

# Приключения КИИ в 2022 г.

Год 2022-й стал для критической информационной инфраструктуры России переломным. Для усиления безопасности КИИ было принято очень много законодательных решений, причем в обход Государственной Думы – на уровне указов Президента РФ, которые имеют даже большую юридическую силу. Первым был Указ от 30 марта № 166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ», направленный на ускорение процесса импортозамещения. Следующим стал Указ от 14 апреля № 203 «О Межведомственной комиссии Совета Безопасности РФ по вопросам обеспечения технологического суверенитета государства в сфере развития КИИ РФ», фактически создавший альтернативное правительство для дальнейшего стимулирования импортозамещения, которое с этого времени получило новое наименование – технологический суверенитет. А 1 мая был принят еще один Указ – № 250 «О дополнительных мерах по обеспечению ИБ РФ», который значительно расширил область применения законодательства по КИИ, определенное в Федеральном законе № 187 «О безопасности КИИ РФ».

Именно последний указ отметил директор блока интеграции BI.ZONE Тимурбулат Султангалиев как самый важный: «Наибольшее внимание привлек к себе Указ Президента РФ № 250 «О дополнительных мерах по обеспечению ИБ РФ». Он затрагивает около полумиллиона организаций, так как распространяется на ФОИВ; высшие исполнительные органы государственной власти субъектов РФ; государственные фонды, государственные корпорации и иные организации, созданные на основании федеральных законов; стратегические предприятия, стратегические акционерные общества и системообразующие организации российской экономики; юридических лиц, являющихся субъектами КИИ РФ». Однако рассмотрим указанные нормативные акты по порядку их опубликования.

## В КИИ только отечественное

Первым Президент РФ подписал 30 марта достаточно очевидный Указ № 166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ». Он определяет

требования, которые должны выполнить владельцы значимых объектов КИИ, причем некоторые пункты этого указа вступили в силу сразу – в момент опубликования, а самая отдаленная его часть будет введена действие с 1 января 2025 г. Кроме того, Указ № 166 предписывал Правительству РФ в течение месяца разработать требования к ПО, используемому органами государственной власти в составе ЗОКИИ, а также правила согласования закупок иностранного ПО и услуг, которые будут использоваться для обеспечения работы ЗОКИИ.

В частности, уже с 31 марта текущего года владельцам ЗОКИИ запрещается закупать иностранное ПО, в том числе в составе ПАК, которое приобретает в рамках Закона № 223-ФЗ (распространяется на государственные компании) без согласования с уполномоченным ФОИВ (Минцифры). С 1 января 2025 г. органам государственной власти полностью запрещается использовать иностранное ПО на принадлежащих им ЗОКИИ. То есть уже закупленное иностранное ПО можно использовать только до 1 января 2025 г. – до этого нужно закупить отечественное и перейти на него.

Кроме того, в течение месяца Правительство РФ должно было разработать требования к ПО, которое предполагается использовать в составе ЗОКИИ органов власти, а также правила согласования использования иностранного ПО, видимо, на случай отсутствия аналогов. Такие требования были разработаны Правительством РФ только к 22 августа и приняты Постановлением Правительства № 1478. В нем назначаются ФОИВ, которые ответственны за согласование использования иностранных решений. Минцифры назначается ответственным ФОИВ за контроль соблюдения правил согласования.

Впрочем, некоторые иностранные компании стимулировали отказ от своего ПО, объявив о прекращении деятельности на территории России. Скорее всего, использовать его и так будет невозможно, хотя есть нюансы, связанные с параллельным импортом. Возможно, какое-то время – до перехода на отечественные решения – можно будет использовать иностранное ПО без лицензии.

Наиболее интересные поручения правительству необходимо было исполнить в течение шести

месяцев, т. е. до 30 сентября. За это время предписывается реализовать «комплекс мероприятий, направленных на обеспечение преимущественного применения субъектами КИИ отечественных радиоэлектронной продукции и телекоммуникационного оборудования на принадлежащих им ЗОКИИ». В данный комплекс входят: определение сроков и порядка перехода субъектов КИИ на преимущественное применение доверенных ПАК; внесение законодательных поправок в соответствующие нормативные акты; обеспечение создания и организации деятельности НПО, специализирующегося на разработке, производстве, технической поддержке и сервисном обслуживании доверенных ПАК для КИИ; организация подготовки и переподготовки кадров в сфере разработки, производства, технической поддержки и сервисного обслуживания радиоэлектронной продукции и телекоммуникационного оборудования; создание системы мониторинга и контроля в названной сфере.

