ЭКСПОРТОНАСЫЩЕНИЕ ВМЕСТО ИМПОРТОЗАМЕЩЕНИЯ ИЛИ ДОВЕРЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВМЕСТО (АНТИ)РОССИЙСКОГО

Здирук Константин Борисович,

кандидат технических наук,

директор по технологиям – главный конструктор

ООО "Экстремальные технологии и системы" (г.Москва), zkb_64@mail.ru

Аннотация

Статья содержит анализ недостатков принятой в настоящее время классификации программного обеспечения (ПО), основанной на распространенной трактовке *правообладания / выгодоприобретения*, как ключевых признаках – основаниях формирования позитивного отношения к так называемому "отечественному" программному продукту. Не всегда обоснованными утверждениями о том, что "отечественный" продукт является *доверенным и/или защищенным*, обычно подменяют уход от обсуждения других принципиальных вопросов - о соотношении *качества* (совокупности функциональных и эксплуатационных характеристик) отечественных и зарубежных образцов ПО, о гарантиях сопровождения жизненного цикла, технологических рисках комплексирования с оборудованием (в большинстве – зарубежного производства) и др. Ошибочная методология классификации на практике дезориентирует как разработчиков ПО - проектировщиков прикладных систем, так и конечных пользователей – потребителей программной продукции.

Предлагается иной подход к классификации, предполагающий выделение четырех классов – *абсолютно доверенного, доверенного, условно доверенного и недоверенного* ПО. Формулируются критерии принадлежности программного изделия к каждому классу. Обосновывается необходимость наличия специальных функций *эскроу-агентов* (Escrow Agent) в модели гарантированного хранения доверенного ПО, его совершенствования и применения на интервале жизненного цикла. Рассмотрена примерная номенклатура и модель функционирования специализированного банка "*лучших" образцов* доверенного программного обеспечения и информационных технологий, обладающих *экстремальными* характеристиками (Банк Ex'IT).

Ключевые слова: *доверенное программное обеспечение (ДПО), эскроу-агенты ДПО, банк Ex'IT.*

1. Обоснование методических подходов к процессу создания конкурентоспособной программной продукции

1.1. “Экспортонасыщение” VS “Импортозамещение”

Задача обеспечения устойчиво-опережающего развития российских сегментов производства конкурентоспособной высокотехнологичной продукции (далее - ВТП) остается актуальной на протяжении, по крайней мере, нескольких последних десятилетий (в расширенной ретроспективе - столетий).

В таком случае ее следовало бы формулировать, как некоторую *цель*, достижение которой возможно при решении ряда сопутствующих *задач*, одной из которых является *импортозамещение*, которое может рассматриваться и как *процесс*-задача, и как *свойство* процесса производства продукции, соответствующей или превосходящей зарубежные аналоги[1].

Само по себе *импортозамещение* не является обособленной конечной целью, так как ее достижение не связано с конкурентоспособностью ВТП, которая объективно измеряется экспортируемой долей в общем объеме ВТП (при условии полного насыщения внутреннего рынка) – назовем этот процесс *экспортонасыщением*, а соответствующий показатель - *экспортонасыщенностью*. Отметим, что *экспортонасыщение,* т.е. производство экспорто-ориентированной, конкурентоспособной ВТП, гарантирует (в перспективе) достижение состояния *импортозамещенности*. При этом, обратное утверждение, в общем случае, - неверно.

Ложные представления о сущности и свойствах упомянутых выше процессов, как будет показано далее на примере одного из сегментов ВТП -

---

[1] Далее термином *“импортозамещение”* будем обозначать процесс, а *“импортозамещенностью”* – (качественное) свойство производства ВТП, имеющее определенную количественную *меру* - *показатель* соотношения заимствуемых (импортируемых) компонентов и компонентов собственного производства

программного обеспечения, являются источником ошибок не только целеполагания, но и реализации политики достижения реальной технологической независимости в стратегически значимых направлениях развития РФ. Ниже мы рассмотрим одно их таких направлений – информационные технологии (IT), в состав которых входят программные продукты и разработанные на их основе программно-технические решения различного функционального назначения.

1.2. Экстремальные IT

Если рассмотреть множество IT, составляющих некоторую конечную (прикладную) систему, можно отметить, что ее IT-элементы существенно различны по вкладу в "*качество*" - с прагматичной точки зрения определяемое как степень пригодности системы для целевого применения (по предназначению).

Известные подходы к классификации IT основываются, как правило, либо на выделении ролевых признаков ПО (общее / общесистемное / специальное программное обеспечение), либо на учете функциональных особенностей и способов применения различных IT-подмножеств в составе образцов ВТП (системы управления, геоинформационные системы, системы искусственного интеллекта и др.)[2].

Рассмотрим еще один возможный аспект классификации, основанный на выделении т.н. *экстремальных* IT (далее по тексту - *Ex'IT*), обеспечивающих *гарантированное* достижение *экстремума* (*Max / Min*) частных показателей "*качества*" существенно значимых свойств - характеристик конечной системы.

---

[2] Отметим, что во всех случаях речь идет о различных основаниях (аспектах) классификации одного и того же множества IT, состав и свойства элементов которого могут изменяться во времени.

Такие системные свойства - характеристики (System Characteristics), достигаемые посредством применения *Ex'IT*, будем называть *экстремальными* (далее по тексту - *Ex'SC*).

В общем случае, элементы множеств *Ex'IT* и *Ex'SC* находятся в отношении «многие-к-многим» (***M:N***), поскольку одна технология может обеспечивать экстремум показателей "*качества*" нескольких существенных системных свойств-характеристик *Ex'SC*, и наоборот, каждое такое свойство может достигаться применением одного и более элементов *Ex'IT* .

В качестве примера укажем некоторые элементы из множества *Ex'SC*, значимые в процессе создания перспективных образцов ВТП (таблица 1).

