Директор Отделения
информационной безопасности
Романченко Дмитрий

Аутсорсинг информационной безопасности: взгляд интегратора

Декларируемые ожидания от аутсорсинга ИБ

- Безопасность сервиса
- Соблюдение SLA
- Высокое качество специалистов провайдера
- Комплексное решение проблем
- Соблюдение требований регуляторов

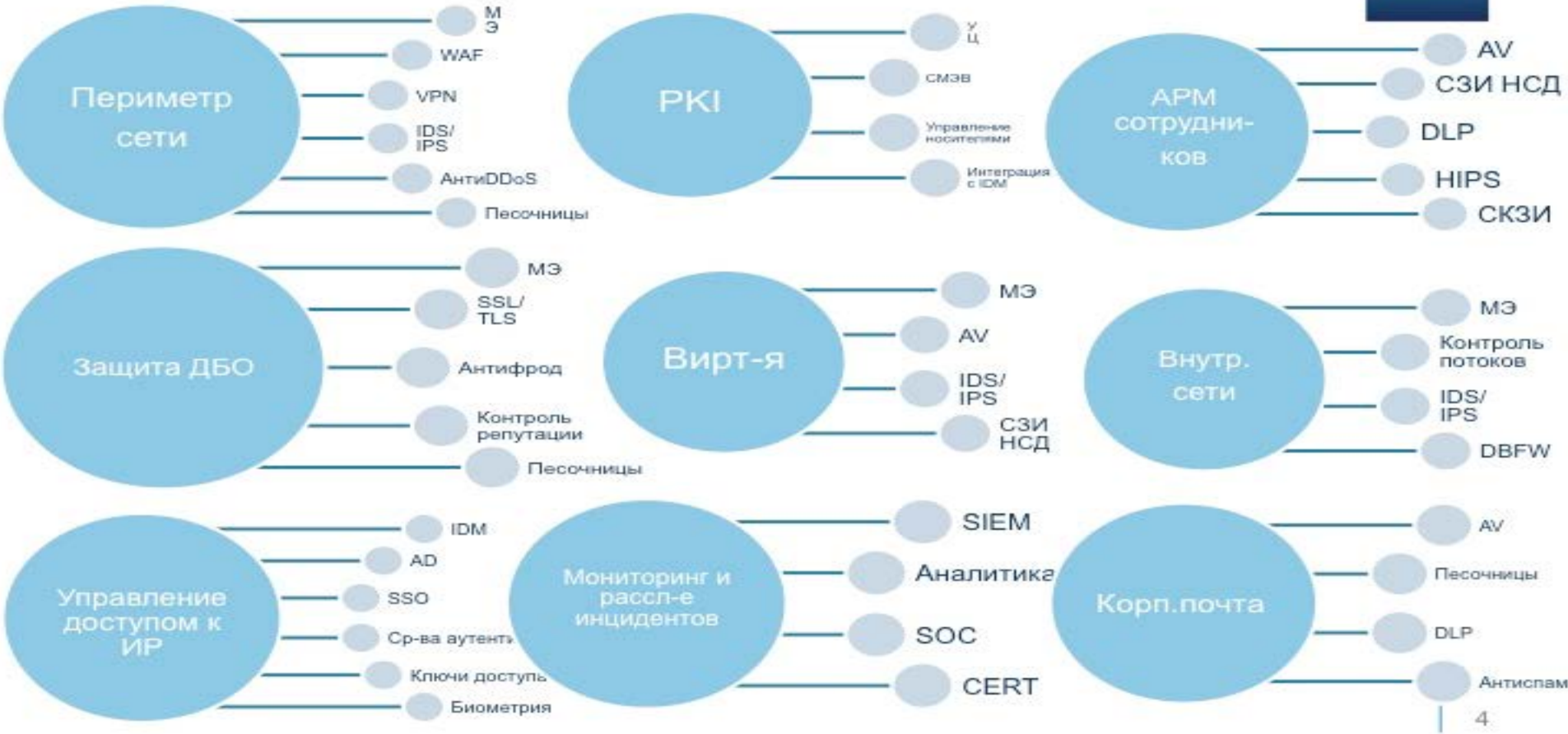
Служба ИБ Компании

- Снижение CAPEX и OPEX
- Возможность штрафа за нарушение SLA
- Возможность смены сервис-провайдера
- Оптимизация штата

Бизнес Компании

Что отдавать на аутсорсинг?

