CNews FORUM 2022

CNews FORUM Кейсы
Опыт ИТ-лидеров

Импортозамещение в ИБ: ошибки и решения

Алия Рахматуллина

Менеджер

Направление кибербезопасности и непрерывности бизнеса
Технологии Доверия (TeDo)
E-mail: aliya.rakhmatullina@tedo.ru
Тел.: +7 (495) 967 6000 доб. 2937

Содержание

1 Вызовы для бизнеса, ИТ и ИБ 4

2 Ошибки при импортозамещении в ИБ 6

3 Подход к управлению импортозамещением в ИБ 9

4 Ключевые моменты 14

Вызовы для бизнеса, ИТ и ИБ

- Уход компаний с российского рынка, приостановка их деятельности на территории РФ
- Существенное усложнение логистических схем
- Расширение санкций
- Рост количества кибератак
- Сложности в кадровом обеспечении
- Замораживание текущих проектов ИТ/ИБ
- Новые требования по ИБ в Указах Президента РФ

Возросли риски нарушения кибербезопасности

- Уход с российского рынка иностранных поставщиков услуг и решений в сфере кибербезопасности, грозящий **существенным сокращением возможностей по обеспечению кибер-защиты**
- Нарушение **непрерывности ведения бизнеса и повседневных операций** в результате целенаправленных атак со стороны киберпреступников и хакерских групп
- Распространение недостоверных новостей и усиление активности по манипулированию информацией, которые могут **негативно** повлиять на **репутацию бренда** и **затруднить привлечение высококвалифицированных кадров**
- Отсутствие технической поддержки зарубежных бизнес-систем, увеличивающее подверженность киберугрозам и вероятность **возникновения сбоев и аварийных ситуаций**

Ошибки при импортозамещении в ИБ (1/5)

Основная ошибка

Отсутствие понимания существенно изменившейся картины рисков ИБ

- Слабое понимание основных угроз и рисков ИБ для организации у заинтересованных лиц и руководства
- Неправильные решения в области замены технологий, перестройки процессов и кадровых изменений

- Определите критичные активы
- Проведите переоценку профиля угроз и рисков ИБ
- Обеспечьте пересмотр контрольной среды ИБ в зависимости от того, как выглядят киберриски и приоритетные угрозы

Ошибки при импортозамещении в ИБ (2/5)

Ошибка 1

Основная задача для бизнеса – замена продуктов по ИБ

- Нет связи ИБ с задачами бизнеса
- Отсутствие реестра критичных активов
- Импульсивная замена средств защиты информации

- Обозначьте цель мероприятий по импортозамещению в ИБ и защитите её перед руководством организации
- Определите критичность замены продуктов по ИБ
- Определите дополнительные компенсационные меры по ИБ

Ошибки при импортозамещении в ИБ (3/5)

Ошибка 2

Отсутствие плана миграции на новые решения ИБ

- Ошибки при выборе и планировании технических решений
- Ошибки при проектировании систем безопасности
- Отсутствие проработки совместимости решений и интеграции с текущей инфраструктурой

- Проводите сравнение и пилотирование систем ИБ
- Сверяйте архитектуру с поставщиком решения
- Определите и разработайте дорожную карту по миграции на новые решения ИБ
- Заложите ресурсы не только на внедрение технологий, но и на создание и поддержку процессов ИБ

Ошибка 3

Open Source – это бесплатно

- Отсутствие бесплатной технической поддержки
- Необходимость доработки продукта под конкретные задачи
- Отсутствие дорожной карты по развитию продукта
- Наличие уязвимостей в программном коде

- Планируйте найм персонала с соответствующими компетенциями
- Учитывайте характер «неопределенности» при использовании open source
- Уделяйте внимание безопасной разработке
- Используйте дополнительные меры ИБ (анализ кода, предварительная загрузка кода в локальный репозиторий, др.)

Ошибки при импортозамещении в ИБ (4/5)

Ошибка 4
Выбор модели сервиса ИБ

- Отсутствие адекватной оценки процессов ИБ в организации
- Отсутствие ресурсов на развитие или внедрение процессов ИБ
- Нехватка квалифицированных специалистов

- Проведите сравнение нескольких моделей работы сервисов ИБ
- Помимо внедрения технических средств, закладывайте ресурсы на развитие или внедрение процессов ИБ
- Учитывайте уровень зрелости функции ИТ (инвентаризация ИТ-активов, каналы связи, др.)

	Внутренний SOC	Внешний SOC (MDR)
Оказываемые сервисы	Узкий спектр сервисов	Широкий спектр сервисов
Персонал	Нехватка квалифицированных специалистов, 8x5	Гибкая численность, 24x7
Уровень ответственности	Низкий (нет внутренних штрафов, слабое влияние на бизнес)	Высокий (SLA с заказчиком, штрафы)
Опыт	Небольшой (малое кол-во реальных инцидентов)	Большой (> кол-во заказчиков, персонала, инцидентов)

Ошибки при импортозамещении в ИБ (5/5)

Ошибка 5

Кадровое обеспечение

- Ошибки при подсчете оптимальной численности персонала
- Смена технических средств по ИБ - драйвер к пересмотру численности персонала службы ИБ
- Влияние репутации бренда организации на привлечение высококвалифицированных кадров

- Заложите время на поиск или обучение персонала
- Планируйте достаточно персонала на поддержку систем и сервисов ИБ
- Учитывайте размер компании, сервисы ИБ и охват мониторинга

Подход к управлению импортозамещением в ИБ

Переоценка профиля угроз и киберрисков

- Оценка последствий от введения санкций и оценка необходимости производить замену ПО
- Выявление пробелов в механизмах детектирования и противодействия вредоносной активности
- Переоценка профиля угроз и киберрисков для организации

Оценка контрольной среды ИБ

- Оценка ранее принятых решений по набору контролей ИБ, их применимости и зрелости в зависимости от того, как выглядят киберриски и приоритетные угрозы
- Актуализация набора метрик по операционной эффективности контрольной среды и профилю риска

Стратегия и дорожная карта

- Разработка стратегии перехода к альтернативным решениям и внедрение доп.мер защиты
- Разработка или корректировка стратегии развития SOC
- Создание дорожной карты с расставленными приоритетами, сроками реализации, перечнем ресурсов, рисками
- Анализ запущенных и планируемых к запуску стратегических ИТ и ИБ-инициатив на предмет релевантности

Выбор и внедрение

- Сравнение и выбор альтернативного набора средств защиты
- Внедрение и интеграция с текущей инфраструктурой
- Кадровое обеспечение

Фаза 1: Оценка

Фаза 2: Реализация

Результаты

- Перечень наблюдений на основе анализа инфраструктуры кибербезопасности
- Профиль угроз и киберрисков

Результаты

- Набор контролей ИБ с учетом киберрисков
- Набор метрик

Результаты

- Дорожная карта поэтапного перехода к альтернативным решениям ИБ
- Определение ключевых инициатив ИБ
- Бюджетная оценка

Результаты

- Внедрение средств защиты
- Обучение, поиск и найм персонала

Ключевые моменты

В текущих условиях, основная задача для бизнеса - провести переоценку профиля угроз и киберрисков, разработать **стратегию импортозамещения в ИБ** и **планомерно** перестроить существующую **систему безопасности** в организации

Импортозамещение- это долгий процесс, поэтому внедрять его стоит поэтапно исходя из актуальных угроз и рисков ИБ

Важно помнить, что ключевым фактором, обеспечивающим устойчивость организации и ее способность восстановить производственные процессы после кибератак является **сохранение полностью укомплектованной, обученной и адекватно финансируемой функции ИБ**

Вопросы?