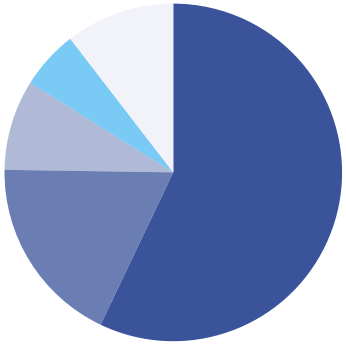
Начало раб. дня	Окончание раб. дня	Длительность раб. дня	Активность пользователя
10:07	**19:04**	**7ч 57м**	**6ч 34м**
Опоздания	Ранние уходы	Ранние приходы	Поздние уходы
5	**3**	**1**	**2**

ЭФФЕКТИВНОСТЬ: 88%



СУММАРНАЯ АКТИВНОСТЬ (ПРОЦЕССЫ):

- Офисные (45ч 34м)
- Почта (33ч 2м)
- Системные (3ч 15м)
- Браузеры (12ч 7м)
- Другие (17ч 40м)



СУММАРНАЯ АКТИВНОСТЬ (САЙТЫ):

- Локальные (6ч 55м)
- Мессенджеры (2ч 12м)
- Поисковые (1ч 3м)
- Новости и СМИ (41м)
- Другие (1ч 16м)

РАССЛЕДОВАНИЯ

Обработка запросов, полученных в свободной форме от различных структур клиента

Предоставление подробного отчета и сопутствующих материалов (копии документов, логи действий и т.п.) по итогам расследования

Анализ внутренних и внешних связей сотрудников для предупреждения рисков

Оценка микроклимата (выявление конфликтов, способных привести к негативным последствиям)

Использование дополнительных критериев и открытых источников информации

РАБОТА С БИЗНЕС-СИСТЕМАМИ

При проведении расследований мы анализируем данные в бизнес-системах, наиболее распространенных в финансовой сфере. В их числе:

SUGARCRM

Microsoft Dynamics

3CARD
ПРОГРАММНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

mfms

metodix

DIASOFT
всё по-настоящему

WAY4™
Payment Processing Solutions

ЦФТ ЦЕНТР ФИНАНСОВЫХ ТЕХНОЛОГИЙ

РЕЗУЛЬТАТЫ

ОПЕРАТИВНОСТЬ

Быстрый поиск значимой информации
во внешних и внутренних источниках

Своевременное выявление инцидентов
информационной безопасности

СИСТЕМНОСТЬ

Мультиканальный контроль
за деятельностью сотрудников

Решение сложных задач и разбор
«нестандартных» инцидентов

РОЛИ В ПРОЕКТЕ

INFOSECURITY

Руководитель проекта

Архитектор сервиса

Инженер

Аналитик

Консультант

КЛИЕНТ

Руководитель проекта

Представитель ИБ

Представитель СБ

Представитель IT

Представитель HR

НАШИ ПРЕИМУЩЕСТВА

Построение персонифицированной системы предотвращения утечек

Привлечение экспертов-аналитиков на всех этапах внедрения сервиса

Обучение сотрудников клиента работе с системой

Внедрение и сопровождение DLP в крупных компаниях

ВЕНДОРНЫЕ РЕШЕНИЯ

gk-is.ru