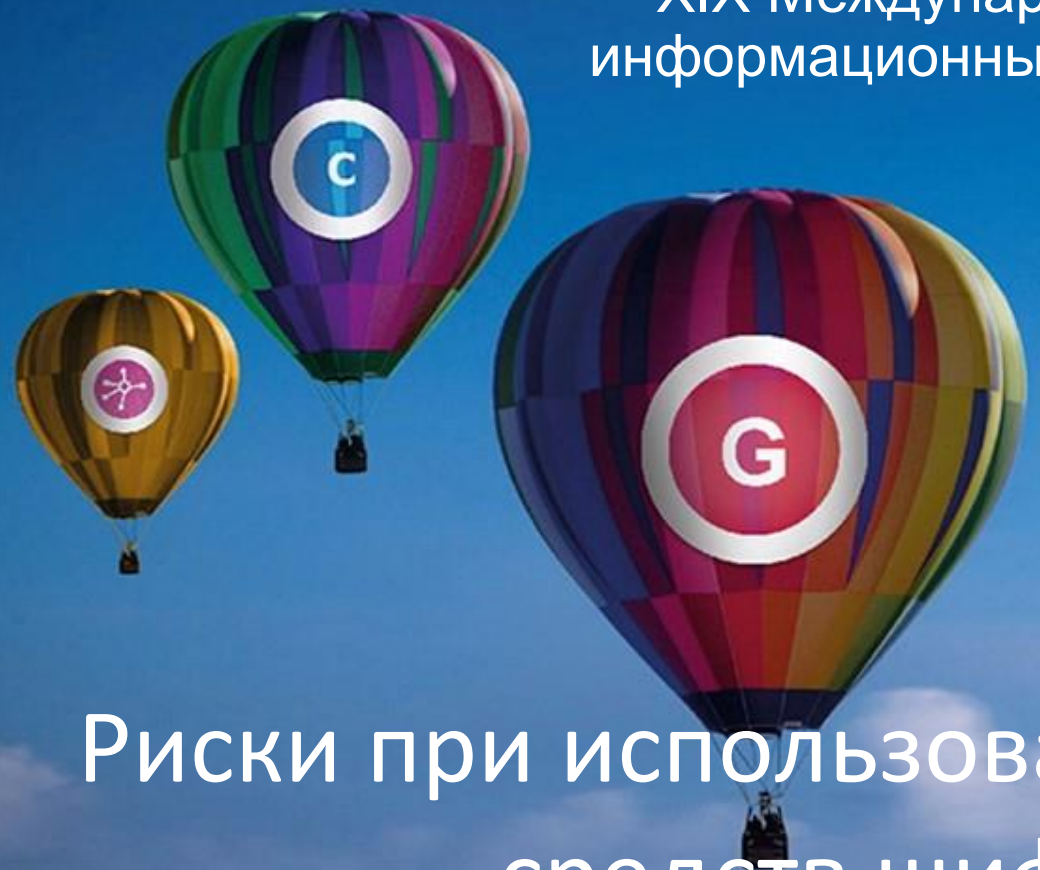
XIX Международный форум по банковским информационным технологиям «БанкИТ-2023»



БАНКИТ´23

БАНКОВСКИЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Риски при использовании опенсорсных средств шифрования

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

02.11.2023, Президент-Отель, Минск

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.)

Наиболее распространённые в Беларуси: itVPN (OpenVPN, США) пр-ва ООО «ИТТАС», БАС (StrongSwan, Швейцария) пр-ва ЗАО 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 отнесено к компетенции спецслужб

Проблема № 1. Нелигитимный ввоз

Ввезенные и используемые на территории Республики Беларусь иностранные опенсорсные средства шифрования не проходили обязательную процедуру идентификации и получения разрешений на ввоз. Тем самым, недобросовестные производители осуществляют нелигитимный ввоз, в частности, ими нарушаются:

- законодательство Республики Беларусь в сфере экспортного контроля (Закон «Об экспортном контроле» от 11.05.2016 г. № 363-З, Указ «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).

К примеру, Bel VPN продукты проходили подобную процедуру идентификации (при вывозе процедура идентична), отнесены к специфическим товарам, требующим разрешений.

Разрешение на ввоз и вывоз СКЗИ дает межведомственная комиссия при Госсекретариате Совета Безопасности Республики Беларусь.

Справочно 1: БАС (stronSwan) и itVPN (OpenVPN) имеют одинаковые уровни защиты – используются в тех же классах информационных систем, что и Bel VPN, а закон для всех одинаков.
Справочно 2: Национальные европейские регуляторы 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 письменно подтвердили невозможность коммерческого распространения любых продуктов, содержащих их программы.

Таким образом, недобросовестные производители СКЗИ на основе ОСШ:

- 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 согласно закону 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 ОСШ от иностранных разработчиков (правообладателей) создает непредсказуемые риски потребителям.

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

⇒ Бюджетные средства расходуются на свободно распространяемые (бесплатные) продукты!

Проблема № 3. Закладки

Проблема № 3. Закладки

Вопросами разработки и встраивания закладок в СКЗИ занимается наука – «клептография».

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

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 РБ не может обеспечить жизненный цикл СКЗИ – в том числе, они не в состоянии ни проектировать, ни разрабатывать, ни развивать Open VPN, StrongSwan и другие. Только брать готовые средства шифрования от иностранного разработчика и добавлять по инструкции от него же белорусскую криптобиблиотеку.

