Куда идем или почему Беларуси так необходимо импортозамещение?

Сапрыкин А.М.
директор ООО «С-Терра Бел»,
представитель Оргкомитета международной конференции «Инфофорум»
в Республике Беларусь

«ИКТ Саммит» на ТИБО, 07.06.2024, г. Минск, пр.Победителей,111

Вспомним, с чего начиналось

Маршрутизаторы, МФУ от иностранных производителей уже четверть века поставляются с функциями шифрования: VPN, IPSec. Конечно, с западными криптоалгоритмами и т.н. «экспортного» назначения.

Сомнения были не в стойкости западных к/алгоритмов (тут все ОК), а в «**экспортной**» начинке самих устройств. Было необходимо убедиться в их надежности и безопасности, в том, что информация «не уходит». Иначе, чем через исследования (сертификацию) это проверить нельзя.

И главная проблема была не в возможности встраивания «брендами» наших криптоалгоритмов (их и было тогда всего 4-5), а в том, что они заявляли о невозможности предоставить исходные коды ПО для сертификации, т.к. это «опасно». С ситуацией знаком не понаслышке, поскольку непосредственно вел переговоры с «брендами» по встраиванию бел/криптографии.

Важно: скомпилированное ПО **тысячекратно** труднее взломать (найти уязвимости), чем ПО в исходных кодах.

Развитие

На пути к созданию Национальной системы соответствия СЗИ, включая СКЗИ, было проделано многое:

1. Собственная «школа» криптографии – НИИ ППМИ. Создали свои к/стандарты. Сейчас во взаимосвязанном перечне их более десятка, включая белорусский алгоритм шифрования БЕЛТ.
2. Наполнилась «жизнью» структура Национальной системы соответствия: законодательство, ведомственные нормы, частные методики исследований для криптостандартов и ТНПА, исследовательские лаборатории, системы экспертиз, проектирования защищенных ИС, производства СКЗИ, аттестации и т.п.

И длительное время главным в развитии было понимание того, что «**свое**», пусть и более простое, но это безопаснее и надежнее, чем непроверенное «**чужое**».

Но с 2018 года прежний ориентир на отечественные продукты и изделия сменился на привлечение опенсорсных СКЗИ, которым дана «зеленая» улица без ограничений.

Смена ориентиров развития?

Опенсорсные средства шифрования (ОСШ) – иностранные СШ с западными криптоалгоритмами с открытым кодом, общедоступные для ввоза/скачивания с сайтов США и Европы с открытой лицензией GNU GPL (GPL).

Создать их просто: надо лишь добавить в плагин ОСШ примерно двести строк ПО + библиотеку с белорусскими криптостандартами и ЭТО уже считается белорусским СКЗИ после несложной сертификации (проверять, кроме плагина, нечего, все на доверии).

Начинали ООО «ИТТАС» (itVPN=OpenVPN), ЗАО «НТЦ Контакт» (БАС=StrongSwan), теперь к ним добавились НИИ ТЗИ, ЗАО «Авест» и другие. Различий в уровнях защиты на уровне продукции нет ни у кого. Смысл разрабатывать что-то свое исчезает.

«Помогли» и специалисты НИИ ППМИ – создали «образцовую» криптобиблиотеку Bee2 и разместили ее в исходных кодах в открытом доступе с той же лицензией GNU GPL, то есть специально для опенсорсных СКЗИ. Для целей развития отечественных СКЗИ логичнее было бы предоставлять ее своим разработчикам (платно). А тут бесплатно и для продвижения иностранных ОСШ!

Они же подготовили соответствующую редакцию базового 27-го стандарта тоже с ориентацией на использование ОСШ.

Информация по теме

Важно: 1. В открытых кодах размещать криптобиблиотеку опасно – у нее тоже уязвимости

2. Защищает не библиотека, а продукт в целом (с протоколом). В случае ОСШ протоколы обмена (VPN, IPSec, TLS) проверить невозможно.

