КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТРАНСФОРМАЦИЯ DLP, DCAP В РАЗРЕЗЕ 2020-2023

Что было и чего ожидать?

Александр Янчук

Заместитель генерального директора
по Северо-Западному ФО

SEARCHINFORM
INFORMATION SECURITY

«СёрчИнформ» сегодня

3 000+ клиентов по всей России в

20+ странах мира **25+** лет в IT

6 решений для комплексной защиты бизнеса

2 000 000+ ПК под защитой продуктов «СёрчИнформ»

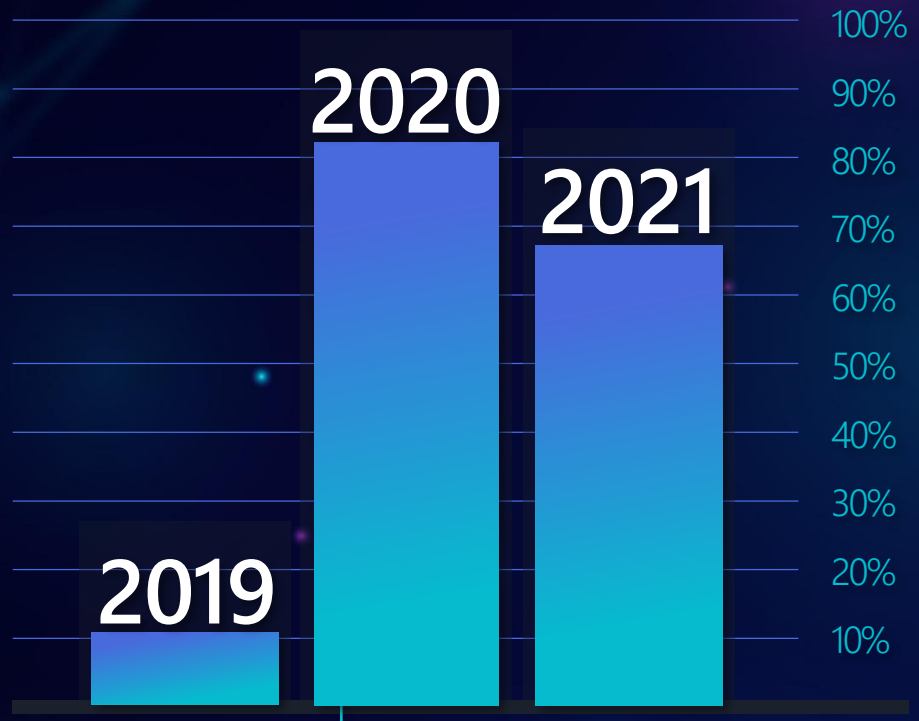
Продукты «СёрчИнформ» входят в Реестр отечественного ПО

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

SEARCHINFORM
INFORMATION SECURITY

ТРЕНД

Гибридный формат работы



Данные «СёрчИнформ КИБ» на ПК вне офиса

39%

специалистов умственного труда во всем мире будут работать в гибридном формате к концу 2023 года. Это на 2% больше, чем в 2022 году.

По данным Gartner.

Нужно строить защиту с учетом этого фактора.

Бизнес проходил 3 стадии

SEARCHINFORM
INFORMATION SECURITY

1

Сделать, чтобы хоть что-то как-то работало.

2

Понять, чем теперь занимаются сотрудники на удалёнке.

3

Старый контроль в новых декорациях.

