



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

3 СЕНТЯБРЯ 2020 ГОДА
Краснодар

Найти и защитить: наводим порядок в файловой системе



Александр Янчук

Руководитель представительства
«СёрчИнформ» в Северо-Западном ФО

SEARCHINF@RM
INFORMATION SECURITY

#CODEIB

Решать ИБ-задачи
нужно в комплексе.



SEARCHINFORM
INFORMATION SECURITY

#CODEIB

Комплексный подход к
информационной безопасности.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB



Защита от инсайдерских угроз – DLP.

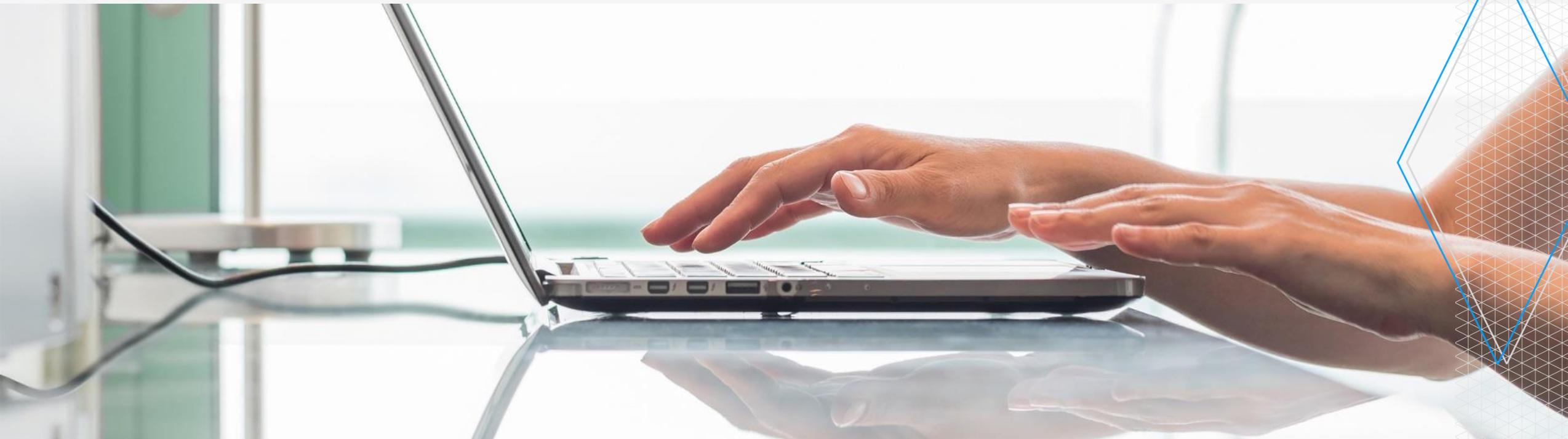
SEARCHINFORM
INFORMATION SECURITY

#CODEIB



ВАЖНЫЕ ВОПРОСЫ

- Сколько в компании файлов с конфиденциальной информацией?
- Где они хранятся?
- Кто имеет к ним доступ?





ПОЧЕМУ НУЖНО НАВЕСТИ ПОРЯДОК?

- коммерческая тайна;
- гостайна;
- ноу-хау;
- планы развития.