Таблица 1. Значимые экстремальные свойства образцов ВТП

Идентификатор	**Наименование**	**Содержание**
Ex'SC₁	*Доверенность / абсолютная доверенность программного кода*	100% - авторизация кода (с независимым подтверждением), наличие комплекта документации (конструкторской, программной и эксплуатационной), контроль жизненного цикла внешней уполномоченной организацией (*эскроу-агентом*), передача *эскроу-агенту* на ответственное хранение (с возможностью отчуждения в оговоренных случаях) полного комплекта документации на образец ВТП (*объективизированных "знаний"* об изделии). Подробно данные вопросы рассмотрены в разделе 2
Ex'SC₂	*Интероперабельность по отношению к*	Стабильность системной архитектуры, декларированных

	различным аппаратным / программно-аппаратным платформам	программных интерфейсов (сервисов) при масштабировании в гетерогенной (неоднородной) вычислительной среде
Ex'SC₃	*Неразрушаемость хранилищ накопленных данных ("вечное" хранение)*	Гарантии обеспечения логической и физической целостности (баз) данных с исключением потери данных вследствие деструктивного воздействия комплекса объективных и/или субъективных факторов
Ex'SC₄	*Гарантированность сервисов доставки и обработки данных*	Однократная отправка данных («отправил-забыл»), исключение потери или искажения данных в процессе передачи, выполнение всех декларированных сценариев – процессов обработки данных на приемной стороне с автоматическим уведомлением отправителя о факте их успешного завершения
Ex'SC₅	*Нейтрализация угроз со стороны "недоверенного" программного кода и привилегированного внутреннего нарушителя (инсайдера)*	Гарантированная (на уровне архитектуры) изоляция критически важных данных, а также процессов обработки от деструктивного воздействия со стороны программных «закладок», вирусов, а также третьих лиц (инсайдеров) – "информационных террористов", привилегированных категорий пользователей (системных администраторов, администраторов

		безопасности) Объективная регистрация вредоносной активности с автоматической обработкой возникающих инцидентов в изолированной области, недоступной для компрометации
Ex'SC₆	*Непрерывность функционирования*	Выполнение всех регламентных операций по обслуживанию (в том числе - восстановлению и модернизации) системы в режиме «online». При условии реализации свойств *Ex'SC₂*, *Ex'SC₃* и *Ex'SC₄* , предполагается выполнение требований кратного «горячего» резервирования (кластеризации) вычислительных ресурсов, и *логически* (виртуально) неограниченной емкости хранилищ данных в режиме оперативного доступа
Ex'SC₇	*Гарантии качества проектирования и эксплуатации в течение жизненного цикла*	Применение количественной меры для оценки текущего уровня и потенциала развития (остаточного ресурса) системы и ее элементов, достижение *гарантируемых* (не ниже заданных) значений показателей эффективности целенаправленных процессов контроля состояния и управления системой с применением технологии «цифровых двойников»[2,3,4]. Принятие решений и перевод системы из текущего состояния в предпочтительное

		на основе достоверной информации с применением доверенных средств (*Ex'SC*$_1$), исключающих возможность их компрометации на уровне системной архитектуры [5].

Подробный анализ способов реализации множества *Ex'SC* в составе ВТП (за исключением *Ex'SC*$_1$) выходит за рамки данной работы. Для наглядности на рисунке 1.1 приведем только общую схему сопоставления реализации существенных экстремальных свойств для различных образцов ВТП.

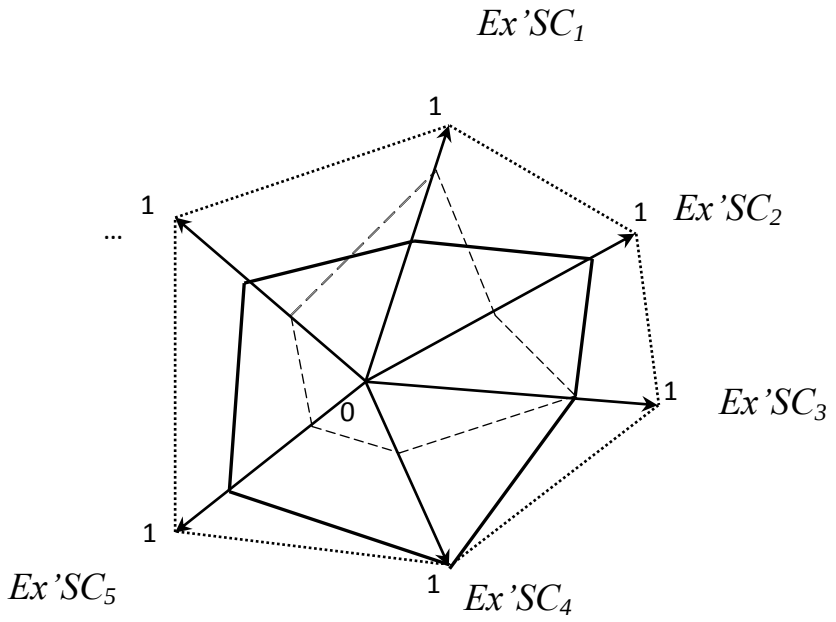

Рис.1.1. Схема сопоставления реализации экстремальных свойств для сравниваемых образцов ВТП

Каждый луч-вектор представляет отдельное свойство-измерение [1] *Ex'SC*$_i$ с нормированной количественной мерой в интервале [0 , 1], длина вектора определяется относительной *значимостью* экстремального свойства *Ex'SC*$_i$ на множестве *Ex'SC* , конечная точка каждого измерения

соответствует достигнутому на текущий момент (предельному) значению $Ex'SC_i$. Площадь внешнего многоугольника (ограничена линиями-точками) соответствует "идеальной" реализации образца ВТП, обладающего превосходными (предельными) показателями всех существенных свойств *Ex'SC*, определяющих его *качество*. Два других внутренних многоугольника представляют образцы ВТП, сопоставляемые по некоторому (заданному) критерию предпочтения, например – площади: образец, ограниченный сплошным контуром - *пригоден*, ограниченный пунктиром - *непригоден*.

