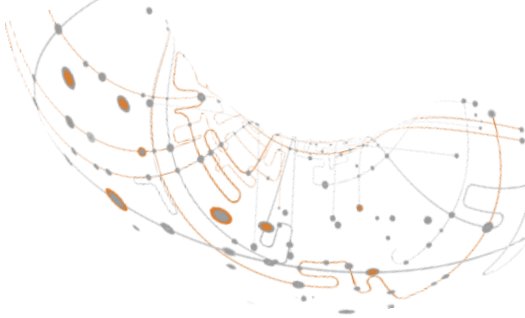
ОПЫТ ПРОВЕДЕНИЯ ПРОЕКТА SAM CYBER SECURITY

АГМУ

www.galex.ru

Начало проекта

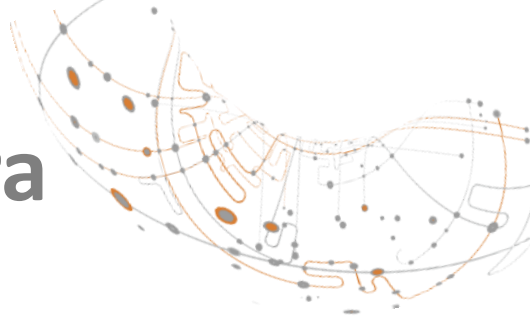


- Смена команды
- 10 лет стихийного развития ИТ
- Полное отсутствие информации о лицензиях
- Полное отсутствие документации по ИТ-инфраструктуре
- 6 корпусов **(об одном узнали в ходе проекта!)**
- 1000 ПК
- Отсутствие единой системы аутентификации

Инструменты

- Ручной сбор информации о наклейках (представители Заказчика).
- Выгрузки из БД Kaspersky Security Center.
- Инвентаризация с помощью WinAudit.
- Информация с DNS, DHCP.
- Сканеры безопасности: NMAP, Metasploit.
- Ручной анализ информации.

Порядок проведения проекта



1. Инвентаризация всего установленного ПО автоматизированными инструментами
2. Опись всех ПК, поиск наклеек подтверждения подлинности Windows
3. Сканирование внешнего периметра сканерами безопасности
4. Ручной анализ периметра для контроля работы сканеров
5. Анализ установленного ПО с точки зрения лицензирования
6. Выработка рекомендаций по развитию ИТ-инфраструктуры
7. Подготовка отчета о проекте

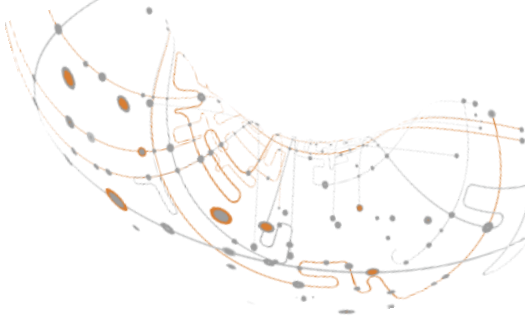
Краткие итоги

По итогам проекта сверки лицензий выявлено ПО необеспеченное лицензиями Microsoft на общую сумму:
3 576 839 рублей.
Размер юридического риска может составить до: **10 730 517** рублей.

В ходе проекта выявлены высокие риски информационной безопасности:

1. Отсутствие обновлений практически на всех ПК.
2. ~80% ПК используют Windows XP.
3. Антивирус только на 60% ПК.
4. Обнаружены следы взлома нескольких сайтов.
5. Найдены персональные данные, доступные из публичных сетей.

Что дало



- ✓ Текущий срез состояния ИТ для руководства
- ✓ План развития инфраструктуры
- ✓ Предложение по оптимизации лицензирования ПО (**снижение бюджета закупки**)
- ✓ Достигли 100% покрытия антивирусом
- ✓ Отчет о потенциальных угрозах ИБ
- ✓ Рекомендации по устранению обнаруженных проблем

Спасибо за внимание!