Версия 1.0

**Инициативы по повышению эффективности госполитики в сфере информационной безопасности и стимулирования развития индустрии в этой сфере**

**1. О статусе компаний сферы инфобезопасности в рамках госполитики.**

Развитие индустрии в обозначенной сфере напрямую зависит от статуса ИБ-компаний и готовности государства к взаимодействию с ними, как с отдельным сектором экономики. В настоящий момент они не имеют четко обозначенного статуса и находятся в менее выгодных условиях по сравнению с ИТ-компаниями (с т.з. мер поддержки).

Представляется важным определиться с вопросом: Выделять ли ИБ-компании в отдельный сегмент? Если да, то каковы критерии? Если нет, то как изменить ситуацию, когда ИБ-компании не могут воспользоваться мерами поддержки для ИТ-компаний.

**2. Меры поддержки предприятий сферы инфобезопасности**

**2.1.** Внести изменения в Положение о государственной аккредитации организаций, осуществляющих деятельность в области ИТ (ПП № 758 от 6 ноября 2007 г.), дополнив его следующим образом: Организация, получившая лицензии регуляторов, заносятся в реестр автоматически. (Например, лицензии на следующие виды деятельности: - техобслуживание защищённых средств обработки информации (кроме криптографических, предназначенных для использования в органах власти); - распространение (продажа, передача) защищённых средств обработки информации (кроме -//-); - разработка, производство, распространение шифровальных (криптографических) средств, инфо- и телеком- систем, защищённых с использованием шифровальных (криптографических) средств, …) Формулировки будут уточнены.

**2.2**. Внести изменения в алгоритм включения в Реестр отечественного ПО. Суть проблемы – невозможно оформить заявку на включение в Реестр ПО (по информационной безопасности), не имеющего действующего сертификата ФСТЭК или ФСБ. Но такой сертификат не всегда нужен. Например:

А) если ИБ-компания делает продукты для Минобороны (МО) и имеет сертификат по линии МО, то включить в Реестр такой продукт сегодня нельзя. Показывать в публичных документах сертификат МО тоже не целесообразно – возникнет риск попасть под санкции.

Б) если ИБ-компания делает ПО для коммерческих банков, частных пользователей или если компания производит дистанционной работы для сотрудников ФОИВ.

Невозможность включить программный продукт по ИБ без сертификата или с сертификатом МО ущемляет права ИБ-разработчиков, такое ПО нельзя поставлять без НДС, цены на ПО, как правило, заранее зафиксированы, следовательно, 20% НДС разработчикам приходится платить из прибыли. ИТ-компании, включившие свое ПО в Реестр, получили существенные преимущества перед ИБ-компаниями по льготам, как следствие – начались перекупка и переток лучших специалистов из ИБ-компаний.

**2.3.** Гармонизировать ситуацию для случаев работы ИБ-компаний на стыке программных и аппаратных средств, а также нахождения продуктов компании в разных реестрах (Минцифры и Минпромторга).

2.3.1. Комплексные поставки

Разработанное специальное программное обеспечение (СПО), реализующее функционал СКЗИ высокого класса защиты, устанавливается на специально выбранные и происследованные материальные платформы (сервера), обеспечивающие доверенную среду функционирования для работы СПО. Согласно требованию регулятора, для обеспечения соответствующего класса защиты, реализация функций безопасности возможна только в комплексе: СПО + Доверенная материальная платформа.

Однако, в таких комплексных поставках сложно обосновать льготы, предусмотренные Налоговым кодексом (ст.284 п.1.15 и ст. 427 п.5) для разработчика программного обеспечения. В данном случае, доля доходов от реализации ПО будет, с учетом реальной стоимости платформы и СПО, практически всегда меньше 90%, т.к. одновременно предприятие продает и программное обеспечение, и специфический материальный носитель (в нашем случае - сервер).

Крайне трудно доказать, что речь идёт о продаже ПО на материальном носителе, так как сами платформы предприятие не производит. Но, данный вариант требует дополнительного комплексного обсуждения совместно с представителями Минцифры, Минпромторга и Налоговой службы.

Ситуация усложняется, когда предприятие начинает разработку и производство собственных платформ для встраивания разработанного программного обеспечения. В этом случае, разработчики ПО становятся одновременно и разработчиками радиоэлектронной аппаратуры и достичь установленных пределов:

- 90% продажи программного обеспечения (льгота, предусмотренная Налоговым кодексом ст.284 п. 1.15 и ст.427 п.5), или

- 90% разработки радиоэлектронной аппаратуры, (льгота, предусмотренная Налоговым кодексом ст.284 п.1.16 и ст. 427 п. 14)

становится нереальным.

Да, и сама льгота, относящаяся к разработчикам радиоэлектронной аппаратуры, сложно достижима для предприятий, реализующих собственные разработки в виде программно-аппаратных комплексов, так как льгота предполагает 90% выручки только за реализацию работ по проектированию и разработке изделий электронной компонентной базы и электронной (радиоэлектронной) продукции.

2.3.2. Стыковка реестров и регулирования

В июне 2021 г. стало известно о поручении премьер-министра М.Мишустина объединить реестры отечественного ПО и телекоммуникационного и радиоэлектронного оборудования отечественного происхождения. Предлагается подключить к процессу гармонизации российские компании в области инфобезопасности, например, в рамках Комитета АПКИТ по ИБ с участием профильных комитетов ассоциаций, входящих в АПКИТ.

