ICL SYSTEM TECHNOLOGIES

Сервисный подход при реагировании на киберугрозы

ФИО

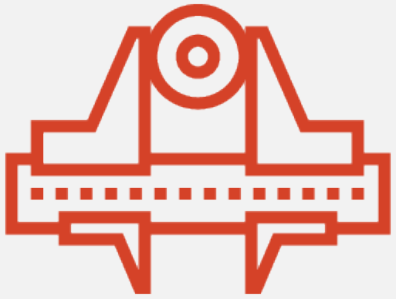
Должность

Типовая ситуация на практике

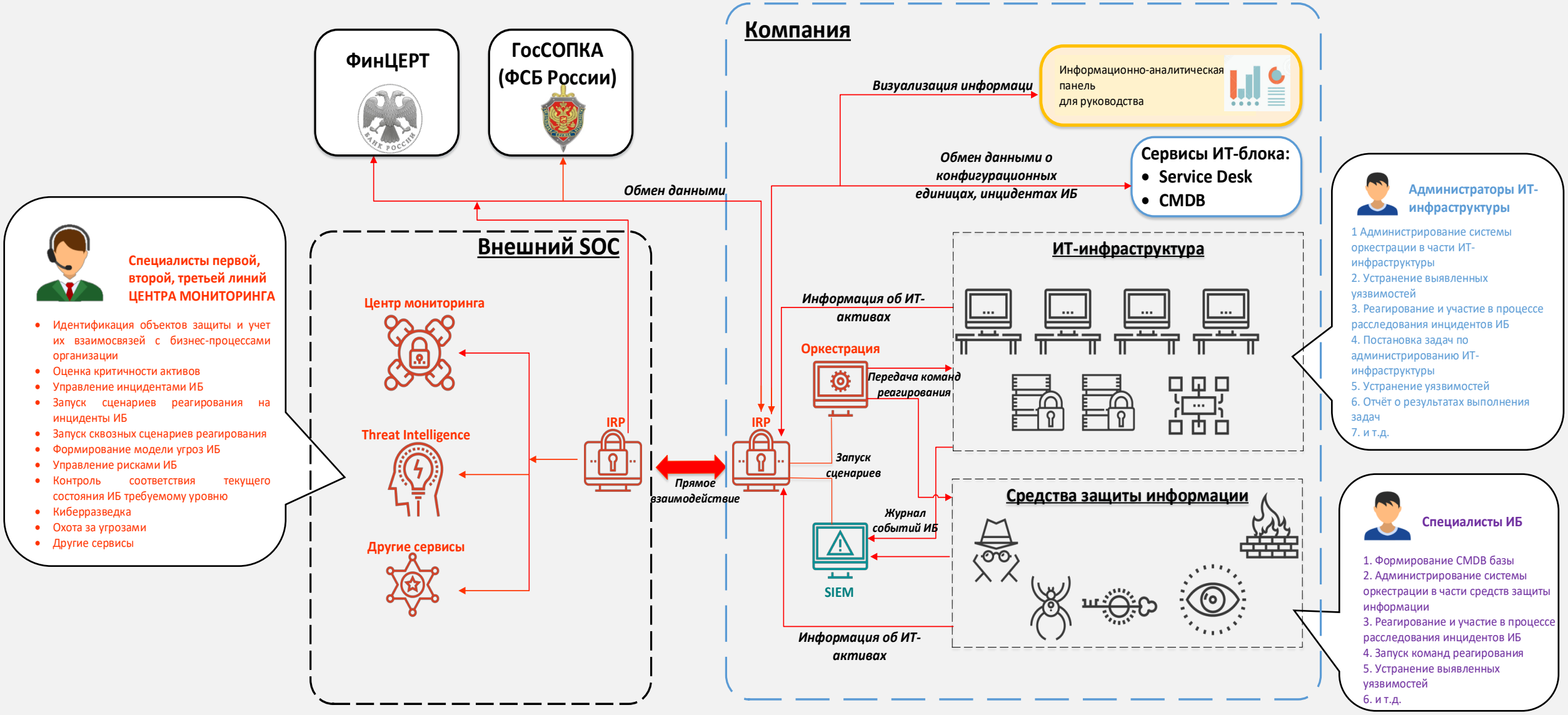
Инфраструктура и персонал в Компании	Взаимодействие с внешним SOC-центром
В Компании есть набор СрЗИ, но мало специалистов по ИБ	*Уведомлений об инциденте ИБ недостаточно для его нейтрализации в кратчайшие сроки*
Большая инфраструктура, в том числе объекты КИИ (значимые)	*Текущее количество сотрудников ИБ в Компании не справляется с реагированием и нейтрализацией на возросшее количество инцидентов ИБ*
Необходимость взаимодействия с ГосСОПКА	*Необходимость выполнения задач по реагированию на удалённых площадках, где ИБ-специалистов вообще нет*
Наличие филиалов/удалённых площадок, где специалисты по ИБ вообще отсутствуют (например, промысловые площадки)	*Двойная переплата за SOC и свою IRP*