Владение *коллекцией* экстремальных IT (как постоянно пополняемого и совершенствуемого систематизированного множества *Ex'IT*) обеспечивает возможность создания конкурентоспособных образцов ВТП, обладающих экстремальными свойствами, - необходимого условия *экспортонасыщения* (см. п.1.1) и одновременно - избавляет от необходимости поддерживать паритет на всем множестве современных IT в условиях объективно неизбежного технологического отставания (зависимости) от лидеров в других направлениях IT.

Далее мы остановимся на методологических аспектах создания и применения *(абсолютно) доверенных защищенных средств*, как выделенного *общесистемного* слоя программного обеспечения, встраиваемого в состав существующих и перспективных образцов ВТП.

2. Методологические основы разработки и применения доверенного программного обеспечения

2.1 Основное противоречие процесса создания ВТП.

При создании ВТП, как правило, возникает противоречие, с одной стороны - между требованиями по конкурентоспособности (необходимость применения *оригинальных*[3] разработок и решений для достижения превосходства над имеющимися аналогами), а с другой – включением *заимствованных* (*общедоступных*[4]*) компонентов* в состав разрабатываемого изделия для *гарантированного* получения на выходе приемлемых характеристик и, в целом, минимизации рисков разработки ВТП.

Если в отношении *оригинальных* компонентов можно сформулировать и, на практике, обеспечить выполнение требований *по доверенности и защищенности* вновь разрабатываемого кода (программного обеспечения – далее ПО), то, к сожалению, в большинстве случаев, применяемые *общедоступные компоненты* ПО не являются *ни доверенными*, *ни защищенными* в рамках определений, содержащихся в работе [5].

> *Примечание–1:* В составе ВТП совместно функционируют как заимствуемые (общедоступные), так и оригинальные (вновь разработанные) компоненты, функциональное соотношение между которыми может изменяться в процессе жизненного цикла изделия.
>
> *Примечание-2:* В условиях конфликтной ситуации с поставщиком *общедоступных компонентов* возникает проблема *гарантированного* вскрытия и нейтрализации возможных (скрытых) вредоносных воздействий со стороны заимствуемых компонентов ПО.

На основании применяемого теоретико-множественного подхода, будем далее полагать, что *защищенное* ПО является подмножеством *доверенного* (в общем случае, эти множества не совпадают). Как следствие – программные комплексы средств защиты, обеспечивающие

---

[3] *Оригинальные* (программные) компоненты и решения рассматриваются как *исключительный (exclusive)* ресурс, разрабатываемый в ходе реализации проекта по созданию ВТП.

[4] *Заимствованные* (программные) компоненты и решения рассматриваются как *общедоступный (share)* ресурс, используемый на (различных) условиях лицензирования.

информационную и функциональную безопасность конечной системы – образца ВТП, могут включать только *доверенные* компоненты (п.2.3).

2.2 Анализ сложившейся терминологии (*“отечественное”-“доверенное” – “защищенное”* ПО)

Для обоснования предлагаемых далее методических подходов к классификации ПО (по уровням доверия), следует уточнить используемые в обиходе IT-специалистами термины, неоднозначность толкования которых зачастую приводит к ошибкам в оценке *качества* (интегральной характеристики набора показателей эксплуатационных свойств) создаваемой системы.

Ниже (в п.2.3) мы рассмотрим интенсионал и экстенсионал понятий “доверенное / “защищенное” ПО, а здесь покажем несостоятельность применения терминов “отечественное” / “зарубежное” ПО и их производных (“российское”, “китайское”, “украинское” и проч.) при выборе и обосновании конструкторских решений в части номенклатуры применяемых в составе ВТП компонентов программного обеспечения.

С точки зрения актуальных угроз информационной безопасности представляется необоснованным использование терминов «российское / отечественное программное обеспечение» в трактовке правообладания (более 50%) субъектом – резидентом РФ, поскольку при таком подходе игнорируется важнейший аспект *доверия* к самому продукту – личная ответственность *автора – разработчика* ПО.

Следует отметить, что сам по себе термин “российское ПО”, как и его отрицание, - “зарубежное ПО” (в формальной логике – *антироссийское*) является анахронизмом в контексте современных моделей организации разработки программных средств.

В настоящее время сложившаяся практика разработки, в частности, может включать нижеперечисленные организационные схемы (варианты):

- долевое софинансирование общего проекта юридическими (или физическими) лицами – резидентами и нерезидентами Российской Федерации;

- разработчик программного обеспечения – резидент Российской Федерации, правообладатель (в т.ч. долевой) программного обеспечения – нерезидент (или наоборот);

- программное обеспечение является (условно) свободно распространяемым, при этом действительное авторство и/или правообладание не могут быть достоверно установлены;

- разработчик и/или правообладатель не установлены, программный код полностью или частично заимствуется (присваивается) из анонимного источника компанией или физическим лицом – резидентом / нерезидентом для использования в своих интересах.

Правообладание программным продуктом, с точки зрения международного права, является объектом рыночных отношений («купли-продажи»), поэтому распространенной практикой является возмездная уступка прав (полностью или частично) на программный продукт с непредсказуемой мотивацией поведения нового правообладателя. В этих условиях говорить всерьез об использовании “временно российского” / “временно зарубежного” ПО не представляется возможным.

Приведенные примеры наглядно демонстрируют несостоятельность подхода к классификации российского и зарубежного программного обеспечения, основанного на трактовке (долевого) правообладания ПО резидентами или нерезидентами Российской Федерации[5].

[5] Еще одним несостоятельным критерием “российскости” программного продукта, является наличие преимущественного выгодоприобретателя (бенефициара) – резидента РФ. Во-первых, выгодоприобретение проистекает из факта правообладания, поэтому не является первичным критерием, а во-вторых, любой из правообладателей (резидент/нерезидент) может “отказаться” от лицензионного вознаграждения, преследуя

Составление так называемого “Единого реестра российских программ для электронных вычислительных машин и баз данных” (Минкомсвязь России) – не менее сомнительная затея, поскольку критерии включения в реестр не предусматривают наличия в составе продукта ТОЛЬКО *оригинальных авторизованных* компонентов, разработанных резидентами РФ, как одного из необходимых условий доверия к программному коду.

