ICL SERVICES

Аутсорсинг ИБ. Головная боль или стратегическое преимущество?

Алексей Морозков
Старший руководитель центра управления кибербезопасностью

Терминология

Аутсорсинг ИБ

Передача части или всех функций обеспечения ИБ на управление и поддержку другой компании.

Управляемые сервисы ИБ

Комплекс услуг ИБ, предоставляемый заказчику на базе SLA в рамках договора с провайдером управляемых услуг.

Одноразовые проекты по ИБ

Управляемые сервисы ИБ на необходимый срок

Примеры задач ИБ для передачи на аутсорсинг

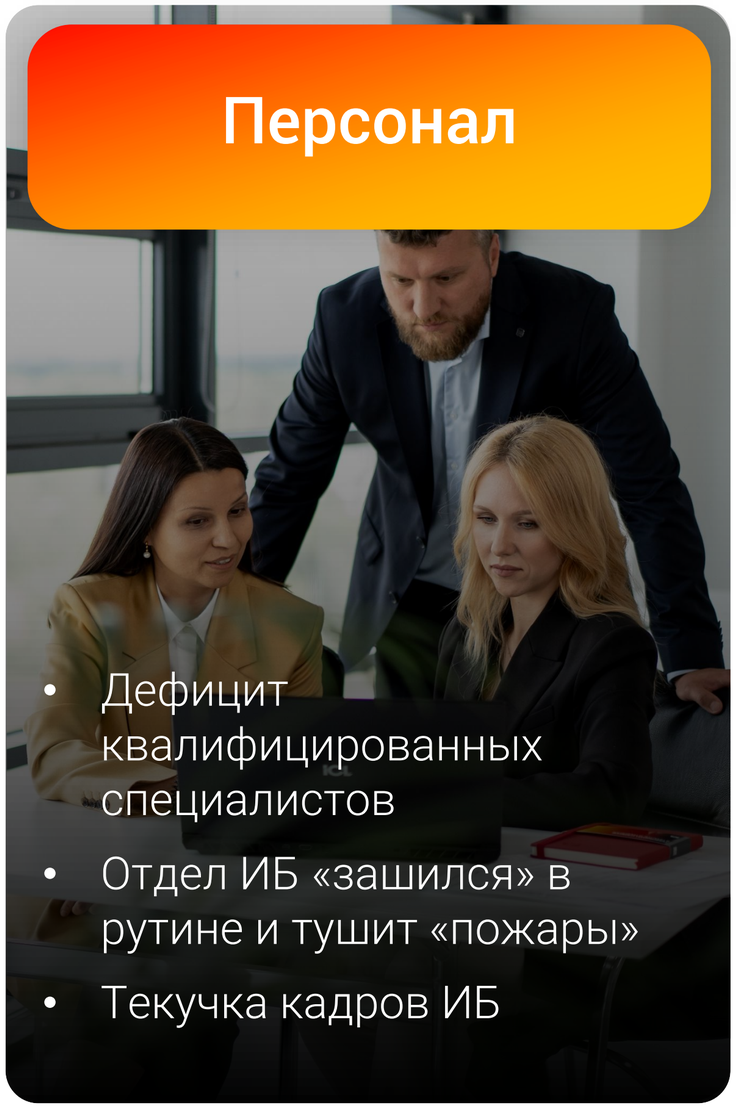
- Поддержка антивируса, защита почты, DLP, МСЭ/NGFW.
- Аудит ИСПДн 152-ФЗ.
- Анализ защищенности.
- Проектирование и внедрение SIEM / XDR.
- Управление уязвимостями.
- Обнаружение и реагирование на киберугрозы (SOC).
- Безопасность АСУ ТП.

Мифы и реальность

Мифы	Реальность
Аутсорсинг ИБ только для крупных компаний с большим бюджетом	Аутсорсинг – это гибкое ценообразование и модульные сервисы
Мы потеряем контроль над нашей безопасностью и данными	Вы влияете на политики и услуги Вы принимаете ключевые решения
Это слишком дорого, чем иметь своих специалистов	Предсказуемый OPEX, включающий экспертизу, технологии и RnD против TCO
Мы будем зависеть от внешнего поставщика	Прозрачные условия прекращения сотрудничества

