



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

01 ноября 2018 г.
г. Тюмень

#CODEIB

«ШПИОН, ВЫЙДИ ВОН!» ИЛИ ПРОФИЛАКТИКА ВНУТРЕННЕГО ФРОДА В МФЦ



НАЧАЛЬНИК СЛУЖБЫ ИБ

ЮЛИЯ КИБАРДИНА,
ГАУ ТО «МФЦ»

EMAIL: KibardinaJA@mfcto.ru



Масштаб



Предпосылки

1021 человек в штате

1.5 млн обращений в год

Рост количества услуг

Распределенная структура



Проблематика



Автоматизация
процесса
мониторинга



Подозрение на инцидент

1. ПЕРИОДИЧЕСКИЙ МОНИТОРИНГ СОБЫТИЙ

Событий по запросу: 3 Выполнил: 16.10.2018 11:42

Отправители: Кибардина Юлия Александровна

Тема: Тест

Сообщение [image001.png \(14.49 KB\)](#) ↓

ФИО: Тестов Тест Тестович

СНИЛС: 112-233-445 95

Паспорт: 1234 567890

мои документы

Подозрение на инцидент

1. ПЕРИОДИЧЕСКИЙ МОНИТОРИНГ СОБЫТИЙ

The screenshot displays a web-based interface for monitoring security events. A prominent window titled "Детальная информация о событии" (Detailed information about the event) is shown, detailing a specific incident. The event's metadata includes a size of 25.38 KB, ID 14997437, and a capture time of 16.10.2018 11:40. The content area shows two identical entries for a document, each containing personal data: "ФИО: Тестов Тест Тестович СНИЛС: 112-233-445 95 Паспорт: 1234 567890 С" and "информационной безопасности ГАУ ТО <МФЦ> Тел. (3452) 399-289 доб. 1085". The interface also features a sidebar with filters for "Объекты" (Objects) and "Содержимое" (Content), and a navigation bar at the bottom with "Компания" and "Веб-почта" options. Orange arrows highlight the flow of information from the event list to the detailed view.

Детальная информация о событии

Объекты

- [Red circle icon]
- Паспорт РФ и ФИО
- СНИЛС
- СНИЛС и ФИО

Содержимое

- Почта на Клиенте

25.38 KB ID:14997437 Дата перехвата: 16.10.2018 11:40 Дата отправки: 16.10.2018 11:40

ФИО: Тестов Тест Тестович СНИЛС: 112-233-445 95 Паспорт: 1234 567890 С
информационной безопасности ГАУ ТО <МФЦ> Тел. (3452) 399-289 доб. 1085

Показать

ФИО: Тестов Тест Тестович СНИЛС: 112-233-445 95 Паспорт: 1234 567890 С
информационной безопасности ГАУ ТО МФЦ Тел. (3452) 399-289 доб. 1085