2.3.3. Критерии отнесения

Экспертизу компаний ИБ было бы целесообразно использовать и в дискуссиях по теме критериев отечественного продукта, отечественного производителя, отечественного разработчика, предлагая согласованные позиции ИБ-бизнеса и профильных регуляторов.

**2.4.** Для тех, кто работает по ГОЗ:

А) Предлагается отменить необходимость предоставления банковской гарантии. По 275-ФЗ с ГОЗ могут работать всего 8 уполномоченных банков. Эти банки требуют 100% финансового обеспечения (что означает изъять сумму аванса из своего оборота и положить в банк на 2-3 года), либо заложить своё имущество (квартиру, дачу, машину, бизнес) в обеспечение 75-80% суммы аванса, плюс выплачивать банку 2.5-5% от суммы банковской гарантии в год (\*3 года)

Б) Необходимо учесть ситуацию на мировом рынке микроэлектроники. Ситуация для России может ухудшиться … Сроки производства микросхем выросли до 1 года. Подтверждённый заказ не является гарантией - готовые заказы перекупаются крупными корпорациями, узнать о срыве поставки можно за 1 день до срока отправки. Цены на ряд ключевых компонентов выросли в 6-8 раз. Суммы валютных перечислений и список поставщиков жёстко зафиксированы, нельзя поменять ни поставщика (кто хотя бы обещает что-то сделать), ни сумму (купить нужные микросхемы за любые деньги чтобы не сорвать контракт)

Ожидаемые риски для экономики и бизнеса: пострадают все поставщики аппаратно-программных средств; будут сорваны поставки по ГОЗ; возможно разорение российских производителей.

Необходимо договариваться с МО об изменении условий работы по ГОЗ, иначе бизнесe будет не выгодно работать с ним. Необходимо увеличивать сроки поставки и согласовывать их с вендорами с учетом новых условий и рисков.

**2.5**. Увеличить до 50% доли авансирования ИТ-организаций, исполняющих контракты на поставку товаров, работ и услуг для государственных нужд, связанных с обеспечением инфобезопасности. Рассмотреть вопрос отмены внесения обеспечения исполнения контрактов при казначейском сопровождении этих контрактов.

Данные меры позволят улучшить финансовое положение ИТ- организаций, обеспечат их необходимыми ресурсами для своевременного исполнения обязательств по выплате заработанной платы, для сохранения численности штатного персонала и решения задач опережающего развития отечественной сегмента инфобезопасности.

**2.6**. Улучшить условия для создания СП в другой стране для совместной разработки и выпуска средств ИБ содержащих СКЗИ.

Российское законодательство жестко регулирует процесс экспорта готовых изделий ИБ содержащих СКЗИ, что порождает препятствия для развития экспорта и экспансии на мировой рынок (без чего мы не станем конкурентоспособными на мировом рынке).

С одной стороны, создание СП с зарубежными партнерами, с вероятной передачей партнерской стороне части технологий, используемых в собственных продуктах компаний, российским законодательством не регламентируется. С другой - исключается передача зарубежной стороне каких-либо технологий и документов, признанных в России сведениями ограниченного распространения.

В указе Президента РФ от 12 апреля 2021 г. № 213 "Об утверждении Основ государственной политики РФ в области международной информационной безопасности" прямо указано на продвижение на международной арене российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в области международной инфобезопасности а также продвижение национальных стандартов РФ в области инфобезопасности при осуществлении международного и регионального сотрудничества в сфере стандартизации, содействие их принятию в качестве международных, региональных и межгосударственных стандартов.

Требуется активная поддержка профильных регуляторов для устранения барьеров по выполнению Указа Президента.

**2.7.** Устранить барьеры экспорта подконтрольных гос.регуляторам товаров (СКЗИ)

2.7.1. Сократить срок получения лицензии ФСТЭК на экспорт подконтрольных товаров. Например, путем выдачи экспортной лицензии в 2 этапа:

А) Предварительное одобрение/не одобрение гос.регуляторами экспорта самой продукции со списком стран, разрешенных для экспорта.

Б) Рассмотрение гос.регуляторами каждого договора поставки на продукцию, предварительно разрешенную к вывозу (например, проверка поставки на назначение (гражданское / военное)) в менышие сроки, например, до 10 дней.

2.7.2. Разрешить экспорт продукции на склады партнеров / дистрибьюторов с последующим уведомлением гос.регуляторов о конечных заказчиках в этой той же стране (партнеры / дистрибьюторы и конечные заказчики в одной стране).

2.7.3. Разрешить вывоз с любого таможенного поста

**3. О необходимости доверенной экспертизы**

В области инфобезопасности государство имеет ответственных регуляторов, отвечающих за техническую и организационную стороны. Но в ряде случаев возникает вопрос независимой оценки финансово-экономической стороны крупных проектов.

Представляется целесообразным создать **Центр экспертизы** в этой сфере на базе некоммерческого объединения (например, АПКИТ и входящих в неё ассоциаций)

**4. О подготовке квалифицированных кадров**

ИТ – это прежде всего квалифицированные кадры. В рамках национальной системы квалификаций за профстандарты в сфере инфобезопасности отвечает СПК-ИТ. Предлагается выделить ответственных от профильных регуляторов для консультаций по теме подготовки кадров в области инфобезопасности (разработке и оценке новых профстандартов, образовательных программ, ФГОСов и т.п.)

Ваши поправки/ замечания/ предложения/ дополнения присылайте на [komlev@apkit.ru](mailto:komlev@apkit.ru)

---