Возможные решения

- *Развёртывание IRP на территории Компании как сервиса по предоставлению в аренду*
- *Логическая связка IRP SOC и IRP Компании*
- *Развёртывание системы оркестрации на территории Компании как сервиса по предоставлению в аренду с подключением к IRP*
- *Реализация сквозных сценариев реагирования с помощью арендуемых (с возможностью последующего выкупа) IRP и системы оркестрации*



Архитектура решения

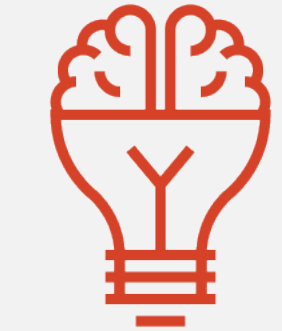


Оркестрация. Для чего она?

- *Возможность удалённого запуска согласованных сценариев реагирования на типовые инциденты ИБ*
- *Возможность внесения согласованных изменений в инфраструктуру филиалов (блокировка IP, хэш файлов и т.д)*

Оркестрация. Преимущества использования

- *Соблюдение принципа сервисной изолированности*
- *Отсутствие избыточных прав в IRP при доступе к ИТ-инфраструктуре Компании*
- *Возможность разнесения областей реагирования за счёт применения нескольких оркестраторов*



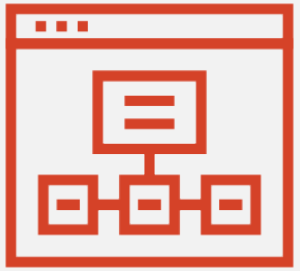
Реализация сквозных сценариев реагирования

- *Сценарий, предполагающий действия SOC и Заказчика в рамках интеграции IRP*
- *Формирование SOCом рекомендаций по запуску конкретного сценария реагирования для нейтрализации инцидента ИБ*

Сквозные сценарии без IRP

SOC

IRP



Оповещение Заказчика

Компания

Service Desk

Детектирование и Анализ

Проверка на False Positive

Обогащение доп. информацией

Расширенный Анализ

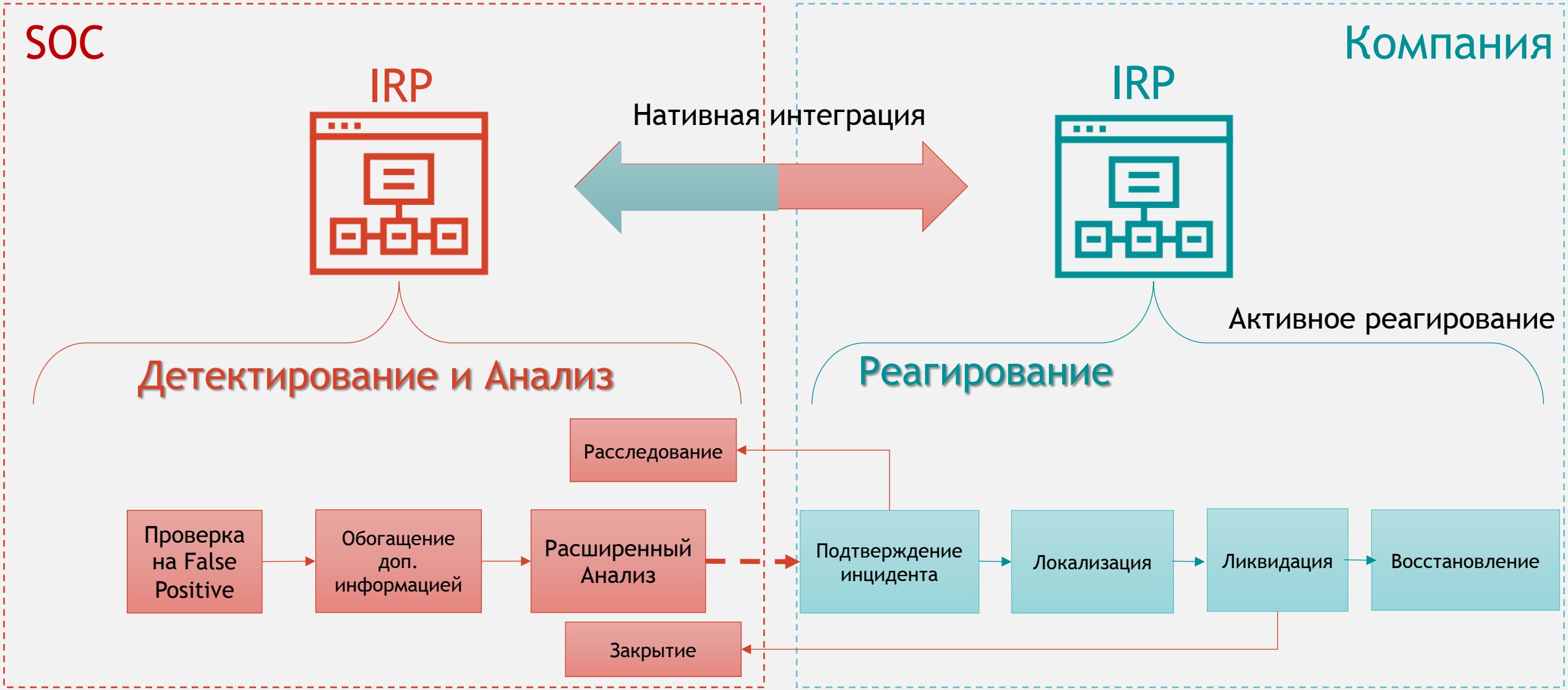
Реагирование

???

