ЦЕНТР СТРАТЕГИЧЕСКИХ РАЗРАБОТОК

ВНЕШНЯЯ ПОЛИТИКА И БЕЗОПАСНОСТЬ

БУДУЩЕЕ **ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:** ГЛОБАЛЬНЫЕ ТРАНСФОРМАЦИИ И СЦЕНАРИИ ДЛЯ РОССИИ

ДОКЛАД

ТЕКСТ: О. В. **ДЕМИДОВ**

РЕДАКЦИЯ: А. Ф. **ЗУЛЬХАРНЕЕВ**, С. В. **УТКИН**

ПИР-ЦЕНТР

СОДЕРЖАНИЕ

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АСУ ТП	автоматизированные системы управления технологическим процессом
АРФ	Региональный форум Ассоциации государств Юго-Восточной Азии по безопасности
БСО	безопасность, стабильность и отказоустойчивость
ГПЭ ООН	Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности
ЕАЭС	Евразийский экономический союз
ЖВУ	жизненно важные услуги
ИБ	информационная безопасность
ИКТ	информационно-коммуникационные технологии
ИТ	информационные технологии
КИ	критическая инфраструктура
КИИ	критическая информационная инфраструктура
МАГАТЭ	Международное агентство по атомной энергии
МГП	международное гуманитарное право
НДВ	недекларированные возможности
НПА	нормативный правовой акт
НЦИ	новая цифровая инфраструктура
ОБСЕ	Организация по безопасности и сотрудничеству в Европе
ОДКБ	Организация Договора о коллективной безопасности
ООН	Организация Объединенных Наций
СКЗИ	системы криптографической защиты информации
УИИ	уникальные идентификаторы Интернета
ФОИВ	федеральный орган исполнительной власти
ШОС	Шанхайская организация сотрудничества
BGP	Border Gateway Protocol (Протокол граничного шлюза)
CERT	Cyber Emergency Response Team (центр реагирования на компьютерные инциденты)

CSIRT	Computer Security Incident Response Team (команда компьютерной безопасности по реагированию на инциденты)
ccTLDs	Country-code Top Level Domains (страновые домены верхнего уровня)
DNS	Domain Name System (система доменных имен)
ICANN	Internet Corporation for Assigned Names and Numbers (Корпорация Интернета по распределению имен и адресов)
IEEE	Institute of Electrical and Electronics Engineers (Институт инженеров электроники и электротехники)
IETF	Internet Engineering Task Force (Рабочая группа по проектированию Интернета)
NIST	National Institute of Standards and Technology (Национальный институт стандартов и технологий)
RFC	Request For Comments (запрос комментариев)
RIR	Regional Internet Registry (Региональная регистратура Интернет)
SOC	Security Operation Center (центр управления информационной безопасностью)

1.

УСЛОВИЯ ЗАДАЧИ

1. *Трансграничная деятельность государств и других субъектов в сфере использования ИКТ не охвачена международно-правовыми нормами в части обеспечения безопасности.* Отсутствуют механизмы и нормы, которые бы эффективно определяли и разграничивали правомерные и неправомерные действия, а также устанавливали ответственность за совершение неправомерных действий. В частности, речь идет об использовании ИКТ в военно-политических целях, в том числе в обстановке международных конфликтов.

В отношении ИКТ как средства ведения военных действий и киберпространства как синтетического понятия, применяемого для обозначения новой техногенной среды действий, неочевидна возможность применения существующего корпуса норм международного гуманитарного права и права вооруженного конфликта. Буквальное применение существующих базовых норм (Женевские конвенции 1949 г. и проч.) невозможно в силу технологической специфики ИКТ, а эффективная адаптация таких норм с учетом технических нюансов ИКТ пока не выработана. Отдельной проблемой является отсутствие универсальных определений и классификаций объектов и активов (критические информационные инфраструктуры/критически важные объекты), для которых должна обеспечиваться безопасность.

2. *Не выработано фундаментальное решение проблемы атрибуции неправомерных действий с использованием ИКТ, включая военные кибероперации и акты компьютерной преступности.* Как на национальном, так и на международном уровне отсутствует единый подход к квалификации полученных в ходе расследования инцидента технических данных в качестве юридически значимых фактов, которые могут быть приняты в качестве доказательств в различных юрисдикциях. Технические возможности атрибуции также серьезно ограничены за счет анонимности как фундаментального свойства коммуникаций в компьютерных сетях, включая интернет. Невозможность эффективной атрибуции действий с использованием ИКТ служит стимулом для роста компьютерной преступности и противоправных действий, осуществляемых государствами и субъектами-посредниками.

