

SEARCHINFORM

INFORMATION SECURITY

Защита импортозамещенной ИТ-инфраструктуры объектов КИИ



Алексей Парфентьев

Заместитель генерального директора
по инновационной деятельности
«СёрчИнформ»

Специфика ИБ-импортозамещения на объектах КИИ

- ▶ ИБ-импортозамещение активно ведется с 2017 г.
- ▶ Создан пул ИБ-решений для защиты по всем направлениям

> 2000 решений включено в Реестр ФСТЭК

90% доступных СЗИ – российские разработки

Процедура сертификации СЗИ:

- ППРФ № 608 от 26.06.1995
- Приказ ФСТЭК от 03.04.2018 № 55

Несертифицированные СЗИ не могут применяться на объектах КИИ



Специфика ИБ-импортозамещения на объектах КИИ

В 2023-2024 гг.

Определены типовые объекты КИИ в отраслях:



Промышленности



Транспорта



Связи



Здравоохранения

и иных

Указ Президента РФ № 846 от 08.11.2023: новые полномочия ФСТЭК

- Контроль состояния защищенности ОКИИ;
- Оценка эффективности работы организаций в части защиты ОКИИ
- Разработка и внедрение отраслевых мер защиты КИИ

До 01.01.2025:

- Всем субъектам КИИ завершить ИБ-импортозамещение
- Субъектам КИИ в госсекторе – завершить переход на российское ПО

Прикладные проблемы ИБ-импортозамещения

Навыки
пользователей

Поддержка и доработка

Прикладное ПО

Слой совместимости

Системное ПО

Слой совместимости

Оборудование

Стандарты и технологии

Люди

Проблемы, требующие решения

SEARCHINFORM
INFORMATION SECURITY

- 1** **Отсутствие стандартов** по слоям совместимости
- 2** **>15 отечественных ОС,** для которых нужна интеграция
- 3** **Отсутствие на рынке** российской аппаратной базы в нужных объемах
- 4** **Задержки до 6 месяцев** при проверке недекларируемых возможностей



Прикладной аспект обеспечения ИБ

Случай 1

Российское СЗИ не совместимо со всеми российскими ОС

ИЛИ

Российское СЗИ спроектировано под зарубежные ОС

Тиражирование затруднено

Случай 2

ИБ-решение разработано в России, но не включено в Реестр ПО

(не имеет действующего сертификата ФСТЭК)

Применение невозможно

Прикладной аспект обеспечения ИБ

Случай 3

Каждое обновление российских СЗИ требует проверки и сертификации ФСТЭК

Задержки при выпуске обновлений

Случай 4

Функции СЗИ для Windows

≠

Функции СЗИ для Linux

Потери эффективности при миграции

Случай 5

Функции СЗИ для Windows

≠

Функции СЗИ для Linux

Миграция без потерь невозможна

Проблемы интеграции: защита бизнес-процессов

70%

Инцидентов
не обрабатываются
без интеграции СЗИ
и бизнес-систем*

**Замкнутый контур
отсутствует**

в большинстве
бизнес-систем

До 75% бизнес-систем
размещаются в облаках*

**Защищенный периметр
размывается**

**Объединение
и автоматизация**

Процессов для комплексной
миграции СЗИ и прикладного ПО

Поддержка интеграционных решений

SEARCHINFORM
INFORMATION SECURITY

- 1 Поддержка российских ОС
- 2 Поддержка российских СУБД
- 3 Поддержка ПО
в защищенном исполнении
- 4 Поддержка платформенных
решений
- 5 Поддержка PaaS-провайдеров



Спасибо за внимание!



[https://t.me/
searchinform](https://t.me/searchinform)



[https://vk.com/
securityinform](https://vk.com/securityinform)

Практика и аналитика



[https://searchinform.ru/
practice-and-analytics/](https://searchinform.ru/practice-and-analytics/)