РАБОТАЕМ С ТЕМ, ЧТО ЕСТЬ

SEARCHINFORM
INFORMATION SECURITY

Доступ:

- Со своей машины либо с корпоративной
- К рабочему месту (RDP, VDI) либо напрямую к сервису
- Тащим документы к себе или нет

БЛОКИРОВКИ

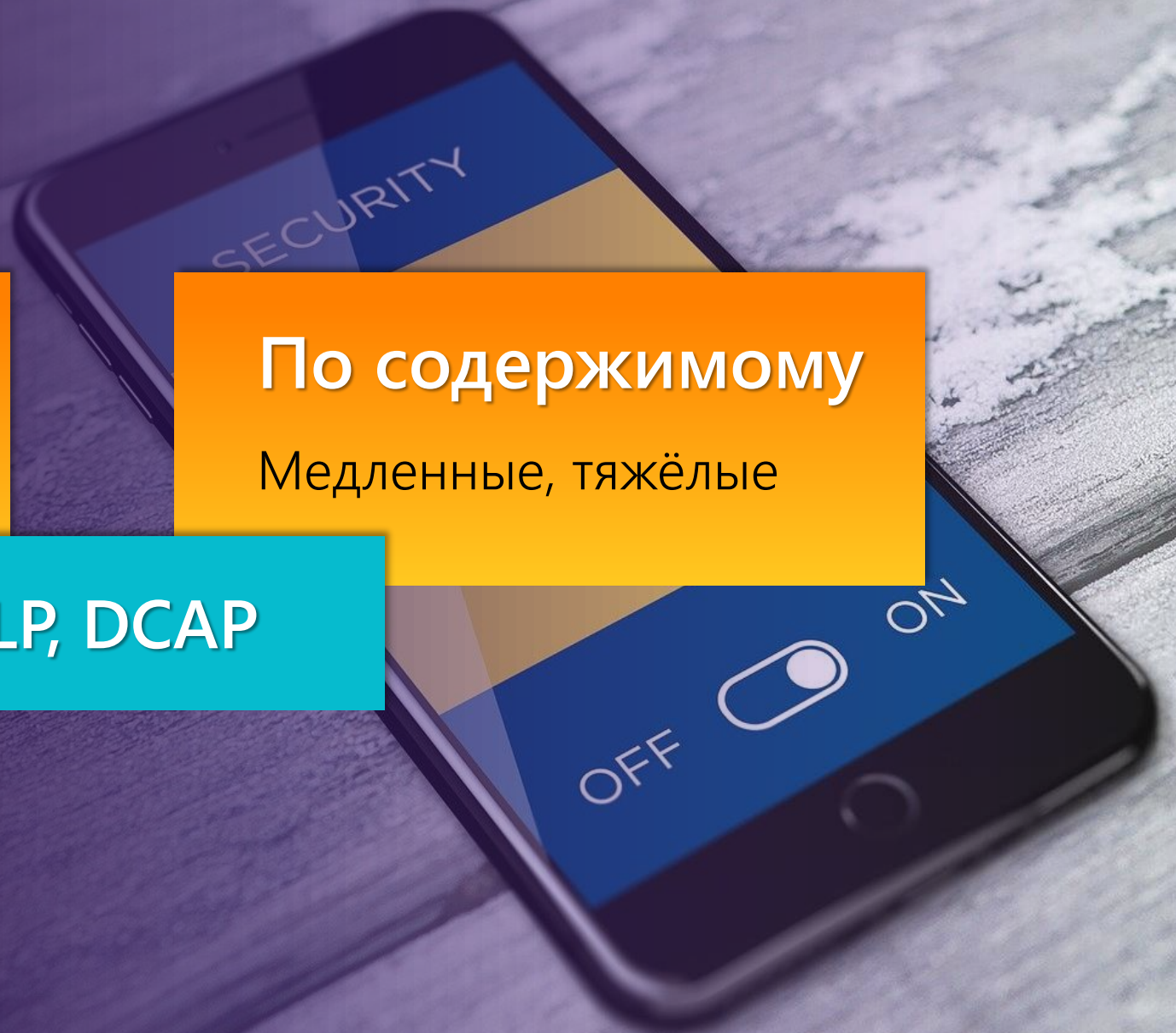
По атрибутам

Быстрые, лёгкие

По содержимому

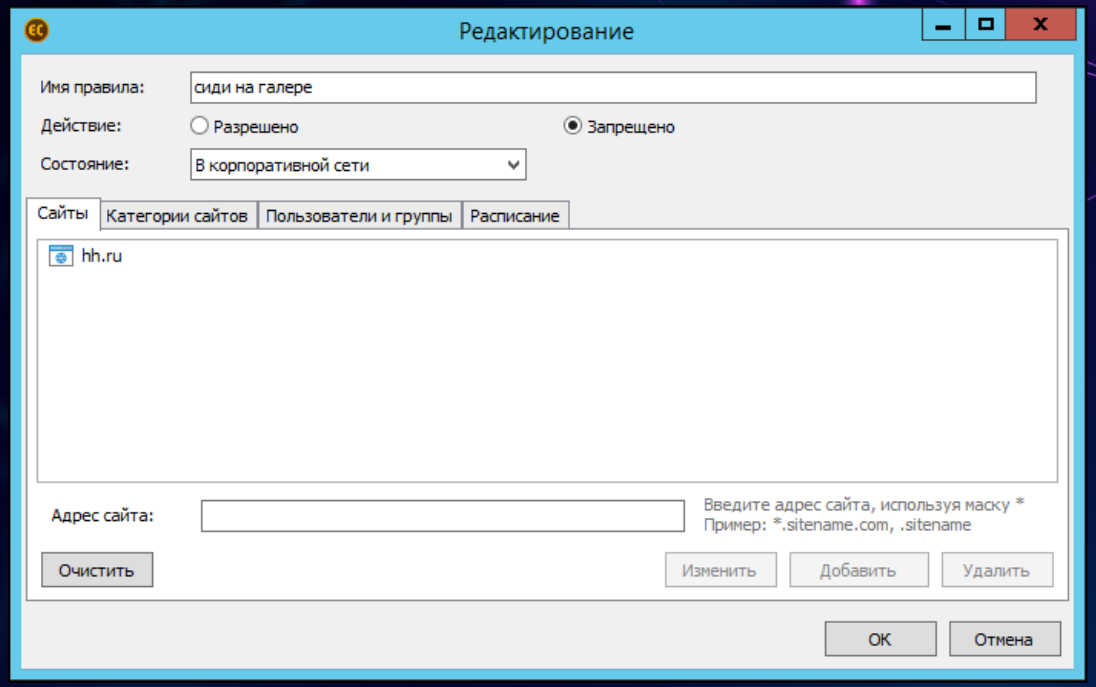
Медленные, тяжёлые

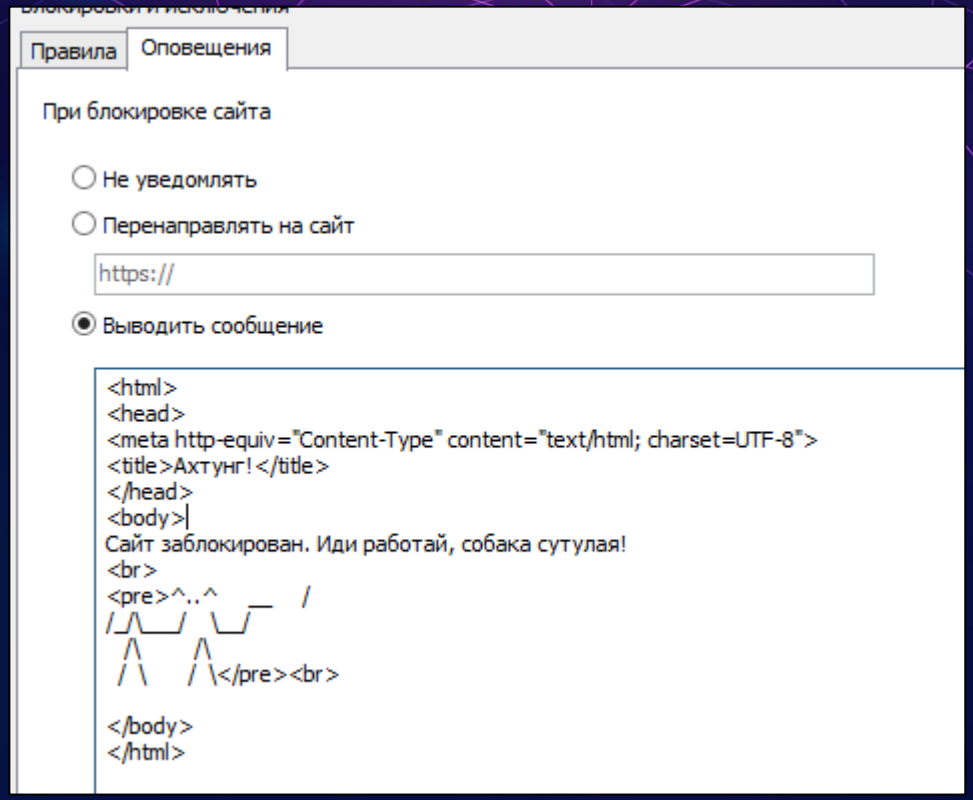
DLP, DCAP

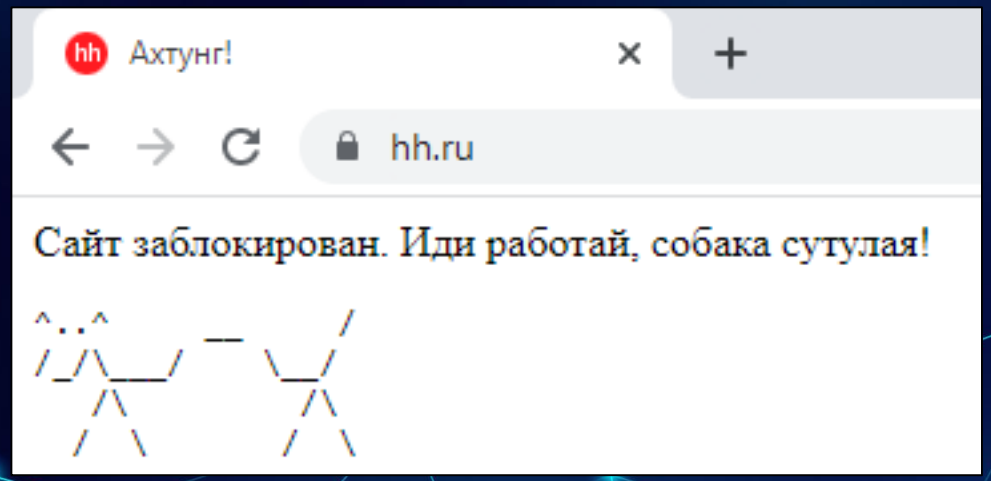


SEARCHINFORM
INFORMATION SECURITY

SEARCHINFORM
INFORMATION SECURITY







Взаимодействие с пользователем

SEARCHINFORM
INFORMATION SECURITY

Инциденты | Параметры политики безопасности

Добавить критерий | Редактировать критерий | Удалить критерий | Копировать | Вставить

Критерий поиска	Описание
Письмо с вложением	Фразовый поиск: доля в уставном капитале
Письма с зашифрованными файлами в черновиках	Черновик: 0 and Поиск по зашифрованным документам
Остановка по ключевому слову	Фразовый поиск: бздыни

Основные | Запуск внешнего скрипта

Получатели уведомлений — Добавить | Удалить

Уведомления
- [x] Уведомлять пользователя о событиях по этим критериям
- [x] Разрешить пользователю разблокировать свои письма, блокированные по этим критериям
- [x] Разблокировать письма без подтверждения отделом безопасности
- [ ] Прикрепить оригинальное письмо

Списки исключений

	Название

Расписание работы критериев карантина
- [ ] Выполнять проверку только в рабочее время

Отладочный режим
- [ ] Включить отладочный режим

Настройка уведомлений

Для аудиторов
- ( ) Не отправлять уведомление
- (•) Дайджест уведомлений — Редактировать шаблон
- ( ) Одиночные уведомления — Редактировать шаблон
- [ ] Отправлять уведомления при ошибках отправки — Редактировать шаблон