Разнообразие систем ИБ в банке



Новая реальность ИБ

Экспоненциальный рост числа инцидентов ИБ

Рост числа латентных атак

"Растворение" понятия информационного периметра

Активная вовлеченность государств

Массовые кражи информации

Активная "виртуальная" жизнь сотрудников

Информационный терроризм

Неразрывность внутренних и внешних угроз

Неразрывность бизнеса и открытой информационной среды

Широкий спектр воздействий: политика, экономика, обществ. жизнь, финансы

Международный информационный криминальный интернационал

Невозможность классического цикла создания ПО с эффективным тестированием

Криминальный ИБ-бизнес от $270 до $400 млрд в год

Изменение подходов к защите

- Защита периметра
- Формальное соблюдение требований
- Разделение задач создания ИС и их защиты
- Защита от известных угроз
- Работа по сигнатурам
- Классические методы защиты

Вчера

- ✓ Тотальная защита
- ✓ Защита от реальных угроз
- ✓ Безопасная разработка ПО
- ✓ Интегрированная безопасность
- ✓ Безопасный код
- ✓ Защита от неизвестных угроз
- ✓ Оценка поведения
- ✓ Новые методы и средства защиты

Сегодня

?

Завтра

Нормативное регулирование и полезные ссылки

- ISO/IEC 27001:2013 «Information technology. Security techniques. Information security management systems. Requirements»
- РС БР ИББС-2.5-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности»
- РС БР ИББС-2.6-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем»
- РС БР ИББС-2.7-2015 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности»
- Проект РС БР ИББС-2.X-20XX «Обеспечение ИБ организаций банковской системы РФ. Аутсорсинг информационной безопасности»
- NIST SP800-35 «Guide to Information Technology Security Services»
- NIS Directive. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Уровни аутсорсинга ИБ

Риски ИБ

Высокие

Средние

Низкие

Примеры аутсорсинга. Операции

№ п/п	Услуга	Риск ИБ (экспертно)
1	Конфигурирование, сервисное обслуживание средств защиты (МЭ, антивирус, IDS/IPS, СЗИ НСД)	Средний
2	Ведение ролевой модели IDM-системы	Низкий
3	Настройка антиспам-системы	Средний
4	Выпуск сертификатов на удостоверяющем центре электронной подписи	Средний
5	Контроль резервного копирования конфигураций средств защиты	Низкий

Примеры аутсорсинга. Системы

№ п/п	Услуга	Риск ИБ (экспертно)
1	Контроль функционирования систем защиты Заказчика (МЭ, антивирус, IDS/IPS, СЗИ НСД, SIEM, IDM, антифрод и пр.)	Средний / Высокий
2	Предоставление в аутсорсинг систем безопасности (antiDDoS, WAF, SIEM и пр.)	Средний
3	Предоставление систем анализа вредоносного ПО (“песочницы”)	Низкий

Примеры аутсорсинга. Процессы

№ п/п	Услуга	Риск ИБ (экспертно)
1	Обеспечение функционирования цикла безопасной разработки ПО в Компании	Средний
2	Поддержка функционирования процессов управления доступом к информационным ресурсам в Компании	Низкий
3	Мониторинг событий и расследование инцидентов ИБ	Высокий
4	Аудит ИБ в Компании	Средний / Высокий
5	Инструментальный аудит защищенности ИТ-инфраструктуры и информационных систем	Высокий
6	Расследование инцидентов ИБ	Высокий

Примеры аутсорсинга. АС в защищенном исполнении

№ п/п	Услуга	Риск ИБ (экспертно)
1	Обеспечение функционирования корпоративной HR-системы (включая выполнение требований ФЗ-152)	Высокий
2	Обеспечение функционирования CRM-системы (включая выполнение требований по защите информации)	Высокий

Что не рекомендуют отдавать на аутсорсинг

№ п/п	Услуга / задача / процесс
1	Разработка политик ИБ Заказчика
2	Контроль результатов функционирования процессов ИБ
3	Инициация изменений архитектуры СОИБ
4	Утверждение результатов аудита ИБ
5	Разработка SLA по аутсорсингу ИБ

А что на самом деле ценно в ИБ-аутсорсинге для банка?

