Конференция об актуальных технологических трендах и решениях

A1 Tech Day 2023

Риски использования опенсорсных средств шифрования

Александр Сапрыкин

- *директор ООО «С-Терра Бел»,*
- *представитель Оргкомитета международной конференции «Инфофорум» в Республике Беларусь*

Отель Пекин, Минск, 29.11.2023

s•terra A1

Введение. Опенсорсные средства шифрования

Опенсорсные средства шифрования (ОСШ) – иностранные средства шифрования с западными криптоалгоритмами с открытым кодом, общедоступные для ввоза/скачивания с интернет-сайтов с открытой лицензией GNU GPL (GPL)

Иностранное опенсорсное средство шифрования с западными К/Б

(до 1 млн. строк исходного кода в сети Интернет)

98-99%

(StrongSwan, Open VPN и др.)

Белорусская К/Б

1-2%

Сертифицированное средство шифрования

100%

(БАС, itVPN и др.)

s•terra A1

Введение. Опенсорсные средства шифрования

Наиболее распространены в Беларуси: itVPN (OpenVPN, США) пр-ва ООО «ИТТАС», БАС (StrongSwan, Швейцария) пр-ва ЗАО «НТЦ Контакт»

Важно: 1. Условия GPL (п.4) запрещают копировать, изменять, сублицензировать или распространять программу иначе, чем на условиях, описанных в GPL (свободное распространение)

2. Белорусская криптобиблиотека не защищает, защищает продукт в целом

3. Средства шифрования (СКЗИ) относятся к специфическим товарам двойного (военного) назначения

4. Законодательно в развитых странах мира создание, ввоз и вывоз СКЗИ входит в компетенцию спецслужб

⇒ *это не обычное опенсорсное ПО!*

Проблема № 1. Нелегитимный ввоз

Ввезенные и используемые на территории Беларуси иностранные опенсорсные средства шифрования не проходили обязательную процедуру идентификации и получения разрешения на ввоз

Тем самым, недобросовестные производители нарушают:

- законодательство Республики Беларусь в сфере экспортного контроля (Закон «Об экспортном контроле» от 11.05.2016 г. № 363-З, Указ Президента Республики Беларусь «О государственном регулировании в области экспортного контроля» от 28.02.2017 г. № 49 и целый ряд ведомственных нормативных актов)
- Положение о ввозе на Таможенную территорию Евразийского экономического союза шифровальных (криптографических) средств (решение Коллегии ЕЭК от 13.12.2017 г. № 17)

Проблема № 1. Нелегитимный ввоз

К примеру, Bel VPN продукты проходили подобную процедуру идентификации при вывозе согласно законодательству по экспортному контролю (при ввозе процедура идентична), отнесены к специфическим товарам, требующим разрешений

Разрешение на ввоз и вывоз средств шифрования дает межведомственная комиссия при Госсекретариате Совета Безопасности Республики Беларусь

Это делается для определения целей и задач, а также сфер применения СКЗИ

Справочно 1: БАС (StronSwan) и itVPN (OpenVPN) имеют такие же уровни защиты, как и Bel VPN (предназначены для тех же классов ИС)

Справочно 2: Национальные европейские регуляторы (из 5 стран!) не разрешили ввоз белорусских шлюзов на территорию своих стран

⇒ как мы относимся к ним, и как они к нам?

Проблема № 2. Контрафакт

Согласно GPL (п.10) производная программа, созданная с использованием оригинальной программы с GPL, может распространяться на условиях отличных от GPL только с разрешения автора

Мы обращались к некоторым правообладателям опенсорсных СКЗИ (strongSwan, OpenVPN)

Они подтвердили невозможность коммерческого распространения любых продуктов, содержащих их программы

Общепринятая в мире бизнес-схема использования ОСШ заключается не в продажах, а в оказании платных услуг по технической поддержке продуктов

При этом: не нарушаются права, обеспечивается сравнительно безопасная эксплуатация ОСШ, ну, и появляется возможность легитимного заработка

Проблема № 2. Контрафакт

А что у нас? Недобросовестные производители опенсорсных СКЗИ:

- нарушают Закон Республики Беларусь № 262–З от 17.05.2011 «Об авторском праве и смежных правах» (ст. 44), ГК Республики Беларусь (ст. 985). Такие продукты являются контрафактными
- не обладают исключительными правами и не имеют прав на коммерческое распространение своих продуктов
- нарушают авторские права правообладателей, что в условиях полной зависимости жизненного цикла СКЗИ от иностранных разработчиков (правообладателей) влечет непредсказуемые риски потребителям
- на свободно распространяемые (бесплатные) продукты расходуются бюджетные средства