В результате владельцы ЗОКИИ должны готовиться к максимально быстрому переходу на доверенные ПАК – сроки и порядок будут разрабатываться в ближайшие полгода, но до 2025 г. отказаться от использования иностранного ПО точно придется. В упомянутом указе запрет на использование относится только к государственной сфере, однако уже в Постановлении Правительства № 1478 перечислены все упомянутые в Федеральном законе № 187-ФЗ сферы деятельности.

Разработчикам отечественных средств защиты со временем, видимо, придется войти в научно-производственные объединения в целях создания, производства и техподдержки доверенных ПАК специально для КИИ. Туда же должны войти и производители отечественного радиоэлектронного и телекоммуникационного оборудования. Скорее всего, такими консорциумами будут разработаны типовые ПАК, из которых,

как из запрещенного в России Lego, можно будет строить все ЗОКИИ. Учебным центрам и вузам необходимо разработать программы для подготовки и переподготовки кадров, которые будут эксплуатировать эти доверенные ПАК, поскольку работать с ними смогут, вероятно, исключительно сертифицированные специалисты.

Собственно, Минцифры уже анонсировало разработку и обсуждение программы перехода на российские продукты, которая будет опираться на реестр отечественного ПО. Министерство анонсировало разработку и общественное обсуждение новых правил включения отечественных разработок в реестр, куда теперь может попадать не только программное обеспечение, но и ПАК. Также существенно меняются правила включения ПО в реестр – теперь недостаточно, чтобы программное обеспечение было разработано российскими компаниями, важно, чтобы оно работало на основе российского программного и аппаратного обеспечения. Пока новые правила только обсуждаются, но направление совершенствования законодательства по импортозамещению уже вполне понятно.

## Промышленное правительство

Чуть больше, чем через две недели после издания Указа № 166, 14 апреля текущего года глава государства подписал другой Указ – № 203 «О Межведомственной комиссии Совета Безопасности РФ по вопросам обеспечения технологического суверенитета государства в сфере развития КИИ РФ». Согласно документу должна быть образована межведомственная комиссия Совета Безопасности России по обеспечению технологического суверенитета страны в сфере развития ИТ-инфраструктуры. Утвержден состав комиссии – ее будет возглавлять заместитель председателя Совета Безопасности РФ, эту должность занимает Дмитрий

Медведев. Ему поручается в месячный срок утвердить персональный состав комиссии.

Впрочем, в тексте указа состав комиссии вполне определен – в нее входят силовые ведомства России (Минобороны, МВД, МЧС, Росгвардия, СВР, ФСБ, ФСО, ФСТЭК), поддерживающие (Минэнерго, Минтранс, Минфин, Минэкономразвития, ЦБ РФ), а также исполнители (Минобрнауки, Минцифры и три руководителя госкорпораций «Росатом», «Роскосмос» и «Ростех»). То есть в состав создаваемой комиссии входит практически половина действующего состава Правительства РФ, причем как заказчики, так и исполнители с поддерживающими ведомствами, которые необходимы для производства отечественного оборудования и программного обеспечения. Никакой социалки, никакого спорта, никакого искусства – только самые важные министерства.

На комиссию возлагаются следующие функции: оценка уровня технологической независимости объектов КИИ от иностранных технологий; анализ эффективности деятельности органов и организаций по выполнению решений Совета безопасности, направленных на обеспечение технологического суверенитета государства в сфере развития КИИ; прогнозирование, выявление и оценка внутренних и внешних угроз национальной безопасности в следующих сферах: развитие ИТ, сетей электросвязи и информационно-телекоммуникационных сетей; развитие и поддержка производства отечественной продукции; развитие промышленности и ОПК в части, касающейся обеспечения технологического суверенитета; координация деятельности органов и организаций при решении оперативных, среднесрочных и долгосрочных задач по обеспечению национальной безопасности в области развития ИТ, производства средств связи, радио-промышленности и электронной промышленности; участие в разработке и реализации документов стратегического планирования;

рассмотрение в установленном порядке проектов государственных программ РФ в области развития ИТ, производства средств связи, радиопромышленности и электронной промышленности, оценка эффективности их реализации; разработка основных направлений совершенствования правового регулирования в области обеспечения технологического суверенитета.

