PULKOVO
Saint Petersburg Airport

ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ В СЕТЯХ АСУ ТП

Март 2024

ВСТУПЛЕНИЕ

На фоне событий начала 2022 г. многие иностранные ИТ-компании объявили об уходе с российского рынка.

С этого момента направление по импортозамещению технологического стека стало необходимостью, и промедление в этом вопросе недопустимо.
Отечественные разработчики приняли условия игры и включились в разработку решений для защиты объектов критической информационной инфраструктуры.

ПРОБЛЕМЫ НА РЫНКЕ ИБ

- Уход ключевых иностранных игроков с рынка ИБ;
- Появление аналогов российского производства на импортной элементной базе;
- Зрелость продуктов российского производства на недостаточном уровне, по сравнению с импортными аналогами, ушедшими с российского рынка;
- Риски наличия «закладок» в имеющихся продуктах иностранного производства;
- Значительное увеличение стоимости поставляемых продуктов иностранного производства по «параллельному» импорту.

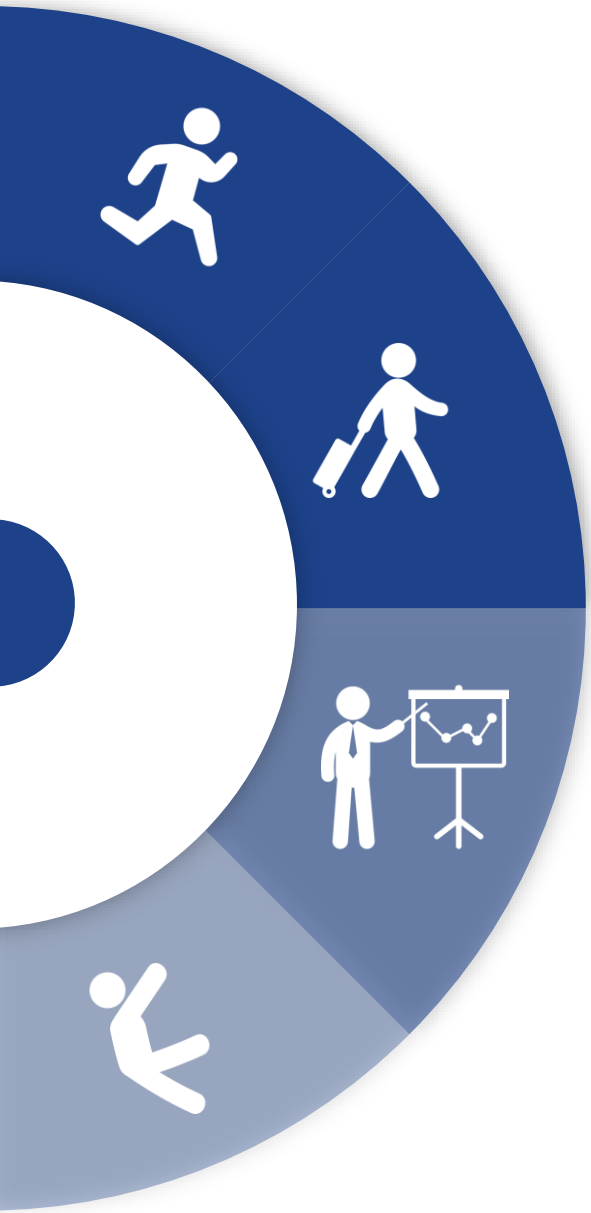
ПОСЛЕДСТВИЯ КУРСА ИМПОРТОЗАМЕЩЕНИЯ

+

- Дан толчок для развития рынка продуктов информационной безопасности, применяемых на объектах КИИ (сертифицированные регуляторами);
- Разрабатываются ОС российского происхождения;
- Разрабатываются базы данных российского происхождения;
- разрабатывается офисное ПО российского происхождения.

—

- Отсутствие конкуренции со стороны иностранных лидеров рынка ИБ приводит к завышению цен порой на «сырые» продукты российского производства.



НЕДОСТАТКИ ИМПОРТОЗАМЕЩЕНИЯ

Необходимость импортозамещения

Уход иностранных компаний-производителей систем ИБ

Потеря конкуренции. Увеличение стоимости

Падение качества разрабатываемых систем ИБ и их поддержка

СОСТОЯНИЕ РОССИЙСКОГО РЫНКА СЗИ

- Рост количества отечественных разработчиков СЗИ;
- Максимально бесшовная интеграция российских СЗИ, ввиду схожести архитектуры с иностранными СЗИ;
- Необходимость в дополнительных работах по настройке и испытанию функций безопасности на новых СЗИ;
- Недоработка интерфейсов на новых СЗИ;
- Необходимость «параллельной» работы новых СЗИ, наряду со старыми для обеспечения безопасности;
- Реализация поэтапного перевода предприятий на новые СЗИ.

ИЗМЕНЕНИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ РФ В ОБЛАСТИ ИБ

Указ Президента РФ от 30.03.2022г. №166 *«О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»*

ИЗМЕНЕНИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ РФ В ОБЛАСТИ ИБ

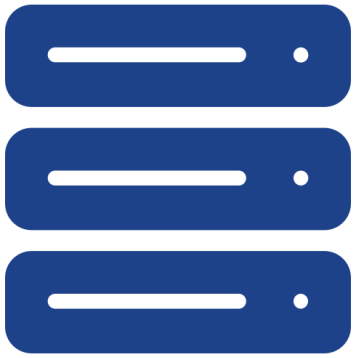
Постановление Правительства РФ от 22.08.2022г. №1478 *«Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с федеральным законом "о закупках товаров, работ, услуг отдельными видами юридических лиц« (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры российской федерации, правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с федеральным законом "о закупках товаров, работ, услуг отдельными видами юридических лиц« (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры российской федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, заказчиками, осуществляющими закупки в соответствии с федеральным законом "о закупках товаров, работ, услуг отдельными видами юридических лиц" (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры российской федерации»*

ИЗМЕНЕНИЕ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ РФ В ОБЛАСТИ ИБ

Постановление Правительства РФ от 14.11.2023г. №1912 *«О порядке перехода субъектов критической информационной инфраструктуры российской федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры российской федерации»*

ЗАЩИТА АСУ ТП

В последнее время участилось количество компьютерных атак



АСУ ТП являются одной из ключевых целей

Нарушение функционирования АСУ ТП может влиять на процессы жизнедеятельности предприятия

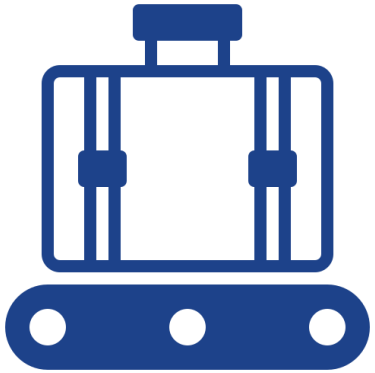
ПРОБЛЕМЫ ПРИ ЗАЩИТЕ АСУ ТП

Не для всех решений, ушедших с рынка, имеются аналоги российского производства

Отсутствие необходимого количества специалистов ИБ, особенно по защите АСУ ТП, имеющих необходимую квалификацию

Законодательством РФ установлены сроки перехода на российские решения СЗИ

ОСНОВНЫЕ СИСТЕМЫ АСУ ТП ТРАНСПОРТНОЙ ОТРАСЛИ



Система сортировки и обработки багажа

Система светосигнального оборудования

Система досмотра багажа

РИСКИ В СИСТЕМАХ АСУ ТП АЭРОПОРТОВ

Уход иностранной технической поддержки установленных систем и оборудования, что привело к возникновению проблем при замене неработоспособного оборудования, конфигурации систем управления;

Требования законодательства РФ в области информационной безопасности требует провести процедуру импортозамещения, что на данный момент невозможно ввиду отсутствия полноценных аналогов и стоимости;

Отсутствие международной сертификации российских систем, что может привести к потере международной сертификации аэропортов, при использовании такого оборудования и систем.

ВАРИАНТЫ РЕШЕНИЯ ПРОБЛЕМ В СИСТЕМАХ АСУ ТП АЭРОПОРТОВ

Локализация иностранных производителей на территории РФ, с получением соответствующих разрешений, лицензий и сертификатов, а также вхождение в реестры российских производителей.

Создание российскими производителями оборудования, полностью аналогично иностранному, с вхождением в реестры российских производителей. Сертификация его по российским стандартам, с возможностью сертификации, в дальнейшем, по международным стандартам.

Создание российскими разработчиками систем управления с функционалом аналогичным иностранным системам. Сертификация их по российским стандартам, с возможностью сертификации, в дальнейшем, по международным стандартам.

ВЫВОД

Санкции повлияли на рынок СЗИ очень серьезно, ввиду неготовности российских производителей одномоментно заменить ушедшие с рынка решения иностранного производства.

Остро ощущается нехватка квалифицированных специалистов, имеющих опыт и компетенции в управлении системами, вышедшими на российский рынок информационной безопасности.

В обозримом будущем направление информационной безопасности является достаточно перспективным и имеет большой запас для развития.

СПАСИБО ЗА ВНИМАНИЕ!

Начальник отдела информационной
безопасности
ООО «Воздушные Ворота Северной Столицы»
Савченко Сергей Юрьевич
S.Savchenko@pulkovo-airport.com