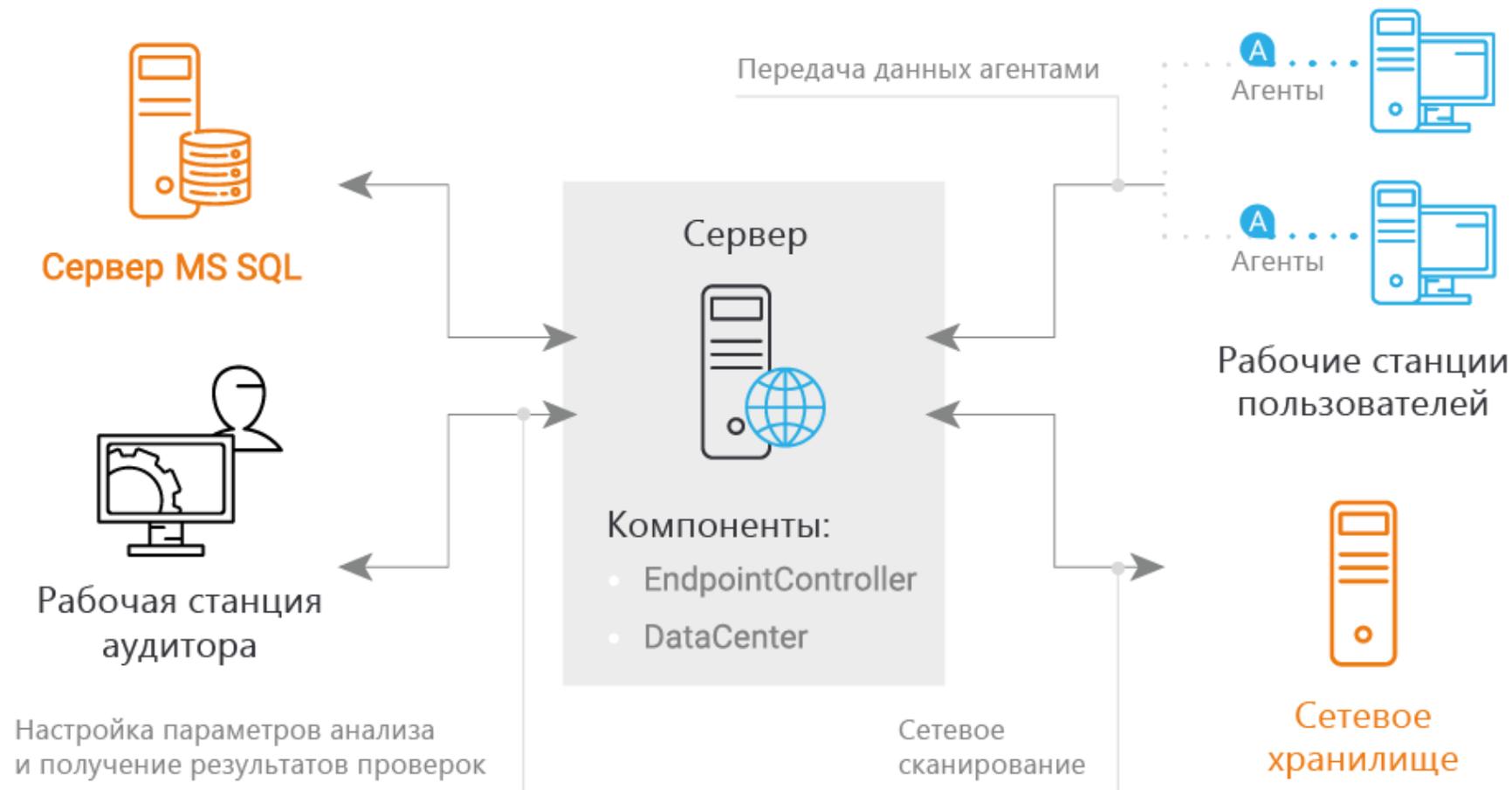


Data-Centric Audit and Protection – НОВЫЙ класс продуктов:

СёрчИнформ FileAuditor



СХЕМА РАБОТЫ



КАКИЕ ЗАДАЧИ РЕШАЕТ FILEAUDITOR

- Классификация документов с конфиденциальной информацией (ПДн, коммерческая тайна и др.).



МАРКИРОВКА ДОКУМЕНТОВ

Файловый аудитор - Консоль аналитика (1.17.128.4)::Администратор@kos.local

Поиск Текущая активность Отчеты **Файловый аудитор** Профайл центр

Файл	Кол-во	Критерии	Дата созда...	Разм...	Дата модифик...
work10-3.kos.local	1				
с	2				
users	1				
adminis	3				
desktop	5				
новая папка	3				
test13.doc		Секретный договор	12.03.2019 11: 143 KB		12.03.2019 11:06:5
договор о слиянии.docx		Новые документы Секретный договор	19.03.2019 18: 12,7 KB		19.03.2019 18:22:1
bolivia.doc		Секретный договор	11.02.2019 17: 142,5 К		23.01.2019 17:58:0
документ проверки.docx		Новые документы	19.03.2019 18: 11,06 К		19.03.2019 18:32:5
docs	3				
служебная инструкция менеджера.docx		Новые документы Служебные инструкции	19.03.2019 18: 11,08 К		19.03.2019 18:34:2
протокол 13.xlsx		Новые документы	19.03.2019 18: 7,71 KB		19.03.2019 18:33:4
documents	1				
appdata	1				
reget deluxe	1				
eula-ru.rtf		Секретный договор	01.10.2018 12: 71,84 К		07.07.2008 11:01:4