Вместо этого допускается (как утверждают - *временное*) применение в составе т.н. “российских” программ - неавторизованного (условно) свободно распространяемого программного кода, как правило *иностранного происхождения*[6]. Появление в реестре номенклатурных единиц ВТП, перелицованных и состоящих на 90 и более процентов из *заимствованных* (см. сноски 3,4) компонентов, - свидетельство утраты как технологической независимости РФ в ключевых сегментах ПО (ОС, СУБД, платформы middleware), так и определенных нравственных ориентиров со стороны участников этого процесса.

С точки зрения безопасности ПО еще одной порожденной проблемой является представление *посредником* (правообладателем, не автором-разработчиком) на сертификацию заимствованных из внешних источников исходных кодов программного продукта. При отсутствии контроля за процессом их создания и анонимности реальных разработчиков невозможно гарантировать проактивное обнаружение и нейтрализацию программных закладок. Результаты тестирования ПО, предъявляемого на сертификацию по требованиям отсутствия недекларируемых / соответствия реальных и декларируемых возможностей, в большинстве своем носят вероятностный

собственные, недекларируемые цели. Аналогичные соображения касаются всего т.н. (условно)свободно распространяемого кода, применяемого в т.н. «отечественном/российском» ПО

[6] См. Решение Экспертного совета по программному обеспечению при Минкомсвязи России № 467 пр. 12.11.2018г. «О поэтапном отказе от использования программного обеспечения, базирующегося на программных продуктах иностранного происхождения в части СУБД, серверов приложений и платформ”

характер (прошедшим проверку считается код, процент сомнительных участков которого не превышает установленного предела). Объективно существующие риски ошибок I-II рода, а также возможности создания самомодифицирующихся в процессе исполнения программ – в совокупности делают практически бессмысленным процесс анализа исходных текстов без привлечения (реальных) авторов-разработчиков программного кода, предъявляемого на сертификационные испытания.

Таким образом, существуют достаточные основания утверждать, что не все т.н. "*отечественное"* ПО является *доверенным*, и уж тем более – *защищенным*.

Попытки обосновать предоставление законодательных преференций т.н. "отечественному производителю" тезисом о том, что отечественный продукт является, по определению, *доверенным / защищенным*, обычно затушевывают обсуждение других принципиальных вопросов - о соотношении *качества* (набора функциональных и эксплуатационных свойств) отечественных и зарубежных образцов, о гарантиях сопровождения жизненного цикла, технологических рисках комплексирования с оборудованием (в большинстве - зарубежного производства) и др.

В целом, стратегию наложения искусственных ограничений на импортируемое ПО можно считать неэффективной, ей можно и нужно противопоставить альтернативу – стимулирование экспортно-ориентированного производства *доверенных защищенных* компонентов ПО (по-настоящему *отечественной* разработки), а также решений по их комплексированию в составе ВТП с *недоверенными* средствами – технологическими лидерами в своих сегментах глобального рынка ПО.

Рассматриваемый в данной статье альтернативный подход базируется на выделении в составе ВТП *доверенного* общесистемного слоя ПО, включении в него средств *гарантированной изоляции* критических данных и

процессов от возможного вредоносного воздействия *недоверенных* компонентов и их последующего эволюционного замещения *доверенными*.

Этот механизм, как представляется, обеспечивает возможность практической реализации процессов *импортозамещения* в сегментах критической информационной инфраструктуры, а в остальных – разработку (на общих основаниях) конкурентоспособных компонентов ПО, функционирующих в составе (лучших) образцов ВТП.

2.3 Классификация программного обеспечения по критериям доверия

Вместо терминов “программное обеспечение зарубежного и российского производства” предлагается использовать термины *недоверенное* и *доверенное* программное обеспечение, обобщив приведенные в работе [5] критерии доверия с учетом различных вариантов (п.2.2) организации разработки программного обеспечения в современных условиях (специализации / глобализации / транспарентности).

Определения:

Абсолютно доверенное программное обеспечение (А-ДПО), функционирующее в среде некоторой абстрактной аппаратно-программной платформы (АПП) предполагает совместное выполнение следующих условий – так называемых “обобщенных критериев доверия” (далее ОКД $D_{[4]}$):

d_1 - подтвержденную (независимым органом) авторизацию программного кода и 100% (в совокупности) декларированное правообладание им юридическими и/или физическими лицами;

d_2 - наличие полного состава авторизованной проектной документации и ее представление (правообладателем);

d_3 - сопровождение всех этапов жизненного цикла продукта (проектирование, разработка, сертификация, эксплуатация, модернизация/замена) внешним независимым уполномоченным органом;

d_4 - передача *эскроу-агенту* (*Escrow Agent*) на ответственное хранение (с возможностью отчуждения в оговоренных случаях) исходных и исполняемых программных кодов и проектной документации в полном объеме[7].

Доверенное программное *обеспечение* (ДПО) предполагает совместное выполнение условий $< d_1 , d_2 , d_3 >$.

Условно доверенное программное обеспечение (УПО) предполагает невыполнение хотя бы одного из условий определения ДПО.

Недоверенным программным обеспечением (НПО) считается программное средство, в отношении которого не выполняются все 3 условия ДПО.

Как представляется, изложенный выше подход к классификации ПО на основе ОКД $D_{[4]}$ является *универсальным*, т.е. не имеющим государственно-обусловленных границ применения. Иными словами, как некоторая *логическая формула*, ОКД $D_{[4]}$ может быть *общезначимой* (т.е. *истинной*) на всех возможных интерпретациях, под которыми понимаются специфические условия законодательно-правовой системы отдельных государств.