Кроме того, на комиссию возлагается подготовка предложений и рекомендаций Совету Безопасности России по вопросам, касающимся: формирования государственной политики в области развития и поддержки производства отечественной продукции, разработки, внедрения и использования информационно-телекоммуникационных технологий; принятия правовых, организационных, научно-технических, финансовых и иных мер, необходимых для реализации мероприятий по обеспечению технологического суверенитета; выявления и предотвращения угроз национальной безопасности в области обеспечения технологического суверенитета; оценки соответствия систем государственного и военного управления современным требованиям, касающимся устойчивости и надежности функционирования объектов КИИ, с учетом цифровой трансформации экономики; разработки комплекса мер по оптимизации использования бюджетных ассигнований, предусмотренных в федеральном бюджете на реализацию мероприятий по обеспечению технологического суверенитета; научного, научно-технического и технологического обеспечения развития сетей электросвязи и информационно-телекоммуникационных сетей, радиоэлектронной промышленности, а также создания и развития национального центра хранения и верификации пакетов программ и электронных библиотек данных, необходимого для осуществления деятельности органов и организаций в области создания отечественной продукции.

Таким образом, на комиссию возлагаются фактически те же обязанности, что и на Правительство РФ, но только в части промышленности и производства, без социальных обязательств. Даже состав большей частью дублируется, но при этом отвечает межведомственная комиссия не перед главой Правительства РФ, а перед Советом Безопасности России, который возглавляет напрямую Президент РФ. Возглавляет комиссию Дмитрий Медведев – бывший глава Правительства РФ. Однако с точки зрения КИИ именно этот орган, похоже, будет в дальнейшем определять возможности использования тех или иных информационных и промышленных технологий.

Интересно, что в Правительстве РФ есть альтернативная структура – Правительственная комиссия по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности. Она является координационным органом, образованным в целях обеспечения взаимодействия федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ по вопросам развития экосистем цифровой экономики и повышения уровня использования информационных технологий и связи в целях формирования в РФ информационного общества и электронного правительства. Образована она еще в феврале 2020 г., но особых результатов ее деятельности не заметно. Будем надеяться, что у Дмитрия Медведева лучше получится обеспечить технологический суверенитет, чем цифровое развитие.

## Расширение ГосСОПКА

В день весны и труда, 1 мая 2022 г., Президент РФ подписал еще один документ – Указ № 250 «О дополнительных мерах по обеспечению ИБ РФ», в котором для повышения устойчивости и безопасности функционирования информационных ресурсов РФ

было существенно расширено применение государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА). До недавнего времени подключение к ней было обязательно только для владельцев значимых объектов КИИ, а данный указ обязывает организовать такое взаимодействие всем «федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов РФ, государственным фондам, государственным корпорациям, компаниям и иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры РФ», а не только владельцам ЗОКИИ.

Когда Федеральный закон № 187-ФЗ был принят и начал внедряться на предприятиях, все эксперты по ИБ предупреждали, что правительство будет постепенно усиливать «необходимость» его внедрения: вначале меры рекомендательные, затем обязательные только для государственных компаний, далее – для тех, кто работает с государственными, потом будут приняты предельные сроки приведения в соответствие и т. д. до тех пор, пока все владельцы КИИ так или иначе не реализуют требования по защите. Однако сейчас скорость «усиления», видимо, не устраивает руководство НКЦКИ, даже принятие законодательных поправок через Госдуму – для них слишком медленный процесс. Поэтому решили пойти наиболее быстрым путем – через указы Президента РФ, которые могут перекрывать юридическую силу федерального закона.