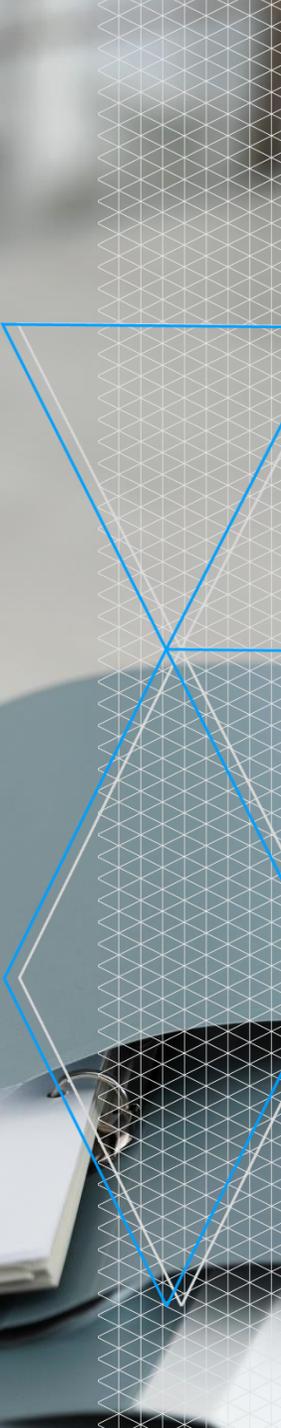
КЕЙС

[персональные данные
в общей папке]



SEARCHINFORM
INFORMATION SECURITY

#CODEIB



КАКИЕ ЗАДАЧИ РЕШАЕТ FILEAUDITOR

- **Аудит прав доступа** к ресурсам и файлам, отслеживание учетных записей с привилегированными правами.



КЕЙС

[дорогое
маркетинговое
исследование в
общем доступе]



SEARCHINFORM
INFORMATION SECURITY

#CODEIB

КАКИЕ ЗАДАЧИ РЕШАЕТ FILEAUDITOR

- **Архивирование документов** – теневое копирование критичных файлов и сохранение истории операций с ними.



+ 134:23:454:12

+

КЕЙС

[восстановление
данных, удаленных из
мест]

Business Strategy

Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management

134:23:454:12

+

Business Strategy

Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

ОТСЛЕЖИВАНИЕ ВЕРСИЙ ДОКУМЕНТА

The screenshot displays the 'Файловый аудитор' (File Auditor) interface. The main window shows a file tree for 'ivanov.company.com' with a folder 'doc' containing 22 files. A table below lists these files with columns for 'Файл', 'Кол-во', 'Размер', 'Дата создания', 'Дата обновления', 'Правила', and 'Права доступа'. The file 'антикризисный план.docx' is highlighted, and its version history is shown in a 'Версии файлов' (File Versions) table.

Файл	Кол-во	Размер	Дата создания	Дата обновления	Правила	Права доступа
ivanov.company.com	1					
с	1					
doc	22					
антикризисный план.docx		14,93 KB	08.02.2017 18:45:18	11.12.2017 11:11:08		F M R W X L
антикризисный план - present.pptx		14,93 KB	15.12.2017 9:36:56	11.12.2017 11:11:41		F M R W X L
rinok_podshipnikov_2010.doc		1,68 MB	07.09.2010 18:54:53	25.03.2011 12:37:06		F M R W X L
rinok_podshipnikov_2010 - edit.doc		1,68 MB	15.12.2017 9:36:56	25.03.2011 12:37:06		F M R W X L
plan_po_marketingy.doc		739,5 KB	07.09.2010 18:54:53	02.04.2011 14:08:39		F M R W X L
plan_po_marketingy - 2017.doc		597,5 KB	15.12.2017 9:36:56	14.12.2017 17:30:43		F M R W X L
knizhny_rinok_2010.doc		1,01 MB	07.09.2010 18:54:53	25.03.2011 12:36:45		F M R W X L
knizhny_rinok_2010 - edit.doc		1,01 MB	15.12.2017 9:36:56	25.03.2011 12:36:45		F M R W X L
example.xlsx		10,1 KB	05.07.2017 19:08:13	11.12.2017 11:09:59		F M R W X L
example - 1010.xlsx		10,1 KB	15.12.2017 9:36:56	11.12.2017 11:09:39		F M R W X L
стратегия развития - презентация.pptx		265,28 KB	15.12.2017 9:36:56	12.08.2010 17:33:50		F M R W X L