С учетом сложившихся в нашей стране специфических правовых отношений в сфере производства и внедрения программной продукции (лицензирование, сертификация, регистрация и пр.) общее определение

[7] Количественная оценка “полноты”, и как следствие – “стоимости”, может быть произведена на основе работ [3,4], содержащих описание методических подходов к оцениванию результатов объективизации “знаний” о предмете (продукте) по его цифровому двойнику

А-ДПО в ОКД $D_{[4]}$ применительно к РФ (А-ДПО$_{(РФ)}$) может быть сформулировано следующим образом:

d_1 - регистрация ПО уполномоченным государственным органом с проверкой и подтверждением авторизации кода (авторы – физические лица-резиденты РФ), 100% правообладание программным кодом резидентами РФ (юридическими и/или физическими лицами);

d_2 - представление (при регистрации, далее – в течение жизненного цикла) полного состава проектной (конструкторской и программной) документации в соответствии с ГОСТ ЕСКД / ЕСПД;

d_3 - сопровождение всех этапов жизненного цикла продукта (проектирование, разработка, сертификация, эксплуатация, модернизация/замена) уполномоченным государственным органом (ФСТЭК РФ, МО РФ, ФСБ РФ);

d_4 - передача уполномоченной организации – резиденту РФ на ответственное хранение (с условием возмездного отчуждения в оговоренных случаях в пользу государства) всей проектной документации (в т.ч. исходных и исполняемых) кодов в полном объеме с обязательством владельца по ее актуализации в течение всего жизненного цикла программного продукта.

В условиях действия определения А-ДПО$_{(РФ)}$, соответствующие определения ДПО$_{(РФ)}$, УПО$_{(РФ)}$ и НПО$_{(РФ)}$ остаются без изменений.

Примечание–3: Отнесение программного обеспечения к какому-либо классу (ДПО, УПО или НПО) не влияет на другие функциональные свойства продукта, определяющие его *качество*.

Совместное функционирование А-ДПО / ДПО / УПО / НПО на некоторой платформе[8] (средстве вычислительной техники) требует гарантированной защиты и нейтрализации угроз информационной безопасности со стороны *недоверенных* компонентов (УПО / НПО). Поэтому множество *Ex'IT* должно включать элементы-технологии, обеспечивающие выполнение условия (свойства) экстремальности $Ex'SC_5$, в соответствии с приведенной в п.1.2 таблицей 1.

[8] Приведенная классификация, а также рассмотренные в работах [5,6] подходы к реализации безопасного функционирования ПО относятся к уровням (кольцам) защиты гипервизора безопасности (Ring -1), ядра базовой ОС (Ring 0), драйверов (Ring 1/2) и приложений (Ring 3). Уровни System Management Mode (Ring -2) и Active Management Technology (Ring -3) в настоящее время не могут рассматриваться, как защищенная среда исполнения, поскольку состав ПО этих уровней полностью определяется производителем оборудования

3. Роль и функций эскроу-агентов в создании ВТП на основе доверенного программного обеспечения

Различие в определениях п.2.3 *абсолютно доверенного* и *доверенного* ПО (А-ДПО и ДПО соответственно) состоит в передаче независимому гаранту (посреднику) - *эскроу-агенту* на ответственное хранение (с возможностью отчуждения в оговоренных случаях) исходных и исполняемых программных кодов и проектной документации на авторизованный *продукт*, созданный *разработчиком*, принадлежащий *владельцу* и эксплуатируемый *потребителем*[9]. Продукт содержит *оригинальные* (см. сноску 3) программные компоненты и технические решения, обладающие экстремальными характеристиками и придающие конкурентоспособность созданному на их основе образцу ВТП.

В отличие от *заимствуемых* в составе образца ВТП компонентов (см. сноску 4), являющихся *общедоступным (share)* ресурсом, утрата или ограничение по какой-либо причине возможности применения *оригинальных доверенных* компонентов и технических решений могут иметь критические последствия для *потребителя* (в т.ч. возможно - *заказчика* ВТП).

> *Примечание–4:* Известны случаи, когда потребитель - государство (в лице органа государственной власти), затрачивая значительные средства на создание/приобретение доверенного ПО, оказывается не в состоянии контролировать его жизненный цикл в силу отказа или объективной невозможности со стороны владельца/разработчика поддерживать оригинальные компоненты. Их программные реализации и применяемые технические решения, в ряде случаев - безвозвратно утрачиваются (существенно ограничиваются в применении), а вновь создаваемые аналоги или уступают прототипу, или разделяют его судьбу.

Таким образом, *владелец / разработчик* оригинальных доверенных компонентов является ключевым элементом цепочки жизненного цикла образца ВТП, чьи функции не подстрахованы, поэтому сам *потребитель / заказчик* в рамках принятой на сегодня модели взаимоотношений становится

---

[9] *Владелец* программного продукта может одновременно являться и его *разработчиком*. *Потребитель* продукта также может выступать и как его *владелец*.

заложником объективных обстоятельств и/или субъективных взаимоотношений с *владельцем / разработчиком*. В ряде случаев, в интересах «спасения» проекта и личной репутации *потребитель / заказчик* вынужден отказаться от ранее заявленных существенных свойств – *экстремальных* характеристик образца ВТП.

В целом, описанные выше явления, с точки зрения проблематики работ [2,3,4], можно охарактеризовать как утрату определенного количества “знаний” (компетенций), объективизированных на теоретическом и практическом уровнях в виде комплекта документации и навыков (опыта) эксплуатации ВТП.

Наличие *эскроу-агента*, принявшего на себя риски ответственного хранения оригинальных доверенных компонентов и технических решений, отчуждения (в оговоренных случаях) и последующего гарантированного сопровождения жизненного цикла ДПО исключает утрату “знаний” (достигнутого уровня компетенций), обеспечивает условия воспроизводства и улучшения показателей *экстремальных* свойств-характеристик, а также контролирует рациональное применение доверенных компонентов и решений (посредством Банка Ex’IT, раздел 4).

Эскроу-агент , для реализации вышеописанных функций, должен обладать средствами объективизации совокупности *критических* “знаний” в *информацию* о продукте, количественной оценки степени ее (не)полноты и представления в виде коллекции «цифровых двойников» - т.н. *информационных контейнеров знаний* (свойство $Ex'SC_7$, таблица 1, п.1.2). Учитывая исключительную ответственность *эскроу-агента*, как посредника – хранителя критически важной информации, он должен также обеспечивать собственными средствами реализацию свойств $Ex'SC_3$ и $Ex'SC_5$.