Указ «перескакивает» сразу несколько ступеней усиления критичности объектов информатизации, и в этом его революционность. В частности, он расширяет

сферу применения ГосСОПКА на ФОИВ, государственные фонды, стратегические предприятия и другие организации, перечисленные выше. НКЦКИ всегда приглашал присоединяться к построенной им системе не только владельцев ЗОКИИ, но и всех нуждающихся в защите, и теперь, по мнению Президента РФ, список таких организаций нужно значительно расширить. Однако важно, чтобы в подключаемых компаниях работали все-таки специалисты, которые смогут адекватно отреагировать на предупреждения НКЦКИ. Именно поэтому в указе есть следующие требования: возложить на заместителя руководителя организации полномочия по обеспечению ИБ; создать в организации структурное подразделение, осуществляющее функции по обеспечению ИБ (это и есть служба ИБ – СИБ) или назначить из существующих; принимать при необходимости решения о привлечении внешних организаций к выполнению мероприятий по обеспечению ИБ (аутсорсинг); обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются ФСБ России и ФСТЭК России.

Важность Указа № 250 подчеркнул Тимурбулат Султангалиев, который отметил следующие существенные изменения: «Во-первых, указ требует создать в организациях из перечня подразделения информационной безопасности, на руководителей этих организаций возложить персональную ответственность за обеспечение ИБ, а на заместителей руководителей – полномочия по обеспечению ИБ. Это также скажется на рынке информационной безопасности. Во-вторых, одно из основных требований указа состоит в том, что с 1 января 2025 г. организациям из вышеприведенного перечня запрещено использовать средства защиты информации (СЗИ), если страна происхождения СЗИ – недружественное иностранное государство или если производитель

СЗИ – организация, находящаяся под юрисдикцией недружественной страны, подконтрольная ей либо аффилированная с ней. Этот запрет инициирует пересмотр используемых средств защиты и явно повлияет на российский рынок ИБ в ближайшем будущем».

Интересным пунктом Указа № 250 является требование «обеспечивать должностным лицам органов ФСБ беспрепятственный доступ (в том числе удаленный) к принадлежащим организациям либо используемым ими информационным ресурсам, доступ к которым обеспечивает посредством использования информационно-телекоммуникационной сети Интернет, в целях осуществления мониторинга». Алексей Лукацкий в своем блоге отметил, что «бояться этого не стоит – это просто формулировка. Она существовала и в законодательстве по КИИ и всего лишь означала, что если у вас произойдет инцидент ИБ и к вам придут разбираться и проводить расследование сотрудники ФСБ, то чинить препятствия им вы не имеете права. Сейчас, правда, добавили еще про удаленный доступ, но тут пока сложно что-то сказать». В общем, организациям стоит предусмотреть собственную систему мониторинга инструментов удаленного государственного мониторинга, «чтобы чего не вышло». Но появление этого требования было, в принципе, предсказуемо.

Стоит отметить, что в самом указе нет ответственности за его несоблюдение, кроме фразы: «возложить на руководителей органов персональную ответственность за обеспечение ИБ соответствующих организаций». Скорее всего, ответственность будет в рамках изменений в КоАП и УК, которые были внесены ранее за несоблюдение требований к безопасности КИИ – штрафы и уголовная ответственность. Но для юристов здесь есть хорошее пространство, для того чтобы показать свою компетентность в крючкотворстве.

Аналогичная проблема и с проверками: если в текущей версии Закона № 187-ФЗ предполагаются проверки прокуратуры, то в указе процедура проверки не предусмотрена.

Одно дело – «оценка уровня защищенности», другое – «обеспечение информационной безопасности». Для первого срок определен, для второго – нет. Это и понятно, поскольку большая часть организаций – государственные, а в их бюджетах не предусмотрены средства для исполнения данного указа. Для его реализации нужно пройти как минимум один цикл бюджетирования, проведения тендеров и всего того, что связано с контролем расходования бюджетных средств. А это процесс не быстрый.

Также не совсем очевидна необходимость построения системы управления информационной безопасностью (СУИБ). Если в законодательстве о КИИ ее построение предусмотрено на уровне приказа ФСТЭК № 235, то текущий указ обтекаемо требует только «обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются ФСБ РФ и ФСТЭК РФ». Но распространяется ли требование приказа № 235, который разработан в рамках законодательства КИИ, на организации, которые подпадают под действие Указа № 250, не совсем понятно. В результате требование по созданию средств обеспечения безопасности может не распространяться на новых членов «содружества КИИ».