Версии файлов	Доступен	Дата обновления	Размер файла	Атрибуты	Правила
11.12.2017 11:11:08		11.12.2017 11:11:08	597,5 KB	Архивный	
02.11.2017 09:12:54		02.11.2017 09:12:54	793,5 KB	Архивный	
30.10.2017 15:27:26		30.10.2017 15:27:26	625,2 KB	Архивный	
21.10.2017 17:36:47		21.10.2017 17:36:47	712,1 KB	Архивный	
15.10.2017 13:54:01		15.10.2017 13:54:01	654,0 KB	Архивный	
10.10.2017 11:34:14		10.10.2017 11:34:14	521,3 KB	Архивный	

Содержание документа

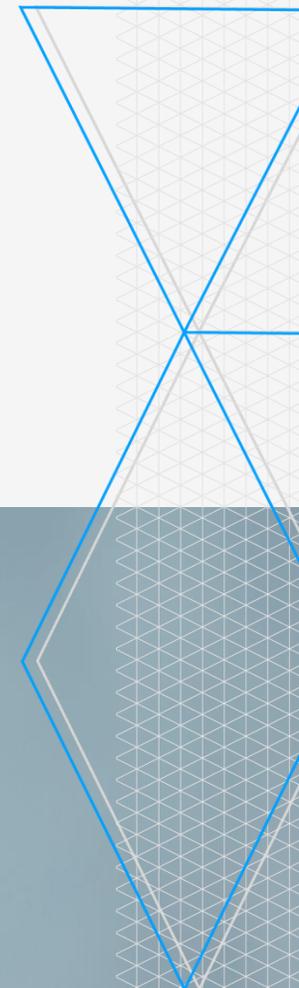
ООО "БЕЛЫЕ НОЧИ"

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "БЕЛЫЕ НОЧИ". МОСКВА, УЛ. ОРДЖОНИКИДЗЕ Д.11, ИНД: 115419. ТЕЛ (495) 956-21-01 (МНОГОКАНАЛЬНЫЙ). ФАКС: (495) 956-45-17 ИНН/КПП 7715805253/771501001

последний файл - в первой строке

КАКИЕ ЗАДАЧИ РЕШАЕТ FILEAUDITOR

- **Контроль за действиями пользователей**
– создание, редактирование,
перемещение и удаление критичных
файлов.



КЕЙС

[данные компании в
Интернете]



http://

Search

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

КЕЙС

[белые прайсы на ПК менеджеров]

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

ПРЕИМУЩЕСТВА:



- проверка только новых и измененных документов;
- гибкая настройка правил;
- сохранение последних версий файла и поиск по удаленным вариантам;
- использование агентов или сетевое сканирование;
- работа на Windows, Linux и других ОС.

Комплексный подход к
информационной безопасности.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB



#CODEIB

МЫ КАЖДЫЙ ДЕНЬ
РАССКАЗЫВАЕМ ОБ ИБ:



[https://t.me/
searchinform](https://t.me/searchinform)



[https://www.facebook.com/
SearchInform](https://www.facebook.com/SearchInform)



[https://vk.com/
securityinform](https://vk.com/securityinform)

SEARCHINFORM
INFORMATION SECURITY



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

3 СЕНТЯБРЯ 2020 ГОДА
Краснодар

Спасибо за внимание! Вопросы?

SEARCHINFORM
INFORMATION SECURITY

#CODEIB