Возмещение собственных затрат на текущую деятельность *эскроу-агента* производится на основании договорных отношений (как гаранта-посредника) с *владельцем / разработчиком* и *потребителем / заказчиком.*

В некоторых оговоренных договорными отношениями случаях (например, при мотивированном отказе *владельца* от сопровождения и развития ДПО, применяемого на объектах критической инфраструктуры) в качестве компенсации затрат на техническую поддержку продукта в течение жизненного цикла к *эскроу-агенту* от *владельца* могут передаваться частично/полностью соответствующие права и обязанности.

Еще одним важным источником обеспечения деятельности *эскроу-агента* является определение номенклатуры и организация специализированного банка т.н. *экстремальных* (“лучших” по функциональным характеристикам) информационных технологий и конструкторских решений (Банк Ex’IT). Как показано на рисунке 4.1, банк содержит набор доверенных программных компонентов, обладающих экстремальными свойствами-характеристиками *Ex’SC* (таблица 1, п.1.2), необходимыми для создания конечных (прикладных) систем с гарантированным *качеством*.

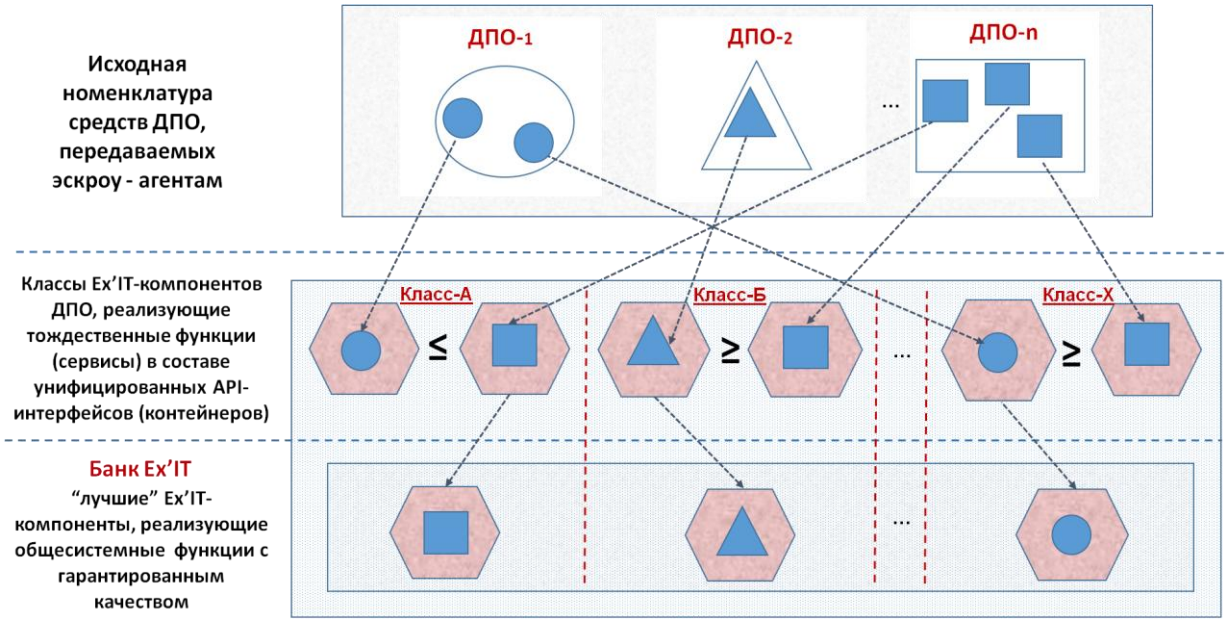

Рис.4.1. Отбор компонентов ДПО и формирование номенклатуры Банка Ex’IT

Эскроу-агент (с согласия *владельца/разработчика* ДПО) может публиковать или распространять по подписке номенклатуру Банка Ex'IT и предоставлять *потребителям* лицензии на использование унифицированных Ex'IT-компонентов с описанием внешних (API) интерфейсов подключения к предоставляемым сервисам (без раскрытия конструкторских решений, содержащихся в передаваемых компонентах). Проектная документация владельца/разработчика (алгоритмы, исходные коды программных модулей и описание технических решений "know-how"), представленная в специальном формате – коллекции «цифровых двойников» находится на ответственном хранении у *эскроу-агента* и не подлежит разглашению или передаче третьим лицам. Как отмечалось выше, документация может быть использована в форс-мажорных обстоятельствах, например, при необходимости срочной доработки или устранения выявленных в процессе эксплуатации критических ошибок в случае отказа *владельца/разработчика* ДПО от его дальнейшего сопровождения.

Основным движущим элементом функционирования Банка Ex'IT является предоставление конечным *потребителям* (заказчикам, разработчикам, пользователям прикладных систем) гарантий достижения декларируемых *экстремальных* свойств-характеристик образцов ВТП с соблюдением имущественных прав *владельцев* ДПО, принимающих на себя основные риски по созданию Ex'IT.

Немаловажным является попутно достигаемый положительный результат функционирования Банка Ex'IT - исключение утраты накопленных и документированных "знаний" (программных реализаций, решений "know-how", алгоритмов, навыков эксплуатации и т.д.). В случае отказа от дальнейшего развития какой-либо технологии ее *владельцем/разработчиком*, она остается банке и может быть использована до вытеснения ее более совершенной (как показано на рис. 4.1) разработкой.

За счет возможности организации централизованного применения “лучших” из накопленных компонентов ДПО исключается параллелизм и дублирование неэффективных разработок, а также существенно (по имеющимся оценкам - примерно в 2-3 раза) сокращается время выполнения и стоимость опытно-конструкторских работ по созданию перспективных образцов ВТП.

4. Описание примерной номенклатуры банка экстремальных информационных технологий и конструкторских решений

Как отмечалось выше, Банк Ex'IT содержит набор отобранных и готовых к непосредственному применению "экстремальных" компонентов ДПО, а также (достаточно) полное описание доверенных информационных технологий и конструкторских решений по эффективному применению элементов номенклатуры банка с гарантией *качества* – достижения заданных показателей выходных свойств-характеристик разрабатываемой ВТП.