???

???

Сквозные сценарии с арендуемой IRP



Сервисная модель аренды. Распределение ролей

SOC-центр	Вендор	Компания
Мониторинг и обнаружение инцидентов ИБ	Предоставление единой платформы взаимодействия	Валидация предложенных SOCом сценариев реагирования на инциденты ИБ по типовым сценариям
Передача информации о выявленных инцидентах и запуск сценариев реагирования через IRP-платформу, интегрированную с арендованной IRP заказчика	Предоставление коннекторов к различным производителям SIEM решений, типовых сценариев реагирования (playbook)	Заведение единой базы учета ИТ-активов (CMDB) на базе арендованной IRP, контроль за устранением инцидентов ИБ
Сканирование и выявление уязвимостей	Автоматический сбор данных об уязвимостях и привязка к ИТ-активам, выполнение работ по их устранению	Выполнение работ по устранению уязвимостей
Подготовка инцидентов на ОКИИ в ГосСОПКА	Предоставление коннектора к ГосСОПКА	Взаимодействие с ГосСОПКА, передача данных о выявленных SOC инцидентах
Адаптация типовых сценариев и разработка новых сценариев реагирования	Интеграция с различными СрЗИ для внесения изменений, применение системы оркестрации	

Что получает SOC?

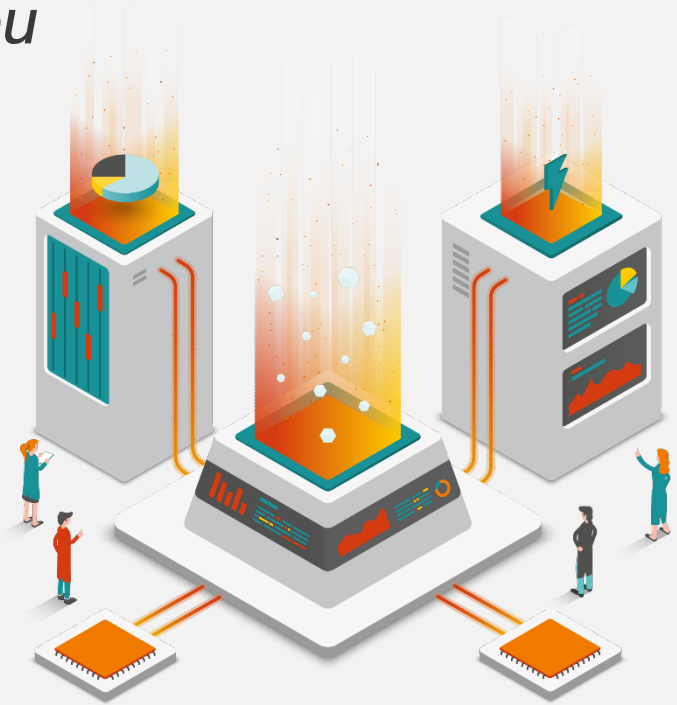
Для SOC

- *Обеспечение оперативной реакции на инцидент ИБ для его устранения*
- *Реализация сквозных сценариев реагирования на инциденты ИБ*
- *Координация и автоматизация устранения уязвимостей*

Что получает Компания?

Для Компания

- *Обеспечение прозрачности работы SOC-центра при реагировании на инциденты ИБ*
- *Наличие собственного инструмента оркестрации для нейтрализации инцидентов ИБ*
- *Вовлечение собственных сотрудников в процессы управления ИБ*
- *«Обкатка» своих компетенций и процессов управления ИБ*
- *Отсутствие единовременных больших затрат на создание системы управления ИБ*
- *Наполнение и наличие в будущем собственной ретроспективной базы информации*



Результат реализации от сервисной модели

- ✓ *Использование текущих ресурсов без кап.вложений*
- ✓ *Сокращение времени реагирования и расследования инцидентов ИБ*
- ✓ *Повышение эффективности борьбы с новыми угрозами и уязвимостями*

СПАСИБО ЗА ВНИМАНИЕ!

Компания ICL System Technologies

420029, Казань, Сибирский тракт, 34

Телефон: +7(843) 279-58-23

Факс: +7(843) 279-49-05

Электронная почта: info@icl.kazan.ru

Веб-сайт: www.icl.ru