КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11 марта 2021 года, Красноярск

#CODEIB

Нулевой этап защиты данных

Дмитрий Стельченко

Куратор представительства
в Сибирском ФО

SEARCHINFORM
INFORMATION SECURITY

«СЁРЧИНФОРМ» СЕГОДНЯ

SEARCHINFORM
INFORMATION SECURITY

25 лет в IT

3 000+ клиентов в
22 странах мира

6 продуктов для
комплексной безопасности

2 000 000+ ПК под защитой
продуктов «СёрчИнформ»

Решения «СёрчИнформ»
рекомендованы к внедрению
и тиражированию в регионах
Минпромторгом РФ, Аналитическим центром при Правительстве РФ, Митистерством цифровизации РФ

Продукты «СёрчИнформ» входят
в Реестр отечественного ПО

Нулевой этап защиты данных

0 – Категоризация

1 – Определение нарушений

2 – Контроль каналов нарушений

3 – Расследование нарушений

4 – Актуализация политик безопасности

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

В ЧЕМ ПРОБЛЕМА?

Информации много, без контроля она утекает, теряется, важные файлы случайно или намерено удаляют или вносят в них ненужные правки.

Поэтому организации необходимо знать:

- Какие документы содержат критичную для бизнеса информацию?
- Сколько в компании таких данных и где они находятся?
- Кто имеет к ним доступ и может их редактировать?

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

ПОЧЕМУ НУЖНО НАВЕСТИ ПОРЯДОК?

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

КАК РЕШАТЬ?

Платформенные средства

✓ Обеспечивают частичный аудит действий и контента.

✗ Нет анализа действий и контента вне определенной платформы.

Средства ОС

✓ Помогают в распределении прав доступа к файлам.

✗ Не учитывают содержимое файлов и ценность этой информации.

DLP

✓ Отслеживают передачу по цифровым каналам, выявляют утечки данных.

✗ Не считают нарушением действия, если конфиденциальные файлы не покидают периметр.

DCAP

✓ Находят и классифицируют уязвимые данные в любой точке инфраструктуры в реальном времени.

✓ Проводят аудит прав и операций с учетом критичности данных для бизнеса.

FILEAUDITOR – ПЕРВАЯ ОТЕЧЕСТВЕННАЯ DCAP

для широкого потребителя

Выявляет в общем документообороте информацию, подлежащую защите.

Защищает конфиденциальные данные.

Следит за операциями с конфиденциальными данными.

Управляет доступом к данным: отслеживает группы сотрудников, которые создают, хранят или обрабатывают данные ограниченного доступа.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

ИСТРУМЕНТЫ ПОИСКА

FileAuditor поддерживает поиск по:

- ключевым словам, фразам и последовательности символов (иноязычные вставки, @, №, $, % и т.д.);
- словарям;
- регулярным выражениям;
- атрибутам.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