Пример формирования номенклатуры Банка Ex'IT представлен на рисунке 4.2.

Рис.4.2. Структурная схема актуальной номенклатуры доверенных защищенных компонентов Банка Ex'IT

Банк Ex'IT содержит оригинальные отечественные программные компоненты и решения, разработанные авторскими коллективами и

организациями. Представленное выше структурированное множество Ex'IT - компонентов обеспечивает наличие у конечных систем – образцов ВТП всего набора *экстремальных* свойств-характеристик *Ex'SC*, заданных в таблице 1, п.1.2.

Краткое описание компонентов 1-9 рисунка 4.2, приведено в таблице 2.

Таблица 2. Описание компонентов – элементов номенклатуры Банка Ex'IT

Наименование компонента	Назначение
1. Инструментальный комплект сервисов интеграции (ИКСИ)	Предназначен для оснащения критически важных информационно-управляющих систем (КВИУС), нарушение или прекращение функционирования которых может привести к потере управления объектом или процессом, деградации инфраструктуры, ухудшению безопасности жизнедеятельности населения
1.1 Транспортная служба гарантированной доставки (GRAF)	Предоставляет гарантированные услуги по доставке, хранению и обработке информации в распределенных неоднородных вычислительных сетях объектов заказчика. Обеспечивает транзит данных с использованием промежуточных узлов и шлюзование протоколов обмена информацией. Применяется для организации высоконадежных, доверенных систем обмена данными в КВИУС общего и специального назначения
1.2 Служба темпорального хранения данных (SLON)	Организация защищенного хранения информации на различных программно-аппаратных платформах с использованием оригинальной многомерно-темпоральной модели данных и поддержкой расширенного

	SQL-интерфейса для обработки запросов на различных «линиях времени» (в прошлом / настоящем / будущем)
1.3.Технологическая платформа интеграции приложений (CAPI)	Организация вычислительного процесса в гетерогенных территориально распределенных автоматизированных системах общего и специального назначения, Реализует различные модели *синхронного* (клиент/сервер) и *асинхронного* (обмен сообщениями) взаимодействия с использованием адаптеров сопряжения, высокопроизводительной защищенной интеграционной магистрали (ESB-шины) и витрин данных
1.4. Платформа автоматизации процессов документооборота (Ъ)	Построение многоуровневых защищенных ECM-систем предприятий и организаций. Использует встроенную интеграционную шину CAPI для подключения внешних систем документооборота и поддержки нескольких параллельных контуров прохождения информации - *служебного* (деловая переписка), *организационно-распорядительного* (управление инфраструктурой) и *личного* (неформальное взаимодействие абонентов с гарантией конфиденциальности)
2. Крипто-временной тоннель (ТРОПА)	Хранение текущего (актуального) состояния объектов файловых систем и баз данных, а также временны*х* версий - последовательности изменений свойств и состояния объектов в прошлом и в будущем (для решения задач ситуационного моделирования). Предоставление доверенных защищенных API-сервисов управления парольной службой, криптографического преобразования потоков данных и поддержки

	электронной подписи
2.1 Обозреватель темпоральной файловой системы (ХРОНОСКОП)	Реализация функций «машины времени» в темпоральной системе хранения именованных информационных объектов (файлов, каталогов, документов СЭД) с визуальным или API-доступом к версиям объектов и их свойствам на всем интервале жизненного цикла
2.2. Криптографический мульти-сервер (ЭНИГМА-$)	Криптографическое преобразование критически важной информации Заказчика, автоматическая генерация и смена паролей доступа, формирование и проверка цифровой подписи
3. Интерактивный экспресс-анализ данных (ALBA-ВИП)	Комплексная оценка и ранжирование заданного множества анализируемых объектов с представлением результатов в виде кластеров на визуальных интерактивных панелях (ВИП)
3.1 Служба экспресс-анализа серий данных (ALBA) Примечание: продукт разработан совместно с компанией «ЭТиС» (Россия)	Автоматическая или ручная настройка на источники данных и проведение по заданному шаблону или самим пользователем анализа множества объектов (т.н. “фоновой группы”), обладающих набором однотипных свойств, значения которых могут быть представлены в количественном или качественном выражении. Формируемая системой интегральная оценка отражает ранг (место) каждого объекта в группе с точки зрения целевой функции (задачи), определяемой конечным пользователем-аналитиком
3.2. Конструктор кластеров визуальных интерактивных панелей (ВИП- Конструктор)	Реализация интерактивных технологий визуального представления состава и динамики изменения свойств объектов с применением различных методов многомерной (многоаспектной) кластеризации

4. Система операционного управления (ПРОКУРАТОР) Примечание: продукт разработан совместно с компанией «ЭТиС» (Россия)	Двухконтурный мониторинг и управление распределенным автоматизированным комплексом на объектах КВИУС, включающим: • сегменты вычислительной инфраструктуры объектов автоматизации; • процессы выполнения бизнес-задач персоналом с использованием имеющейся вычислительной инфраструктуры
4.1. Служба управления распределенной вычислительной инфраструктурой (СКИФ)	Бескомпроматный “online” – контроль текущего функционального состояния всех элементов распределенной гетерогенной (неоднородной) вычислительной инфраструктуры заказчика (вычислительные узлы, каналы связи, программное обеспечение, интерфейсы и сервисы)
4.2. Служба мониторинга бизнес-процессов (ОКО)	Событийно-ориентированный механизм контроля хода и результатов выполнения регламентных процессов решения критически важных задач с использованием имеющейся территориально распределенной вычислительной инфраструктуры
5. Объединенный коммуникационный центр (ОКЦ) консолидации данных от разнородных источников (ПЛАТАН)	Обеспечивает консолидацию (сбор / накопление) и совместную логико-аналитическую обработку данных как открытого, так и ограниченного доступа, в т.ч. конфиденциальной информации, а также сведений, относящихся к категории государственной тайны. В интересах эффективного решения задач управления производством и бизнесом средствами ОКЦ «ПЛАТАН» реализуются операции по вертикальной и горизонтальной миграции (передаче)