⇒ *надо ли изобретать «велосипед» с такими проблемами?*

Проблема № 3. Закладки

ОСШ предназначены всем, в том числе экстремистам и террористам, что предполагает полный контроль разработчика (спецслужб) над жизненным циклом СКЗИ

Как считают белорусские ученые, *«секрет разработчика» (закладку) невозможно получить путем анализа криптосистемы. А в случае обнаружения закладки или канала утечки невозможно доказать умышленность ее создания.*

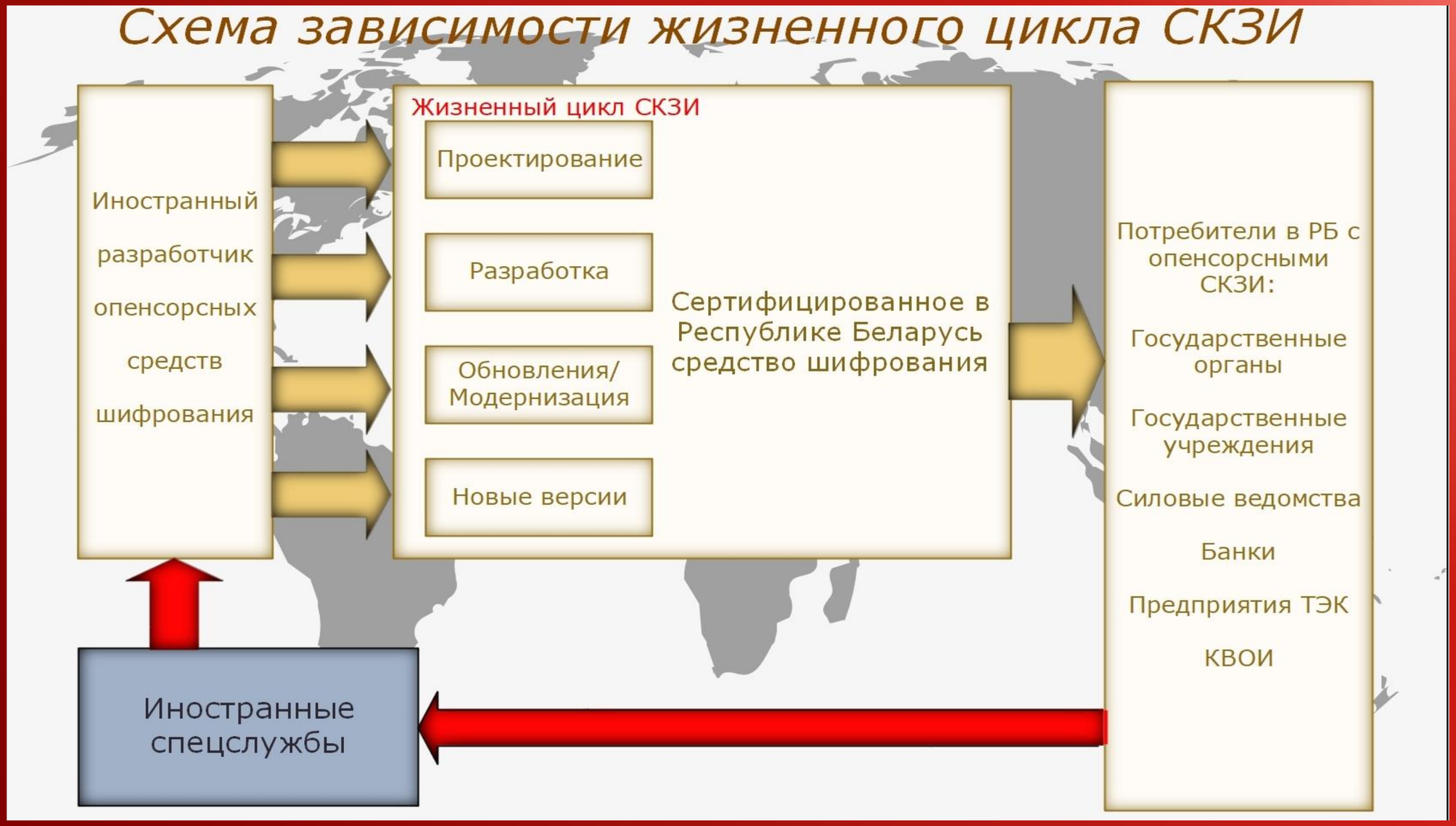
По их мнению, *«особую остроту приобретают вопросы защиты самих криптосистем на всех уровнях их жизненного цикла: этапах проектирования, разработки, развертывания и использования*