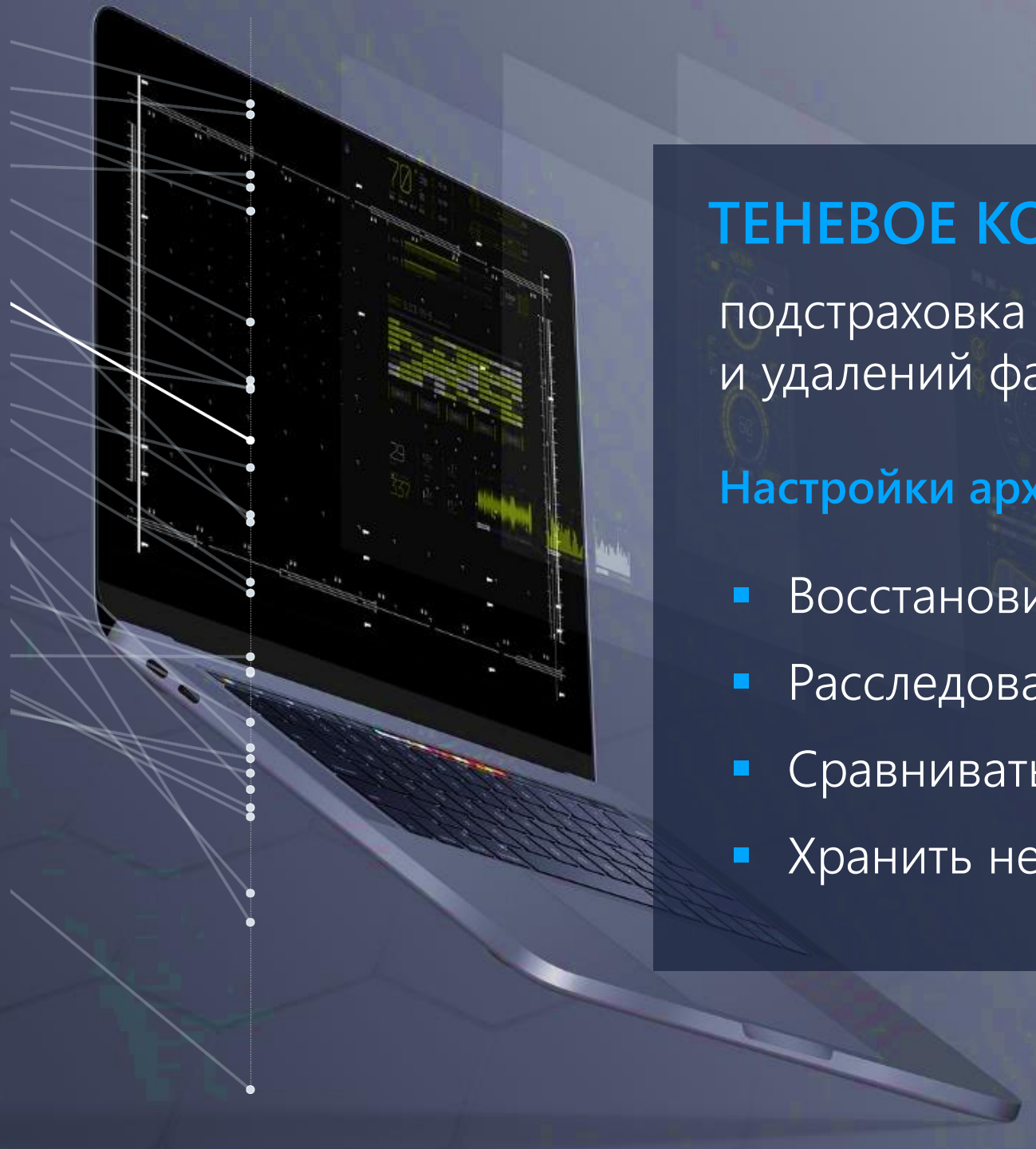
ПРОВЕРКИ ПО ПОЛИТИКАМ БЕЗОПАСНОСТИ

FileAuditor поддерживает **проверки по политикам безопасности** и формирует оповещения о новых событиях в файловой системе по заданным критериям.

Можно отследить «судьбу» конкретных файлов и папок после сканирования хранилищ, получать уведомления при изменении, удалении, перемещении данных. И проконтролировать нарушения в работе с конфиденциальными файлами.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB



ТЕНЕВОЕ КОПИРОВАНИЕ В FILEAUDITOR

подстраховка от нежелательных изменений
и удалений файлов

Настройки архивирования: «спасти» и «сохранить»

- Восстановить удаленный или искаженный файл
- Расследовать, кто, что и как менял/удалял
- Сравнивать версии файла
- Хранить несколько последних версий файла

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

ПРАВИЛА КЛАССИФИКАЦИИ В FILEAUDITOR

безошибочное определение конфиденциальной информации в корпоративной сети

Категоризация всех файлов в корпоративной сети:

- Поиск всех файлов, совпадающих по ключевому признаку (фразовый, по атрибутам, по последовательности символов, по словарю, регулярным выражениям)
- Маркировка конфиденциальных документов разных категорий
- Управление правами доступа к разным категориям файлов

ОПОВЕЩЕНИЯ В FILEAUDITOR

своевременные оповещения об изменениях в файловой системе

Политики безопасности: свежие новости о документах

- появились новые документы с конфиденциальным содержимым
- конфиденциальные файлы были изменены
- важный файл или папка перестали попадать в категорию конфиденциальных
- пользователь получил доступ/совершил нежелательное действие с заданным файлом