3. СКЗИ (ОСШ) относятся к специфическим товарам двойного назначения. Без разрешения спецслужб вывоз ОСШ невозможен. Это тоже «экспортный» вариант, от которого мы пытались «уйти» в начале века.

Мы связывались с правообладателями опенсорсных СКЗИ по поводу возможного сотрудничества. Ответ – невозможно, Беларусь под санкциями, и их СОВЕТ – пользуйтесь ОСШ с GPL лицензией, они разрешены спецслужбами для экспорта во все страны мира и все организации (ИГИЛ, хуситы, Беларусь?). Это точно наш выбор?

На деле ОСШ значительно опаснее изделий от «брендов» (МФУ, маршрутизаторы).

Не только по наличию в них закладок. «Бренд» хотя бы защищает от всех, кроме своих с/с

В случае ОСШ «контролировать» могут все – без уязвимостей на практике их не бывает, у наших «опенсорсников» их десятки(!), а это любимое «блюдо» для хакеров всего мира.

К примеру, в Open SSL с 2023 года насчитали 18 уязвимостей (каждый месяц).

Еще о «достоинствах» опенсорсных СКЗИ

Наука по встраиванию закладок в ОСШ – **клептография** требует **для безопасности** обеспечивать защиту криптосистем на всех уровнях жизненного цикла – от проектирования и разработки ПО до эксплуатации (поддержки), обновления и развития.

1. Как это выполнить при **полной зависимости ОСШ от иностранцев**?

2. Ни один из «производителей» опенсорсных СКЗИ в РБ не сможет обеспечить их жизненный цикл. Только брать готовое. В 27-м стандарте для упрощения добавлен Модуль обновления ПО ОСШ. Закачать закладки можно в любой версии и в любое время.

3. Огромная избыточность (в десятки раз) кодов в ОСШ – для реализации протоколов (VPN, TLS) такого не требуется.

4. Невозможность удалить из ОСШ западную криптографию, без нее продукты не работают

5. Можно отметить фейк западного ЦИПСО о м/н экспертах, которые якобы сделали ОСШ за много лет безопасными продуктами. Мы проанализировали – почти 100% разработчиков берут коды ОСШ из оригинальных источников, «ответвления» не развиваются.

Почему необходимо импортозамещение

Все страны Евросоюза (мы пробовали вывозить в Польшу, Австрию, Голландию – для транзитных проектов) запрещают ввоз белорусских шлюзов (и Россия тоже). В последние 10 лет РФ также перешла на «экспортные» варианты при вывозе СКЗИ.

Смысл – в защите своих коммуникаций и возможности съёма/воздействия на информационные системы (коммуникации) в других странах.

В Беларуси активно развиваются технологии э/государства, цифрового общества и в случае использования опасного фундамента (ОСШ) впереди нас ожидают серьезные проблемы.

Тот, кто поставляет ОСШ (правообладатели), получают возможность:

- доступа к информации, циркулирующей в защищенных ИС
- блокировки защищённых ИС
- организации инсайдерских сливов информации
- имитации «успешных» хакерских атак и т.п.

Как бы в таких условиях Центры кибербезопасности не боролись с инцидентами, реальные причины и исполнители могут остаться неизвестными.

Россия также не согласится с тем, что важнейшие коммуникации стратегического союзника окажутся под западным контролем и уже предпринимает соответствующие меры.

Вариант импортозамещения в сфере СКЗИ

Компоненты СКЗИ: Протокол обмена информацией (VPN, IPSec, TLS) + Криптобиблиотека = Программное СКЗИ

В ПАК добавляется еще Операционная система -ОС (универсальная среда) + АП («железо»).

1. Криптобиблиотеки у нас создали несколько компаний .