(см.стр.106-113 материалы МНК «Теоретическая и прикладная криптография», г. Минск, 2020 год)

Ни один из т.н. «производителей» опенсорсных СКЗИ в Беларуси не может обеспечить их жизненный цикл. Только брать готовые ОСШ от иностранного разработчика и добавлять по инструкции от него же белорусскую К/Б

Проблема № 3. Закладки

A1 Tech Day 2023



⇒Закладки могут быть встроены в любое время и в любой версии опенсорсного СКЗИ!

Проблема № 4. Уязвимости

Опенсорсные СКЗИ с исходными кодами в открытом доступе влекут особые риски с точки зрения нахождения уязвимостей:

- их могут находить все желающие, в том числе хакеры и киберпреступники
- не все уязвимости публикуются
- до появления патчей на опубликованные уязвимости могут пройти недели и месяцы
- требуется жесткое время реагирования после опубликования уязвимостей, что никто из белорусских «производителей» не делает

В Беларуси еще не было опенсорсных СКЗИ без уязвимостей – почти за пятилетнюю историю их предложений на рынке

Для примера, БАС 1 имел более 100 уязвимостей, itVPN в настоящее время – более 50-ти. Обновления не проводятся годами

⇒ общемировая бизнес-схема применения ОСШ уменьшает эту проблему!

Проблема № 5. Некомпетентность

Поскольку весь жизненный цикл опенсорсных СКЗИ обеспечивается иностранными разработчиками, то высока вероятность столкнуться с некомпетентностью персонала «производителей» СКЗИ на базе ОСШ, в частности, связанной с:

- низкой компетенцией в контрафактно заимствованном программном коде ОСШ;
- непониманием технологических аспектов ОСШ;
- не оптимальной сборкой продуктов;
- «зависанием» при решении задач по технической поддержке опенсорсных средств шифрования.

⇒ *только свои разработчики смогут обеспечить полноценное развитие отечественных (белорусских) средств криптографической защиты информации в рамках Национальной системы соответствия*

Итоги

Сертифицированные опенсорсные СКЗИ не гарантируют:

- легитимности ввоза продуктов согласно законодательству РБ и актам ЕАЭС
- наличия у производителей исключительных (авторских прав) на продукты
- независимости жизненного цикла от иностранных производителей
- отсутствия закладок и уязвимостей
- поставок свободно распространяемых продуктов за бюджетные средства

Беларусь становится уникальной страной (из имеющих свою криптографию) по степени доверия опенсорсным СКЗИ. Им преимущества и преференции, «зеленая улица» без ограничений по классам ИС, включая уровень ДСП. При том, что создавать свои продукты несоизмеримо сложнее.

К примеру, случаи блокировок ОСШ в России не доставили ей ощутимых проблем, поскольку сфера их применения незначительна

⇒ *выбор в пользу использования иностранных ОСШ «убивает» на рынке свое, закладывает проблемы для безопасности цифровой экономики Беларуси*

Bel VPN продукты - лучшие на рынке Беларуси!

Bel VPN продукты – СКЗИ с закрытым (проприетарным) кодом, разрабатываемые с 2008 года и совершенствуемые ООО «С-Терра Бел». Выпущено 4-ре полнофункциональные версии продуктов, эксплуатируется несколько десятков тысяч единиц продукции. Весь жизненный цикл Bel VPN продуктов обеспечивается исключительно белорусскими гражданами

ПАК «Шлюз безопасности Bel VPN Gate 4.5»

ПК «Шлюз безопасности виртуальный Bel VPN Gate-P 4.5»

ПП «Система централизованного управления Bel VPN KP 4.5»

ПП «Клиент безопасности Bel VPN Client 4.5» (ОС Windows)

ПАУ «Клиент ДСП 4.5» (под любые ОС)

ПП «Клиент мобильный Bel VPN Client-M 4.5» (ОС Android)

ПП «Модуль линейного шифрования Bel VPN L2 4.5»

s•terra A1

Спасибо

Александр Сапрыкин

директор ООО «С-Терра Бел»

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

+375 (17) 260 60 00

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