**Настройка политик по атрибутам, фразам, последовательности символов, словарю, регулярным выражениям и др.*

SEARCHINFORM INFORMATION SECURITY #CODEIB

СЁРЧИНФОРМ FILEAUDITOR

- Мониторинг файловых хранилищ;
- Аудит прав доступа;
- Алерты об инцидентах: неправомерный доступ, изменение/удаление файлов.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

КЛЮЧЕВЫЕ ФУНКЦИИ FILEAUDITOR

- **Классификация** документов с конфиденциальной информацией (ПДн, коммерческая тайна и др.);
- **Маркировка** документов (новые документы, служебные инструкции, секретный договор);
- **Аудит прав доступа** к ресурсам и файлам, отслеживание учетных записей с привилегированными правами;
- **Архивирование** документов – теневое копирование критичных файлов и сохранение истории операций с ними;
- **Отслеживание** версий и маршрута документа;
- **Контроль за действиями пользователей** – создание, редактирование, перемещение и удаление критичных файлов.

SEARCHINFORM INFORMATION SECURITY #CODEIB

БЛОКИРОВКИ НЕЖЕЛАТЕЛЬНЫХ ДЕЙСТВИЙ С ФАЙЛАМИ И ПАПКАМИ

В FileAuditor реализованы блокировки передачи документов: на документ ставится метка «Финансовые документы», «Коммерческая тайна» и т.д.

После этого можно:

- запретить отправку файла с меткой;
- предотвратить загрузку в облако;
- блокировать отправку в мессенджере документа.

Метки сохраняются при копировании, изменении, пересохранении и переносе файла на USB.

Запреты можно задать для всех или отдельных пользователей/ПК, а также настроить исключения. О файлах, попавших под блокировку, ИБ-специалисты будут узнавать из оповещений на email.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

ДУМАЕТЕ ВАС ЭТО НЕ КАСАЕТСЯ?

8 из 10 сотрудников хранят файлы с паролями от рабочих аккаунтов на ПК. При их компрометации уязвимыми окажутся все корпоративные сервисы.

Конфиденциальный документ без контроля попадает за пределы круга доверенных сотрудников в среднем **за 36 часов.** За **2 недели** круг сотрудников с доступом увеличивается **в 5 раз**.

