Комплексная защита данных в госструктурах страны:
современные реалии

Алексей Парфентьев
Руководитель отдела аналитики «СёрчИнформ»

SEARCHINFORM
INFORMATION SECURITY

КАК ВСЕ ПОМЕНЯЛОСЬ С ПРОШЛОЙ ВСТРЕЧИ

SEARCHINFORM
INFORMATION SECURITY

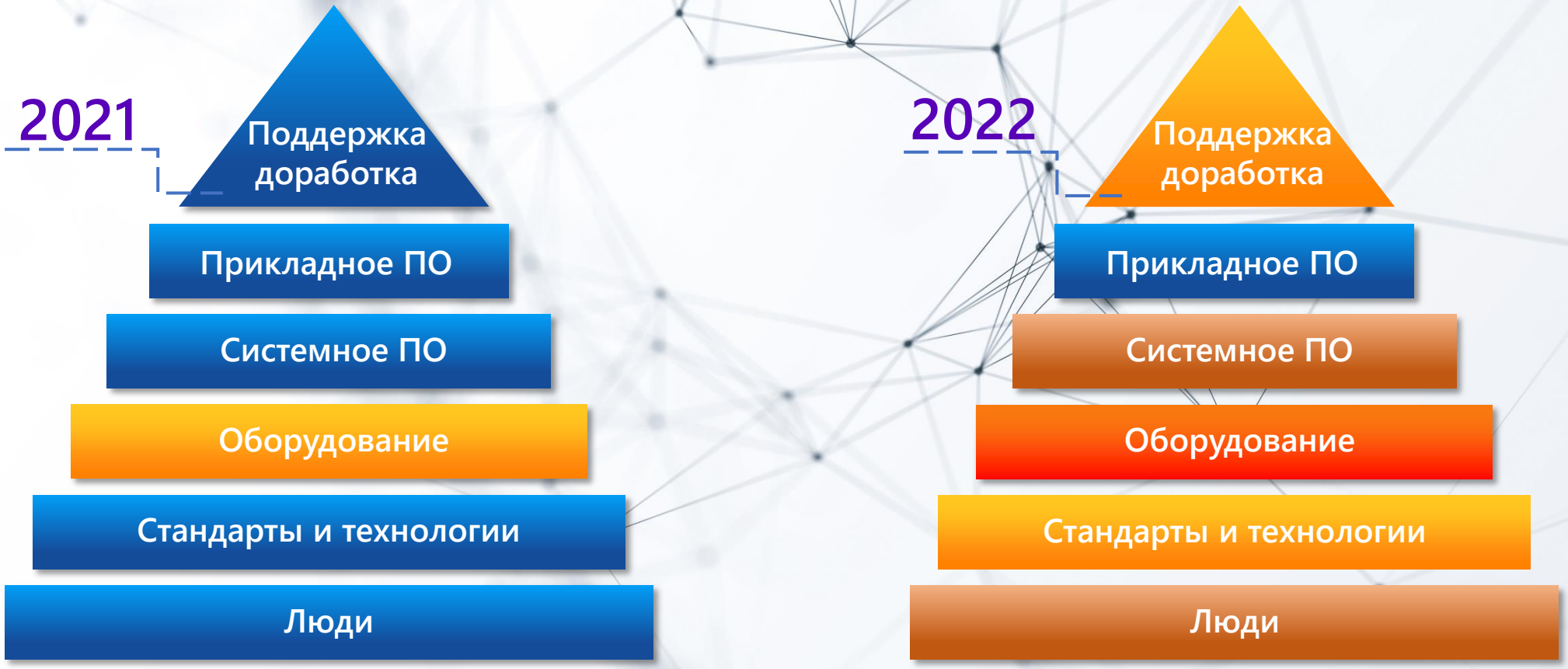
БЫЛО актуально

- Какие угрозы есть.
- Какие технологии существуют.
- Какие инструменты выбрать.
- Как их правильно использовать.