Для пользователей

Отправлять уведомление:
- [x] о блокировке — Редактировать шаблон
- [x] о разблокировке — Редактировать шаблон
- [x] об отправке — Редактировать шаблон
- [x] о попадании в карантин — Редактировать шаблон
- о попадании в карантин со ссылкой — Редактировать шаблон
  - (•) по ссылке ( ) по ответному письм
  - Текст уведомления

- [ ] Добавлять копию письма в уведомления

Не прикреплять оригинал письма если его размер превышает 0 МБ

От KIB <>
Тема **Галактеко опасносте!!!1**
Кому Мне <pc1@tc.com>

Без паники, работают профессионалы!

Ваше письмо было заблокировано супер-секретными разработками на основе ИИ.

Но **если вы не согласны с нашим решением, действуйте сами.**

Для разблокировки и отправки его адресату перейдите по ссылке: Разблокировать сообщение

Дата отправки:	2021-11-25 15:07:40 +03:00
От кого:	<pc1@tc.com>
Кому:	<test1@tc.com>
Тема письма:	5678

С уважением, служба информационной безопасности.

Данное уведомление сформировано автоматически и не требует ответа

Взаимодействие с пользователем

НОВОЕ В ЗАКОНОДАТЕЛЬСТВЕ

1. Запрет на закупки иностранного ПО, полный отказ от использования иностранного ПО к 2025 г. для субъектов КИИ и др. организаций
   - Указ Президента РФ №166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
   - Указ Президента РФ №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
   - Постановление Правительства Российской Федерации №1478 от 22.08.2022
2. Новый порядок отчетности о компьютерных инцидентах с ПДн: поправки в ФЗ №152 (ФЗ №266, приказ ФСБ № 77 о порядке взаимодействия с ГосСОПКА)

Правительство до 1 июля 2023 г. рассмотрит ужесточение штрафов за утечку ПДн:
до 1% от годового оборота компании или до 3%
при попытке скрыть инцидент

НА УВЕДОМЛЕНИЕ – 24 ЧАСА, НА РАССЛЕДОВАНИЕ – 72 ЧАСА

УЖЕ В РЕЛИЗЕ

SEARCHINFORM
INFORMATION SECURITY

Ещё немного про функционал

- Больше функций на агенте
- Нейронки
- Упор на «экономичность»
- Упор на производительность
- Кроссплатформенность
- Уход от «старых» БД
- Поддержка «linux»

«Алло, это прачечная?»

SEARCHINFORM
INFORMATION SECURITY

	DCS	PCS
Пляшем от	Информации	Людей
Главная идея ИБ	Защита информации	Создание позитивной культуры ИБ
По умолчанию	Запрещено всё, что не разрешено	Разрешено все, но правильно (безопасно), вот так
Кто папка?	Безопасник лучше знает, как надо	Бизнес лучше знает, как надо. Безопасник подстраивается.
Принятие ответственности	Сотрудники должны…	Сотрудникам объясняют, как делать безопасно, но решение за ними
Документы	Требования и регламенты	Рекомендации, памятки, учебные материалы
Восприятие сотрудниками	ИБ — карающий контролер	ИБ — доверенный советник
Режим работы DLP	DLP в режиме блокировки	DLP в режиме мониторинга/отправка по требованию

ИНФРАСТРУКТУРА

Облака и ИБА

Гибридный формат работы,
контур безопасности размыт.

КОНТУР БЕЗОПАСНОСТИ

SEARCHINFORM
INFORMATION SECURITY

ПРИЧИНЫ ИНТЕРЕСА:

SEARCHINFORM
INFORMATION SECURITY

- Изменилось отношение работодателей
- Изменилось отношение безопасников
- Нарушение поставок «железа» и ПО

Все наши продукты могут полноценно работать в облаке и с облаками.

Спасибо за внимание!
Вопросы?

https://t.me/
searchinform

https://vk.com/
securityinform

https://www.youtube.com/
user/SearchInform

Практика и аналитика

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

SEARCHINFORM
INFORMATION SECURITY