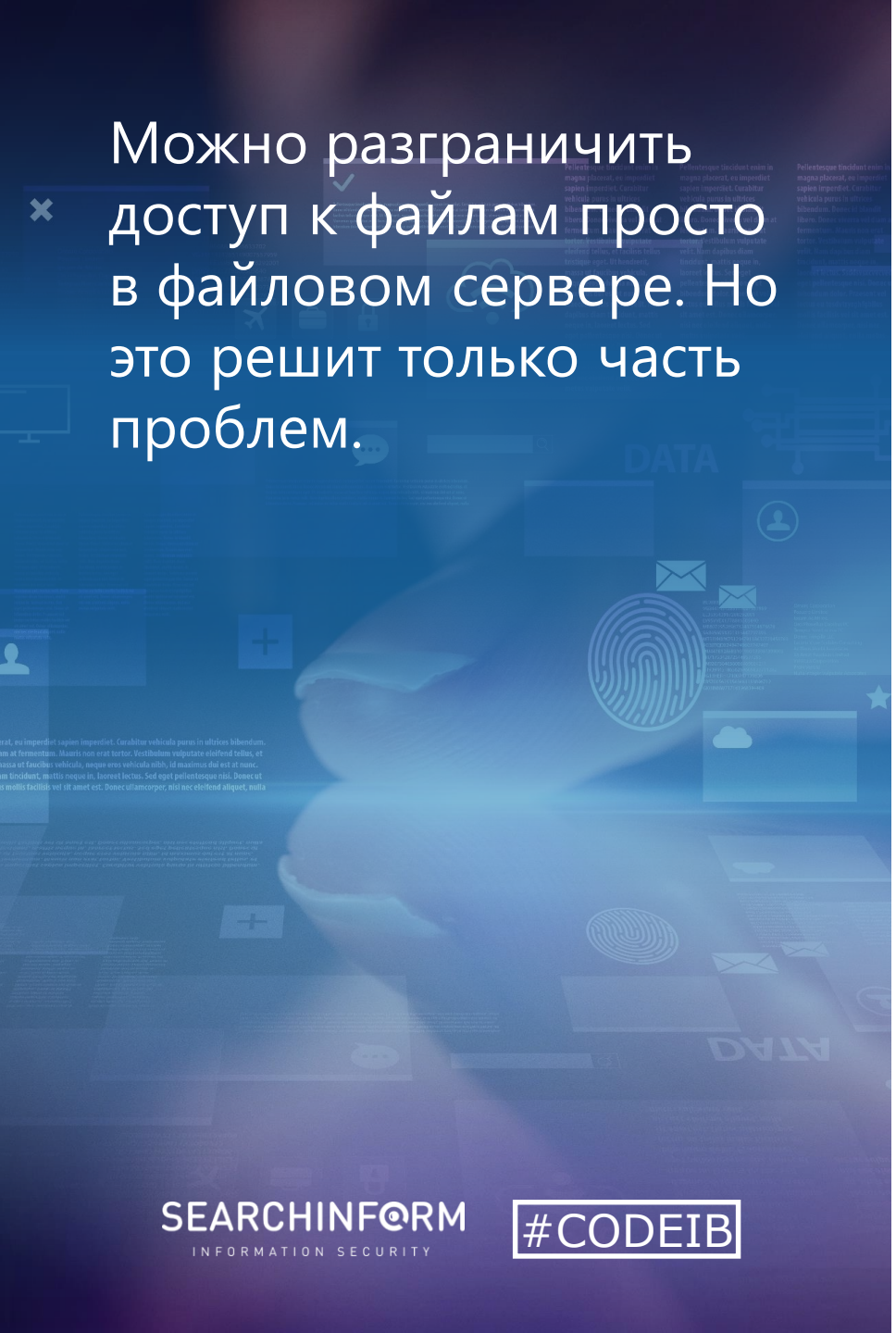
Каждая третья компания обнаруживает неучтенные копии критичных документов на рабочих станциях пользователей. В них вносятся нерегламентированные правки, это порождает неразбериху и открывает поле для махинаций.

100% компаний находят избыточные права доступа к файлам и папкам с конфиденциальной информацией, в том числе для учетных записей давно уволенных сотрудников.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

*Данные собраны в рамках сервисного сопровождения компаний, внедривших или тестировавших FileAuditor в 2020 г.



Представим ситуацию:

- Пользователь с легитимным доступом переложил файл из конфиденциальной папки в общую.
- Личный помощник гендиректора переместила график встреч, к которому имеет доступ по должности.
- Логирование действий покажет: такого-то числа помощница переложила файл «график» из папки на своем компьютере в папку «новости_2020», к которой имеет доступ вся компания.
- Если эта помощница похитрее и догадалась переименовать файл, сделала не «график встреч генерального», а «doc1» – ИБ-специалист такой инцидент пропустит. Если только он вручную не просматривает содержимое каждого из сотен и тысяч перемещенных файлов в организации.

ПОЧЕМУ FILEAUDITOR?

Лидер рынка DCAP в России и мире – Varonis: софт мощный, но дорогой, ресурсоемкий и не адаптирован к реалиям РФ. **Мы сделали FileAuditor по прямому запросу заказчиков**, которые искали доступный аналог с широким функционалом и качественной реализацией, учитывающий локальные особенности и подходящий для импортозамещения.

Интеграционная гибкость
Поддержка любых ОС и подавляющего большинства файловых систем.

Профилактика нарушений
Раннее обнаружение проблем в хранении и работе с данными предупреждает 64% внутренних инцидентов ИБ, которые происходят неумышленно.

Выполнение требований закона
152-ФЗ, 187-ФЗ, приказы ФСТЭК и прочих отраслевых регуляторов.

Заказчики в РФ и 11 странах мира

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

Решать ИБ-задачи нужно в комплексе.

SEARCHINFORM
INFORMATION SECURITY

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

https://t.me/
searchinform

https://www.facebook.
com/SearchInform

https://vk.com/
securityinform

Практика и аналитика

https://searchinform.ru/
practice-and-analytics/

SEARCHINFORM
INFORMATION SECURITY

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11 марта 2021 года, Красноярск

#CODEIB

SEARCHINFORM

INFORMATION SECURITY