	данных между открытыми и конфиденциальными сегментами различных уровней управления (холдинг / предприятие / производственная площадка, обеспечивается получение объективных результатов консолидированной обработки всех источников информации для принятия обоснованных управленческих решений.
6. Система гарантированной защиты ПЛАТО Примечание: продукт разработан совместно с компанией «ЭТиС» (Россия)	Устраняет недостатки применения типовых решений в части гарантированной защиты критически важной информации бизнеса и исключает утечки «чувствительной» информации и возможные последствия компрометации ее владельцев. На уровне архитектуры платформы изолируются критически важные данные и процессы их обработки от любых деструктивных воздействий, как со стороны программных «закладок», вирусов, так и злоумышленников (информационных террористов, инсайдеров и др.). Предлагаемое решение встраивается в существующую (у заказчика) вычислительную инфраструктуру и / или функционирует в отдельном (скрытом) сегменте сети. Применяется для построения высоконадежных, гарантированно защищенных сегментов критически важных систем, компрометация которых наносит ущерб деловой репутации и бизнесу заказчика.
6.1 Средства изоляции БД и критически важных процессов ГИПЕР'ОН	Обеспечивают двухслойную (внешнюю и внутреннюю) изоляцию посредством применения встраиваемых периметров защиты на уровне гипервизора безопасности. Применяется для защиты процессов автоматизированной обработки и баз

	данных систем CRM (*Customer Relationship Management*) - критически важных ресурсов заказчика, доступ к которым гарантированно обеспечивается только в санкционированном режиме. Средства гарантированной изоляции БД и процессов ГИПЕР'ОН в составе «ПЛАТО» обеспечивают организацию недоступной (для недоверенных процессов базовой ОС) защищенной области хранения данных, дополненной средствами объективной регистрации и автоматической обработки возникающих инцидентов безопасности
6.2 Средства нейтрализации внутреннего нарушителя НЕЙТРИНО	Ключевым аспектом является перехват и нейтрализация угроз со стороны всех, в т.ч. - *привилегированных*, категорий пользователей (сотрудник-инсайдер, системный администратор, администратор безопасности). Объективная регистрация действий должностных лиц, хранение событий безопасности и автоматическое выполнение сценариев их обработки производится в защищенной области гипервизора безопасности. Изоляция ресурсов и управление функционированием базовой ОС из среды гипервизора безопасности производится с применением механизмов защищенной аппаратной виртуализации
7. Агентство доступа к разнородным сетям передачи данных (А-ПОРТ)	Агентство «А-ПОРТ» является программным средством, предназначенным для реализации двустороннего доверенного взаимодействия распределенных процессов (задач) обработки данных с

	использованием набора защищенных доверенных API-интерфейсов: • потоковое чтение/запись данных на виртуальные устройства ввода/вывода (VIO); • обмен сообщениями/документами с использованием интеграционной шины CAPI; • доступ к защищенной файловой системе удаленных узлов (абонентов); • обмен с использованием протоколов ЭП (SMTP/POP3); • инкапсуляция интерфейсов «унаследованных» систем (wrapping); • защищенное прокси-соединение с удаленным сервером (port-mapping); • обмен документами в формате МЭДО (межвидовой электронный документооборот) ФОИВ РФ. Агентство реализовано в виде системной службы и функционирует под управлением широкого спектра операционных систем и существующих аппаратных платформ (от мэйнфреймов до мобильных решений)
8. Платформа функционирования «цифровых двойников» ПОЛИСФЕРА (в настоящее время находится в стадии разработки)	Предназначена для создания цифровых моделей (цифровых двойников) - программных (виртуальных) аналогов реальных физических объектов или процессов, воспроизводящих их структуру, состояние, а также динамику их изменения во времени. Может применяться для организации интегрированных хранилищ информации при создании ситуационно-

	аналитических центров (САЦ), а также информационно-управляющих автоматизированных систем на объектах ключевой информационной инфраструктуры

Все перечисленные выше компоненты являются доверенными программными средствами, в их составе отсутствуют неавторизованные заимствованные фрагменты программного кода отечественных или зарубежных разработчиков. Конструкторская и эксплуатационная документация на компоненты и технологии ведется в специализированном архиве «Лаборатории инновационных технологий при МГТУ им. Н.Э.Баумана» (ООО «ЛИНТЕХНО»).

В настоящее время на объектах автоматизированных систем различных заказчиков используется более 110 000 экз. (лицензий) из приведенного в таблице 2 перечня.

Список источников

1. Дэйвисон М. Многомерное шкалирование : методы наглядного представления данных.: Пер. с англ. – М.: Финансы и статистика, 1988. -254 с.: ил.
2. Здирук К. Б., Толпыгин А. С., Гречанюк Ф. А., Ханыгин А. Н. Цифровые модели объектов и модели данных в решении задач управления [Электронный ресурс] // Экстремальные технологии и системы URL: https://www.extansy.com/ (дата обращения 12.02.2019).
3. Здирук К. Б., Гречанюк Ф. А., Толпыгин А. С. Синтез цифровых двойников промышленных объектов с применением многоаспектной рекурсивной декомпозиции [Электронный ресурс] // Экстремальные технологии и системы URL: https://www.extansy.com/ (дата обращения 12.01.2019).
4. Здирук К. Б., Гречанюк Ф. А., Толпыгин А. С. Формальное определение меры представления знаний в информационном пространстве на основе когнитивного подхода [Электронный ресурс] // Экстремальные технологии и системы URL: https://www.extansy.com/ (дата обращения 12.01.2019).
5. Доверенная среда облачных вычислений /К.Б.Здирук, А.В.Зотова, С.А.Петренко, М.П.Сычев//Защита информации.ИНСАЙД. — 2013. № 5. с.28-33
6. Здирук К.Б. Вопросы организации защищенной системы хранения и обработки данных в гетерогенных вычислительных сетях // Вопросы защиты информации: Научно-практический журнал / ФГУП ВИМИ. – 2007. – Вып.3(78). – С.6-10