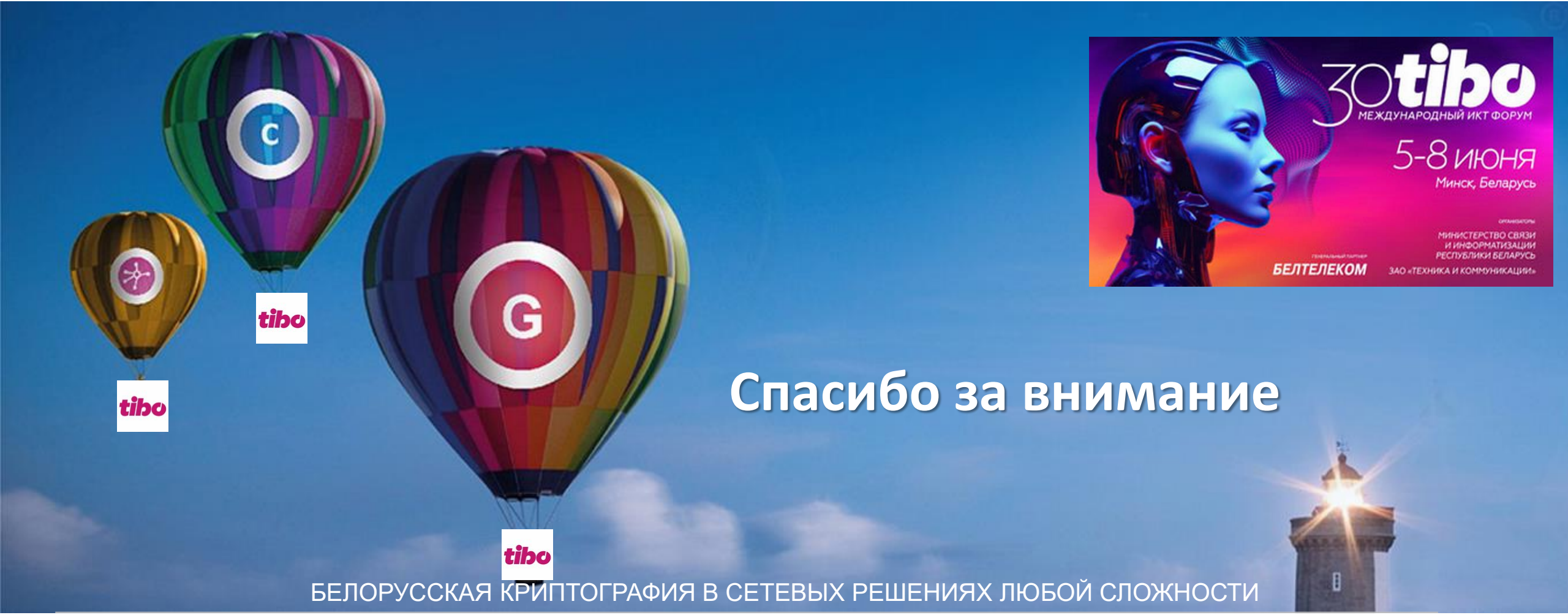
2. Протоколы, возможно, лишь две-три (главная проблема!). Еще две-три могли бы (примерно два года). Сейчас все на одном уровне защиты, а объёмы разработок колоссально различаются, поэтому и берут бесплатные ОСШ. Это «убивает» рынок.

3. Важно обеспечить контроль регулятора за разработками Протоколов, это несложно.

4. Следующий этап - ОС (среда), ее разработчики СКЗИ полноценно реализовать не смогут, максимум, сжатые спец. сборки. И это уже задача государства (регулятора), она решаема несколькими способами. Как и выработка регламента по отношению к АП «железу».

5. Жизненный цикл СКЗИ должен обеспечиваться белорусскими гражданами, а не иностранными спецслужбами.

6. И начинать надо с разделения на «своих» и «чужих» (уровни защиты) - кибервойны в этом не отличаются от обычных. Разница от обычных в том, что кибервойны с нами уже навсегда.



Спасибо за внимание

БЕЛОРУССКАЯ КРИПТОГРАФИЯ В СЕТЕВЫХ РЕШЕНИЯХ ЛЮБОЙ СЛОЖНОСТИ

220004, г. Минск, ул. Клары Цеткин, 51 пом.5

+375 (17) 260 60 00

info@s-terra.by, www.s-terra.by

s•terra