⟹ Закладки могут быть встроены в любое время и в любой версии опенсорного 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.

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

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

Все предлагаемые в н/вр опенсорсные СКЗИ – с уязвимостями, в том числе самого высокого – 10-го уровня.

⇒ *«лайфхак» для Центров кибербезопасности при расследовании инцидентов: если в защищенной ИС используются ОСШ, то причину инцидента можно считать выявленной!*

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 их:

- низкой компетенцией в контрафактно заимствованном программном коде ОСШ;
- непониманием технологий создания ОСШ;
- вероятностью не оптимальной сборки продуктов;
- возможностью «зависания» 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 нормативным актам ЕАЭС
- наличия у производителей исключительных (авторских прав) на поставляемые продукты
- независимости жизненного цикла от иностранных производителей
- отсутствия закладок и уязвимостей
- поставки свободно распространяемых (бесплатных) продуктов осуществляются за бюджетные деньги

СКЗИ на базе ОСШ можно рекомендовать тем, кто не интересен ни западным спецслужбам, ни оппозиции, ни хакерам, а за собственные деньги может покупать и бесплатные продукты.

Беларусь становится уникальной страной (из имеющих свою криптографию) по степени доверия опенсорсным СКЗИ. Им приоритеты и преференции во всем, а также «**зеленая улица**» без ограничений по категориям защищаемых информационных систем, включая уровень ДСП. При том, что создавать свои продукты несоизмеримо сложнее, чем брать всем доступный «бесплатный сыр» из недружественных стран.

СКЗИ на базе ОСШ используются в государственных органах и учреждениях, включая силовые структуры; финансово-кредитных учреждениях, включая государственные банки; предприятиях топливно-энергетического комплекса; объектах КВОИ.

⇒ Западу можно доверить защиту силовых структур, в/ч, банков и объектов КВОИ? А оппозиция может требовать блокирования ИС госорганов и неугодных им организаций и учреждений?

Мы точно сделали выводы из 2020 года?

Bel VPN продукты – лучшие на рынке!

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

ПАК «Шлюз безопасности Bel VPN Gate 4.5»

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

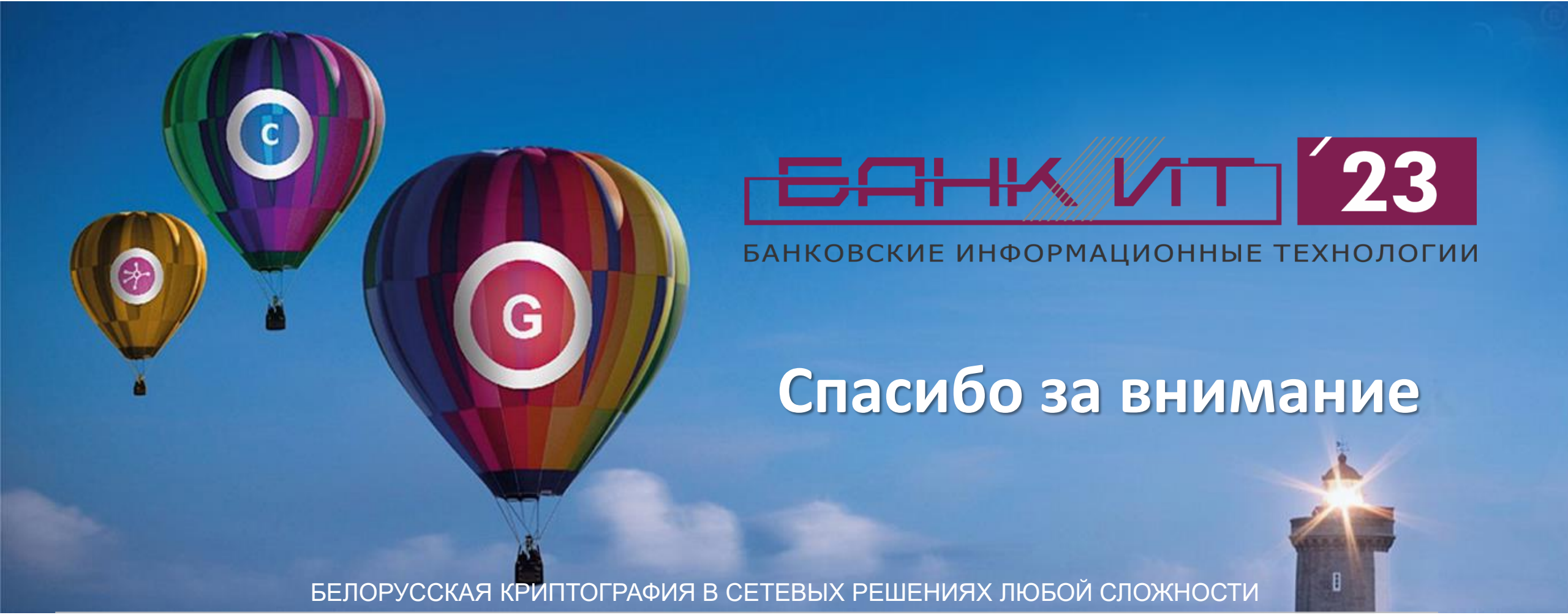
ПП «Система централизованного управления Bel VPN KP 4.5»

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»



220004, г. Минск, ул. Клары Цеткин, 51 пом.5
+375 (17) 260 60 00
info@s-terra.by, www.s-terra.by

s•terra