3. *Противодействие трансграничным угрозам и управление инцидентами ИТ-безопасности остается преимущественно сконцентрировано на уровне отдельных государств или отраслей.* Ключевой проблемой является недостаточный уровень доверия в системе международных отношений, препятствующий созданию совместных

механизмов обеспечения безопасности. Фрагментарно развиты механизмы совместного реагирования на инциденты ИТ-безопасности на объектах критической информационной инфраструктуры (экосистема CSIRT/CERT). Отсутствует глобальный механизм трансграничного реагирования и расследования киберпреступлений, обеспечивающий оперативный трансграничный обмен/раскрытие данных в рамках расследования (в механизме Будапештской конвенции Совета Европы от 2001 г. не участвует большинство государств, включая Россию). В части борьбы с киберпреступностью серьезным барьером к повышению глобального уровня безопасности является фрагментация составов преступлений и методов борьбы с ними по отдельным государственным юрисдикциям, что ведет к появлению «безопасных гаваней» для акторов, пользующихся несовершенством правовой базы и правоприменительной практики в отдельных государствах.

4. *Трансграничный характер и взаимосвязанность ИКТ и глобальных информационных инфраструктур (включая инфраструктуру интернета) делают невозможным обеспечение безопасности в сфере использования ИКТ в масштабах отдельно взятого государства/экономики, включая Россию, исключительно собственными силами.* Зависимость от внешних акторов и ресурсов можно классифицировать по трем категориям:

1. зависимость от трансграничных распределенных инфраструктур и программно-аппаратных ИТ-платформ, обеспечивающих работу критически важных с точки зрения безопасности сервисов (система уникальных идентификаторов Интернета, ИТ-инфраструктура системы SWIFT, экосистема корневых удостоверяющих центров и сертификатов безопасности и проч.);

2. зависимость от глобальных цепочек поставок для комплексных ИТ-инфраструктур (АСУ ТП производственных объектов и технологических комплексов, сетевое оборудование операторов связи, системы обработки и хранения данных и проч.);

3. включенность в трансграничные цифровые экосистемы, основанные на глобальных стандартах цифровой идентификации, криптографической защиты информации, передачи и обработки данных и проч. Включенность РФ в глобальные цифровые экосистемы, инфраструктуры и цепочки поставок является естественным состоянием в глобализованном мире, но серьезно ограничивает возможность нейтрализовать внешние угрозы за счет опоры только на собственные ресурсы.

5. Включенность в трансграничные связи и технологические цепочки ставит лица, принимающие решения в сфере ИТ, перед ***долгосрочной дилеммой:*** *обеспечивать ИТ-безопасность, инвестируя ресурсы в повышение конкурентоспособности своих защищенных технологий и бизнес-решений на глобальном ИТ-рынке, встраивание собствен-*

ных наработок в глобальные цепочки добавленной стоимости ИТ, — или делать ставку на снижение зависимости от зарубежных ИТ-экосистем, инфраструктур, сервисов и стандартов безопасности, создавая их локальные аналоги.

Для России практическое измерение этой дилеммы описывается рядом политических развилок:

1. Каково будущее политики импортозамещения в нише ИТ-безопасности? Возможно ограничение импортозамещения критически важными системами и сегментами либо курс на тотальную локализацию технологической базы и линейки продукции в сфере ИТ (укрепление безопасности за счет выхода из глобальной конкуренции и разделения труда в сфере ИТ);

2. Как обеспечить стабильность и устойчивость Рунета? Путем наращивания распределенности и связности его трансграничной инфраструктуры (DNS, IXP, оборудование магистральных провайдеров и проч.) либо за счет создания резервных автономных инфраструктур и технических решений, снижающих зависимость российского сегмента Сети от глобального.

3. Как подойти к локализации бизнес-процессов и инфраструктур ИТ-отрасли? Ориентироваться на замыкание внутри национальных границ за счет локализации хранения с целью обеспечения безопасности (экстраполяция подхода, заложенного в «пакет Яровой», закон о локализации хранения персональных данных и проч.) либо предпочесть курс на создание общего пространства безопасности за счет продвижения общих трансграничных сервисов, продуктов и стандартов ИТ-безопасности, выстраивания безопасных совместных ИТ-экосистем (проект «цифровой трансформации» в рамках ЕАЭС, вовлечение в европейские и трансрегиональные инициативы и международно-правовые механизмы по обеспечению кибербезопасности, сетевой безопасности и проч.).

6. *В нише ИТ-безопасности нереалистично эффективное «управление будущим» за пределами краткосрочной перспективы.* Ключевым драйвером развития технологий и стандартов ИТ-отрасли служит частная коммерческая инициатива, создание принципиально новых сервисов, а также оптимизация существующих бизнес-процессов. В такой парадигме развития обеспечение безопасности всегда было и будет подчиненной задачей, которая будет решаться не на стадии дизайна новых систем, стандартов и продуктов, а как правило «на ходу», уже после их выхода на рынок. В результате для большинства новых цифровых технологий и сервисов характерен период «окна незащищенности», когда продукт, технология или сервис уже запущены на массовый рынок, но его изъяны в части безопасности еще не выявлены или не устранены. Сегодня примером такой технологии является Интернет вещей (IoT), который в силу крайне низкой защиты своих объектов служит ресурсной

базой для организации сетевых атак, впервые угрожающих устойчивости всего Интернета. В среднесрочной перспективе такими технологиями могут стать «умные» киберфизические системы критически важных объектов и сложных инфраструктур (мегаполисы), а также системы передачи данных на основе квантовых эффектов (квантовые компьютеры). В долгосрочном плане неясны риски безопасности сильного искусственного интеллекта, особенно в промышленном, логистическом и военном применении, а также технологий, связанных с созданием и повсеместным применением нейроинтерфейсов «компьютер-мозг». Непредвиденные риски безопасности могут возникать и в процессе развития более привычных технологий и сервисов (оборудование для маршрутизации сетевого трафика, АСУ ПТП, облачные сервисы, системы обработки и хранения данных, распределенные цифровые реестры, компьютерные социальные сети и проч.).