- Персонал. Специалистов ИБ должного уровня не хватает
- Сложность и длительность запуска новых технологий ИБ в меняющейся палитре угроз
- Сложность обеспечения безопасного жизненного цикла банковского ПО в ситуации постоянных изменений
- Ограниченность собственного опыта Заказчика в противостоянии угрозам ИБ

Международный рынок

Managed Security Service Providers (MSSP)

Gartner не разделяет уровни аутсорсинга ИБ, давая агрегированную оценку по макрорегионам

Имеются оценки, что по результатам 2016 г мировой рынок MSSP превысит $16 млрд.

NIS Directive утверждена Европарламентом 6 июля 2016 г и вступила в силу в августе 2016 г.

- **Предлагается:**
  - Создать в каждой стране-участнике группу реагирования на инциденты CSIRT
  - Вводится обязательное тестирование защищенности в следующих группах компаний:
    - энергетической, транспортной, нефтегазовой, медицинской, финансовой
  - Сформировать реестр аккредитованных компаний для тестирования
  - …

Организация аутсорсинга ИБ в Компании

Ожидаемые проблемы Заказчика при использовании аутсорсинга ИБ

Проблемы ИТ

- Отсутствие у провайдера ИБ-услуг комплексного взгляда на проблемы функционирования защищенных ИТ
- Нестыковка SLA в контрактах ИТ и ИБ сервис-провайдеров
- Усложнение управления изменениями в ИТ при наличии аутсоргинга ИБ
- Влияние качества услуг ИБ-провайдера на KPI команды ИТ

Проблемы ИБ

- Сложность или невозможность контроля специалистов провайдера
- Получение специалистами провайдера доступа в защищенный периметр
- Раскрытие архитектуры систем защиты для внешней компании
- Сложность подтверждения compliance при аутсорсинговой модели ИБ
- Влияние качества сервиса ИБ-провайдера на KPI команды ИБ

Требования к провайдеру услуг аутсорсинга ИБ

Ключевые моменты контракта по аутсорсингу ИБ

1) Полнота описания реестра передаваемых на аутсорсинг операций / систем / процессов ИБ
2) SLA предоставляемых услуг
3) Закрепление квалифицированного персонала провайдера за проектом
4) Обеспечение безопасности обрабатываемой информации, корректное и защищенное сопряжение инфр-ры провайдера и Заказчика. Возможность аудита провайдера в части ИБ
5) Процедуры управления рисками, изменениями и проблемами
6) План реагирования и восстановления в случае непредвиденных ситуаций (DRP)
7) Юридические аспекты, в том числе: распределение ответственности, право привлечения внешних экспертов при разборе инцидентов, право расторжения при систематическом нарушении SLA
8) Соблюдение сервис-провайдером требований регуляторов по защите информации в полном объеме, в том числе требованиям по сертификации оборудования и ПО, аттестации систем (если применимо)

Выводы: препятствия развития аутсорсинга ИБ

- Сложность выделения отдельных сервисов ИБ в развитой КСОИБ Заказчика
- Услуги аутсорсинга ИБ часто маскируются под расширенную поддержку, не имея, однако, при этом всех атрибутов аутсорсингового контракта
- Провайдеры не готовы всегда брать на себя финансовую ответственность в случае инцидентов ИБ
- Страхование рисков ИБ в России не развито
- Массовый ИТ/ИБ инсорсинг крупных Заказчиков, который фрагментирует рынок и не способствует повышению качества сервиса и уровня безопасности

Решение об аутсорсинге ИБ – каждый раз очень индивидуальная история

Выводы: стимулы развития рынка аутсорсинга ИБ

- Инициативы регуляторов:
  - Банк России – FinCERT
  - ФСТЭК – база уязвимостей, выстраивание процессов устранения уязвимостей в сертифицированных СЗИ
  - ФСБ - ГосСОПКА
- Инициативы коммерческих организаций:
  - Лаборатория Касперского – KL ISC CERT для систем АСУ ТП
- Развитие нормативно-методической базы
- Появление страховых продуктов, обеспечивающих адекватное покрытие рисков ИБ
- Формирование профессионального сообщества: стандартизация услуг ИБ-аутсорсинга

Технологическое лидерство

Экспертиза

IBS

Практика эффективных внедрений

Россия, 127434, Москва,
Дмитровское шоссе, 9Б

тел.: +7 (495) 967-8080
факс: +7 (495) 967-8081

ibs@ibs.ru
www.ibs.ru

www.facebook.com/IBS.ru
www.twitter.com/ibs_ru