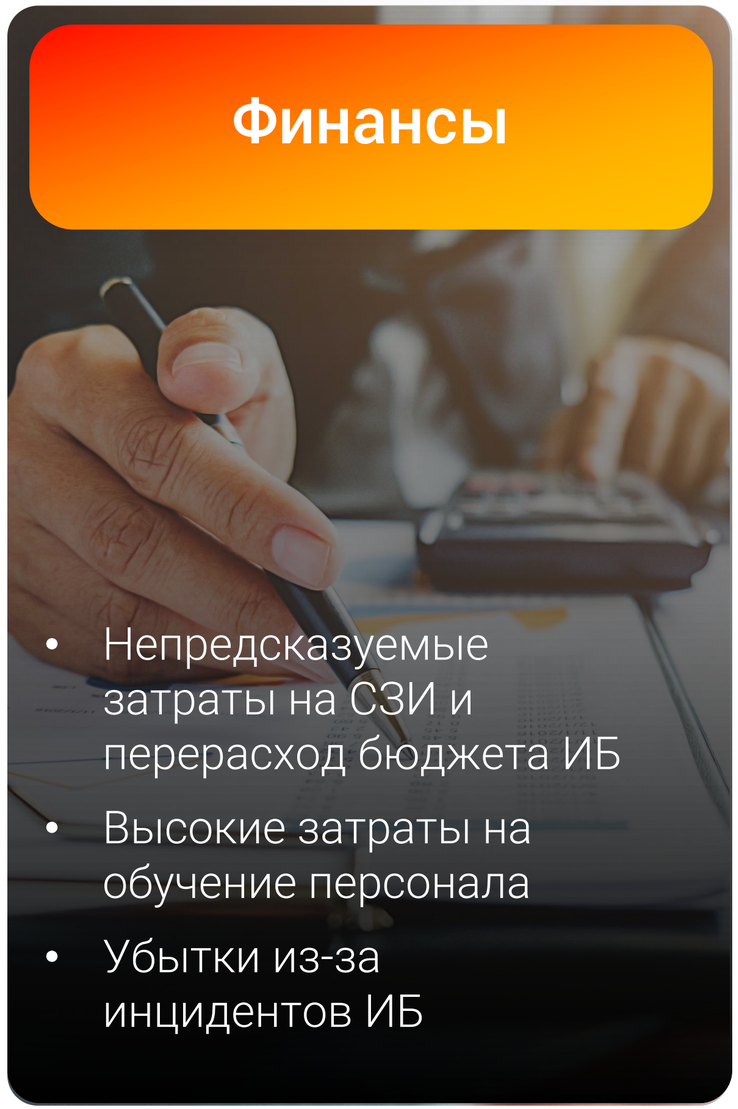
Когда бизнесу нужен аутсорсинг ИБ?

Персонал



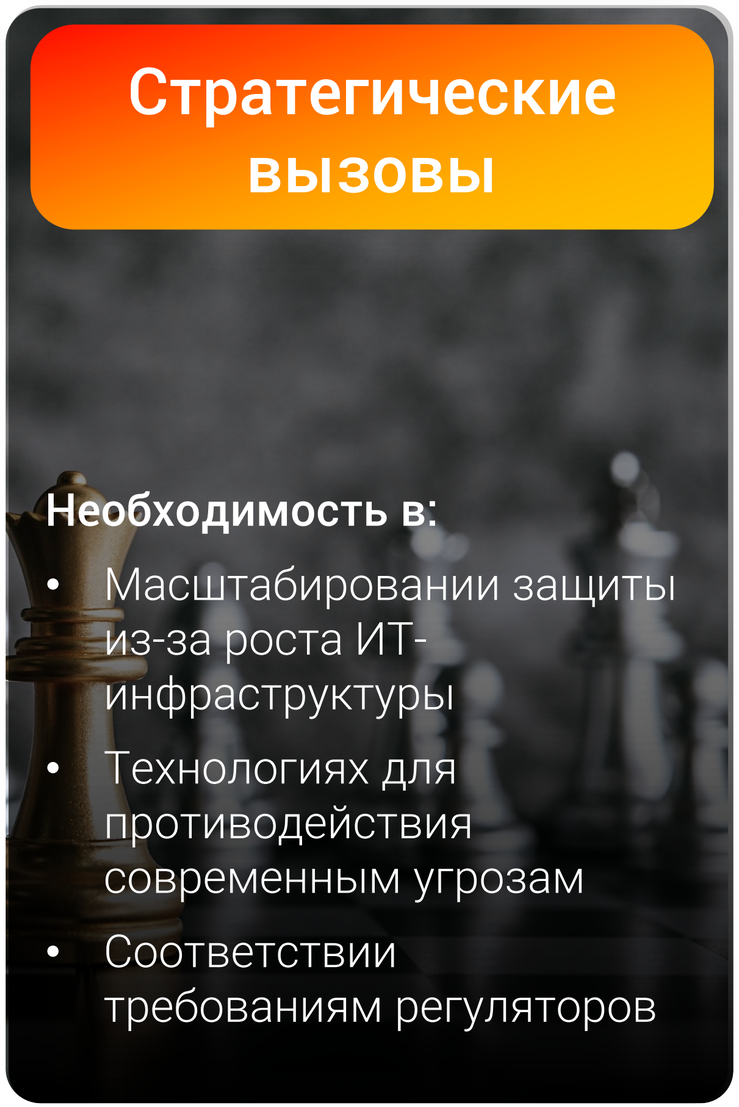
- Дефицит квалифицированных специалистов
- Отдел ИБ «зашился» в рутине и тушит «пожары»
- Текучка кадров ИБ

Финансы



- Непредсказуемые затраты на СЗИ и перерасход бюджета ИБ
- Высокие затраты на обучение персонала
- Убытки из-за инцидентов ИБ

Стратегические вызовы



Необходимость в:

- Масштабировании защиты из-за роста ИТ-инфраструктуры
- Технологиях для противодействия современным угрозам
- Соответствии требованиям регуляторов

Безопасность завтрашнего дня: От проблем к выгодам

Давайте подведем краткие итоги, с помощью Аутсоринг ИБ, Вы:

- получаете доступ к экспертизе и современным технологиям, дополняя вашу команду;
- помогаете ИБ-команде сосредоточиться на стратегических задачах, передав рутину;
- снижаете риск ущерба от инцидентов ИБ без капитальных затрат;
- и переводите их в равномерные операционные расходы с прогнозируемым бюджетом;
- снимаете с бизнеса нагрузку на расширение штата, обучение, сертификацию, RnD;
- можете расширить мониторинг и реагирование на киберугрозы до круглосуточного;
- соответствуете законодательству в области ИБ, которое требует постоянного мониторинга и практики.

Аутсорсинг ИБ — это умная стратегия в условиях дефицита ресурсов

Переход без «головной боли».

ТИПОВЫЕ ОШИБКИ	ПРАКТИЧЕСКИЕ СОВЕТЫ
Выбор провайдера исключительно по цене.	**Разработайте четкие критерии выбора, установите весовые коэффициенты.**
Слабо сформулированные требования к услуге, объёму и SLA.	**Сформулируйте подробное ТЗ сами/с помощью рекомендаций от провайдера. Конкретизируйте состав работ, кол-во, ожидаемый результат, критерии оценки, механизмы измерения качества.**
Отсутствие подготовки всех подразделений компании к переходу на аутсорсинг ИБ.	**Заранее проинформируйте все ключевые подразделения о планах перехода на аутсорсинг. На этапе перехода, разработайте и проведите обучение для них как изменится их взаимодействие.**
Недооценка сложности интеграции и неподготовленность инфраструктуры.	**До перехода подготовьте инфраструктуру и свои процессы для эффективного двустороннего взаимодействия. Совместно с провайдером разработайте детальный план интеграции. Хорошая практика начинать с пилотного проекта.**
Пассивность в работе с поставщиком услуг.	**Регулярно проводите совещания для обсуждения вопросов с провайдером, доводите до него контекст и планируемые значимые изменения, касающиеся или влияющие на услугу, учитывайте его рекомендации .**

Защита по модели «Всё включено»

Это услуга по киберзащите, когда нет необходимости покупать лицензии и ПО, в услугу включено всё что нужно для работы с СЗИ, включая мониторинг и реагирование на инциденты силами экспертов ICL Services.

Что входит:

- современные средства защиты для всех ваших устройств;
- мониторинг и реагирование на инциденты ИБ СЗИ;
- управление поддержкой, администрированием и обслуживанием СЗИ;
- консультации по работе СЗИ, и непрерывное улучшение совместного взаимодействия;
- поддержка покрытия конечных устройств и актуальности сигнатур СЗИ;
- регулярная отчетность о состоянии СЗИ и безопасности.

Какие СЗИ мы предлагаем:

- Kaspersky Endpoint Security для Бизнеса (Стандартный, Расширенный, Total);
- Kaspersky EDR для бизнеса – Оптимальный;
- Kaspersky Security для почтовых серверов;
- Kaspersky Security для интернет-шлюзов;
- Kaspersky Endpoint Detection and Response;
- METASCAN управление ASF.

В планах развития:

- Redcheck – комплексное управление уязвимостями как услуга;
- Security Awareness платформы.

Как это работает:

- Вы обращаетесь к нам
- Мы обсуждаем средство защиты под ваш запрос
- Разворачиваем с «0» или принимаем Ваши СЗИ
- Активируем наши лицензии сервис провайдера
- И приступаем к защите вашей инфраструктуры.

Выгоды:

- Не нужно сразу покупать лицензии на 1,2,3 года
- Вы получаете услугу, а не просто средство защиты
- Гибкое управление количеством защищаемых устройств
- Вы получаете прогнозируемые затраты и прозрачную стоимость ТСО
- Не нужно вкладываться в обучение и расширять штат
- Взаимодействие с вендором мы забираем на себя.

Если вы решите сменить провайдера или самостоятельно работать с СЗИ, не проблема, вся конфигурация СЗИ и настройки инфраструктуры остаются у Вас. Вам просто нужно будет активировать свою лицензию.

Наши услуги:

Внедрение / миграция и сопровождение СЗИ, в т.ч. защита АСУ ТП

Обнаружение и реагирование на киберугрозы (SOC как услуга)

Защита данных и корпоративные риски (аутсорсинг DLP)

Консалтинг, аудиты и комплексное обследование инфраструктуры ИБ

Аудит на соответствие требованиям законодательства (152-ФЗ, 187-ФЗ)

Анализ защищённости и тестирование на проникновение

Управление уязвимостями внутреннего и внешнего периметра

Поставка ПО, оборудования, ПАК

Алексей Морозков

Старший руководитель центра
управления кибербезопасностью

alexey.morozkov@icl-services.com

СПАСИБО
ЗА ВНИМАНИЕ

icl-services.com

8 800 333 98 70

pr@icl-services.com