СТАЛО актуально

- Где взять людей?
- Где взять оборудование и софт?

Почему это произошло?



ИТОГО:

В долгосрочной перспективе – одни плюсы.

В краткосрочной – прогнозируем просадку цифровизации минимум на треть при вдвое возросших затратах.

SEARCHINFORM
INFORMATION SECURITY

ЗАДАЧИ В ИБ У ГОСУДАРСТВЕННЫХ КОМПАНИЙ

SEARCHINFORM
INFORMATION SECURITY

БЫЛИ РАНЕЕ

Совершенствование процессов ИБ.

- Сохранить работоспособность.
- Обезопасить основные процессы.
- Выдержать кадровый голод.
- Выполнять требования регуляторов.

АКТУАЛЬНЫЕ НА ДАННЫЙ МОМЕНТ

Необходимость обеспечения информационной безопасности

SEARCHINFORM
INFORMATION SECURITY

Стратегия национальной безопасности РФ

ИБ

Федеральные законы

- ФЗ-152
- ФЗ-187

Приказы ФСТЭК России

- №17
- №21

SEARCHINFORM
INFORMATION SECURITY

СТАТИСТИКА ПУБЛИЧНЫХ УТЕЧЕК ИЗ ГОСОРГАНОВ

1,1 млн.

паспортных данных проголосовавших онлайн по поправкам в Конституцию появились в продаже.

115 тыс.

записей россиян, которые застряли за границей с началом пандемии коронавируса и ждали вывозных рейсов.

1,2 млн.

записей Белгородского аграрного университета: персданные студентов, платежная информация, расписание занятий.

360 тыс.

записей из информсистем Минюста России, Роструда России, ФАС, Федерального казначейства и Мэрии Москвы.

28 тыс.

записей с портала госуслуг в Ханты-Мансийском автономном округе.

Проблемы

Вопросы обеспечения информационной безопасности требуют совершенствования или не выполняются

SEARCHINFORM
INFORMATION SECURITY

Что происходит?

- Утечки служебной информации
- Небезопасная активность сотрудников
- Утечки персональных данных
- Коррупционная деятельность
- Саботаж

Решение проблемы:

1. **Закупка оборудования и ПО, найм специалистов.**
2. **Подписка на сервис, найм специалистов.**
3. Создание Центра мониторинга информационной безопасности (ЦМИБ)

Решение проблемы

Создание Центра мониторинга информационной безопасности (ЦМИБ)

Центр мониторинга ИБ, предоставляющий услуги аутсорсинга государственным учреждениям региона со штатом квалифицированных *ИБ-специалист ов*

(30-50 сотрудников).

Функции ЦМИБ:

- Предотвращение утечек данных.
- Контроль рабочего активности сотрудников.
- Предоставление заказчику ИБ-аналитики и отчетов.
- Информирование об инцидентах.
- Обеспечение технической поддержки.

SEARCHINFORM
INFORMATION SECURITY

SEARCHINFORM
INFORMATION SECURITY

Структура ЦМИБ:

Технические средства защиты информации:

SIEM-система используется для сбора, анализа и реагирования на события информационной безопасности.

DLP-система защищает от утечек информации и мошеннических действий сотрудников.

DCAP-система необходима для аудита файлов и поиска нарушений прав доступа к документам.

ProfileCenter система составляет психологический профиль сотрудника и оценивает риски личности для общества и организации.

Кадры:

2 ИБ-специалиста

2000-3000 контролируемых компьютеров

Технические средства защиты информации «СёрчИнформ» успешно применяют:

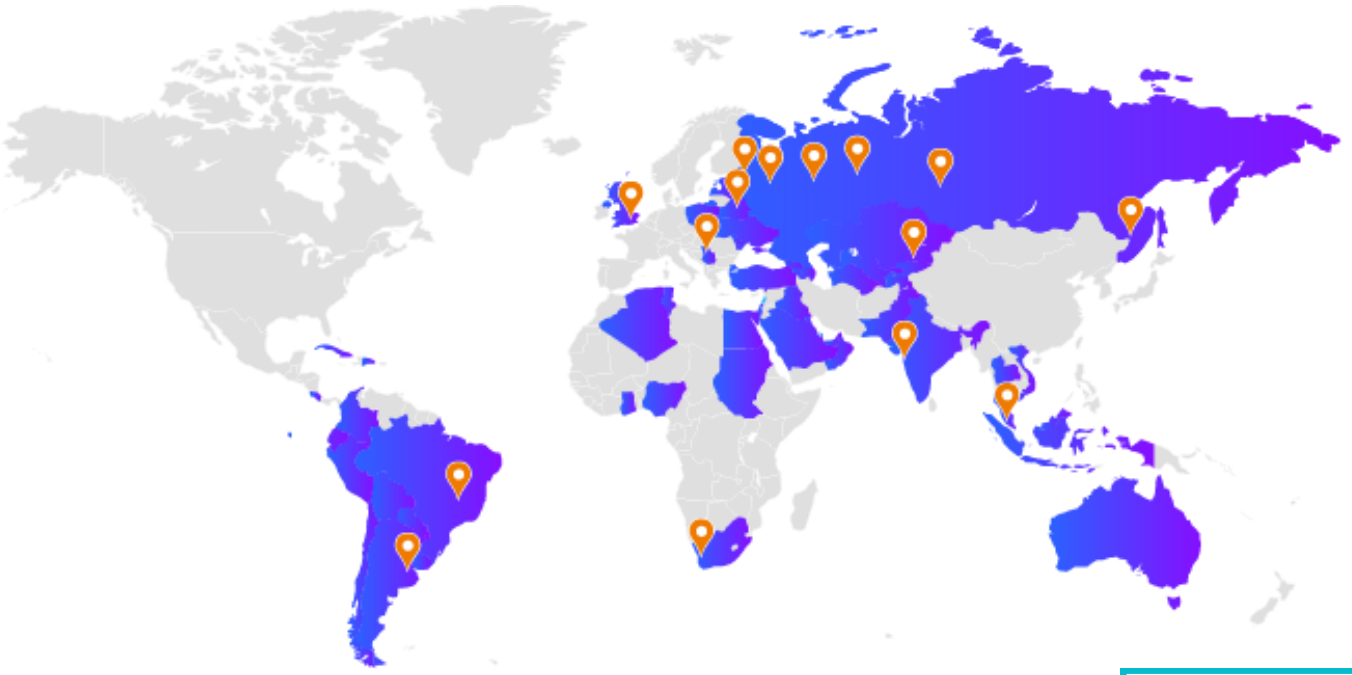
- Правительство Москвы
- Правительство ХМАО
- Правительство Республики Татарстан
- Правительство Республики Коми
- Минпросвещения России
- Минвостокразвития России
- Минтруд России
- Минздрав России
- Росфинмониторинг

Результаты создания Центров мониторинга ИБ:

SEARCHINFORM
INFORMATION SECURITY

- Решение проблем утечек информации из государственных систем, разглашения персональных данных и другой критичной информации.
- Предотвращение неправомерных действий (изменений) с критичными данными (служебной информацией).
- Реализация задач импортозамещения.
- Сокращение расходов на обеспечение ИБ у организации, подключенных к ЦМИБ.
- Обеспечение комплексной защиты ИТ-инфраструктуры государственных учреждений и подведомственных организаций, повышение уровня ИБ.
- Защита от внешних и внутренних угроз информационной безопасности.
- Повышение продуктивности сотрудников государственных структур.
- Создание новых рабочих мест.

«СёрчИнформ» сегодня



3 000+ клиентов по всей России и в **20+** странах мира

25 лет в IT

6 решений для комплексной защиты бизнеса

2 000 000+ ПК под защитой продуктов «СёрчИнформ»

Решения «СёрчИнформ»

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

Продукты «СёрчИнформ» входят в Реестр отечественного ПО

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