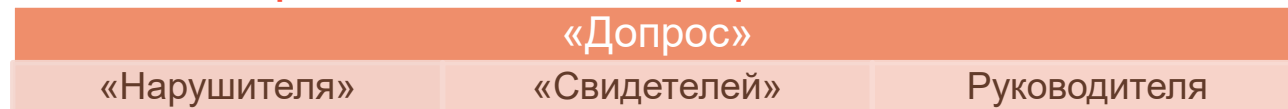
image001.png

Показать

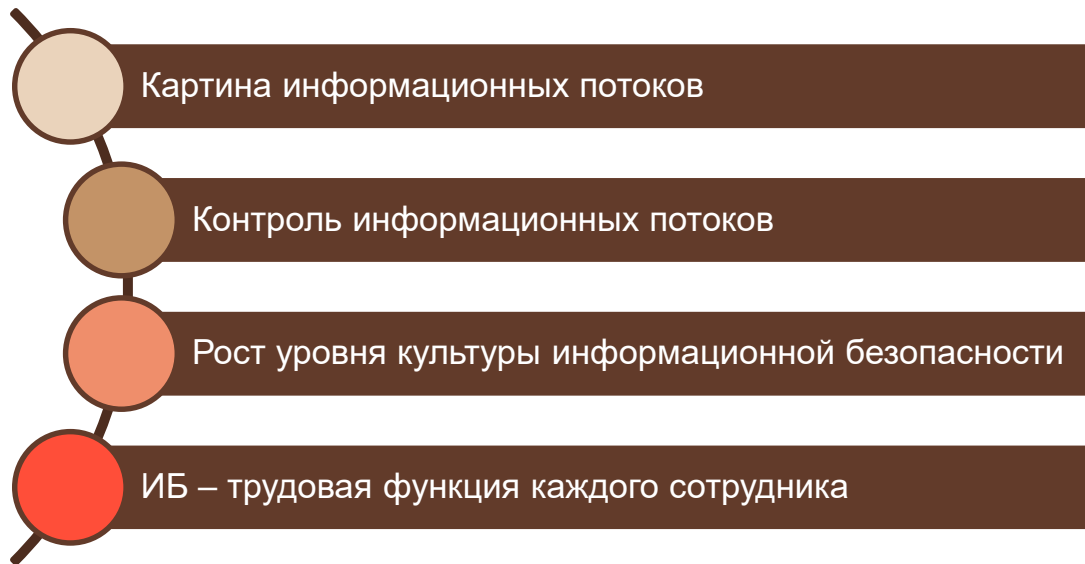
Компания → Веб-почта

Подозрение на инцидент

2. ОРГАНИЗАЦИОННАЯ СОСТАВЛЯЮЩАЯ

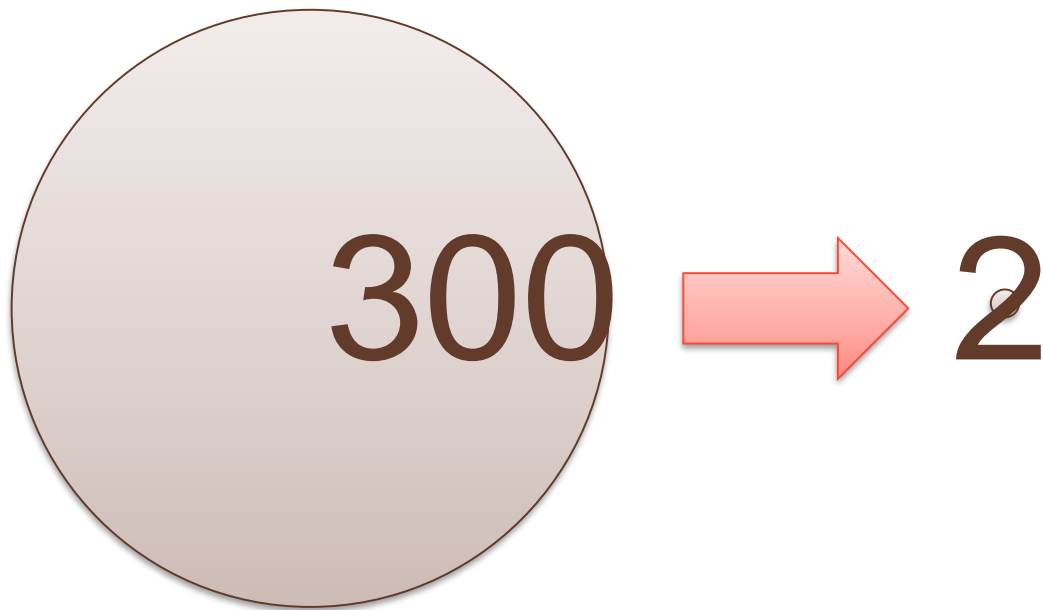


Результат



Результат

СОКРАЩЕНИЕ СОБЫТИЙ С ПОДОЗРЕНИЕМ НА ИНЦИДЕНТ





КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

01 ноября 2018 г.
г. Тюмень



НАЧАЛЬНИК СЛУЖБЫ ИБ

ЮЛИЯ КИБАРДИНА,
ГАУ ТО «МФЦ»

EMAIL: KibardinaJA@mfcto.ru



#CODEIB