Наиболее удобный способ быстро выполнить требования данного указа – воспользоваться услугами коммерческих SOC. Это, как уже было сказано, предусмотрено указом – не строить свою СУИБ, а арендовать готовую. До недавнего времени существовали SOC, которые взаимодействовали с ГосСОПКА в соответствии с соглашениями о сотрудничестве. В новом указе от ФСБ потребовали ограничить срок действия соглашений

и организовать официальную аккредитацию центров ГосСОПКА. Но для этого нужно еще разработать правила аккредитации и утвердить их отдельным приказом. Однако в указе не перечислены даже принципы подобной аккредитации, что подозрительно.

## Дальнейшее совершенствование КИИ

Подписанные Президентом РФ указы, как было отмечено, требуют конкретизации в виде федеральных законов и подзаконных актов. Скорее всего, работа по уточнению и интеграции норм перечисленных указов будет продолжена и реализована уже на уровне федерального

законодательства. Здесь и легализация доверенных ПАК, и различные дорожные карты по достижению технологического суверенитета, и меры поддержки для производителей российских доверенных ПАК и радиоэлектронных компонентов для них, и требования по безопасности к новым участникам критической информационной инфраструктуры, и еще много всяких нормативных актов.

Минцифры выступило с интересной инициативой – создать реестр недопустимых событий на объектах критической инфраструктуры. Если в компании произойдет событие, указанное в этом реестре, то у ее руководства или ответственных лиц могут возникнуть юридические проблемы. Советник генерального директора Positive Technologies Артем

Сычев подтвердил, что работа над созданием и легализацией реестра ведется. «Предполагается сформировать реестр событий, недопустимых для основной деятельности организации, – заявил он. – Причиной таких событий могут быть кибератаки, в том числе с использованием уязвимостей программного обеспечения. Таким образом, Минцифры стимулирует перенос внимания топ-менеджмента компаний к ИБ от исключительно технических вопросов к пониманию важности ИБ для основной деятельности. В свою очередь, это должно способствовать повышению реальной защищенности компаний в киберпространстве». ■

**Валерий КОРЖОВ,**  
*Connect*

## Требования к ЗОКИИ

Правительство приняло Постановление № 1478 «Об утверждении требований к программному обеспечению...», которым утвердило требования к ПО, используемому органами власти и госкомпаниями на значимых объектах КИИ, а также правила согласования закупок иностранного и перехода на отечественное ПО. Оно было принято в рамках реализации требований Указа № 166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ», который был принят 30 марта этого года и требовал от Правительства РФ в течении месяца утвердить требования к ПО, используемому органами государственной власти в составе ЗОКИИ, а также правила согласования закупок иностранного ПО и услуг, которые будут использоваться для обеспечения работы ЗОКИИ.

В результате, необходимые требования и правила были утверждены только в конце августа и уже вступили в силу. Требований всего два:

- 1) все программное обеспечение и ПАК в ЗОКИИ должны быть включены в реестр отечественного ПО;
- 2) все средства защиты должны быть сертифицированы по требованиям ФСТЭК и ФСБ в рамках

их полномочий. Собственно, ради того чтобы включить в реестр Минцифры программно-аппаратные комплексы, сейчас проводится общественное обсуждение новых правил включения продукции в соответствующий реестр.

Правила согласования закупки иностранного ПО также достаточно просты: согласование использования иностранного ПО нужно проводить с ответственными за соответствующую сферу ведомствами, а в целом ответственным за контроль соблюдения правил назначается Минцифры. В постановлении, в частности, Минздрав отвечает за сферу здравоохранения, Минобрнауки – за науку, Минтранс – за транспорт, Минцифры – за связь, Минфин – за банковскую и финансовые сферы, Минэнерго – за энергетику и ТЭК, Минпромторг – за горнодобывающую, металлургическую, ракетно-космическую, оборонную, химическую промышленности, а также в сфере использования атомной энергии. Впервые со времени принятия Закона № 187-ФЗ «О безопасности КИИ РФ» сферы, перечисленные в законе, распределены между ответственными министерствами.