При описании развилок стратегии и обосновании оптимальности предлагаемых вариантов учитывается влияние базовых внешних переменных. Переменные определяются в том числе на основе актуальных документов долгосрочного планирования и прогнозов, а также стратегических документов, разработанных и принятых в РФ.

В рамках настоящего исследования учитывались внешние переменные трех видов:

1. Динамика общего и отраслевого экономического развития РФ;

2. Внешнеполитическая динамика;

3. Динамика развития российской и глобальной отрасли ИКТ.

2.

СНИЖЕНИЕ **РИСКОВ ВОЕННО-ПОЛИТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ ИКТ** И ФОРМИРОВАНИЕ ОСНОВ МЕЖДУНАРОДНО-ПРАВОВОГО РЕЖИМА ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ ГОСУДАРСТВ И АКТОРОВ-ПОСРЕДНИКОВ В КИБЕРПРОСТРАНСТВЕ

Цель:

Укрепление международной безопасности и стабилизация системы международных отношений за счет ограничения использования ИКТ в военно-политических целях, а также снижения риска возникновения и эскалации международных конфликтов с использованием ИКТ.

Задачи:

- Определение и закрепление на международном уровне возможностей и ограничений в части военно-политического использования ИКТ в отношении объектов критической информационной инфраструктуры (КИИ) и критической инфраструктуры (КИ); определение круга категорий либо перечня объектов КИ и КИИ, подпадающих под соответствующие ограничения либо иные нормы, конституирующие режим ответственного поведения в киберпространстве.

- Выработка на международном уровне норм, позиций, подходов в отношении ограничения, запрета или иных особых требований к созданию, распространению (в том числе экспорту, импорту и иной трансграничной передаче) и применению программного обеспечения, программно-аппаратных комплексов либо иных технических средств, специально предназначенных для осуществления проактивных операций вооруженных сил, компьютерных атак на объекты КИ/КИИ, несанкционированного сбора электронных данных и иных действий, запрещенных международными нормами либо национальным законодательством государств-членов ООН.

- Интерпретация ключевых понятий существующей системы международного права, включая понятия «использование силы», «агрессия» с точки зрения возможности и способов их применения к действиям с использованием ИКТ.

- Выработка признаваемого международным сообществом и специализированными международными организациями (МККК) подхода к адаптации ключевых норм международного гуманитарного права (включая Женевские конвенции 1949 г. и проч.) к действиям с использованием ИКТ.

В среднесрочной перспективе разумно ориентироваться на принятие в основном добровольных необязывающих норм в многостороннем (ООН, ОБСЕ) либо двусторонних форматах. Также речь может идти о подписании международного соглашения, обязывающего по форме, но имеющего рамочный формат, устанавливающего общие принципы обеспечения международной безопасности в сфере использования ИКТ и не содержащего обязательств с конкретными сроками выполнения.

В долгосрочном плане возрастает шанс на выработку комплексного обязывающего режима ответственного поведения государств в сфере использования ИКТ, зафиксированного в форме конвенции ООН либо обязывающего международного договора, открытого для присоединения всех стран и содержащего в себе механизмы верификации выполнения принятых обязательств.

Можно выделить как минимум два возможных варианта долгосрочной деятельности по обозначенным направлениям:

Стратегия № 1 — «Стратегия вооруженного пессимиста»: страхование рисков в условиях минимального доверия

Стратегия № 2 — «Стратегия малых шагов» и мобилизации ресурсов частного сектора в управлении вызовами военно-политического использования ИКТ

2.1. «СТРАТЕГИЯ ВООРУЖЕННОГО ПЕССИМИСТА»: СТРАХОВАНИЕ РИСКОВ В УСЛОВИЯХ МИНИМАЛЬНОГО ДОВЕРИЯ

В основе стратегии лежит сценарий, согласно которому в обозримом будущем международному сообществу не удастся создать эффективный международно-правовой механизм, существенно ограничивающий использование ИКТ в военно-политических целях и позволяющий снизить до приемлемого уровня риски отдельных государств, включая РФ. В стратегии учитываются следующие риски:

- Наработки ГПЭ ООН и региональных площадок в области международного сотрудничества и безопасности (ОБСЕ, АРФ) в части выработки международных норм, правил поведения и иных ограничений не будут имплементированы государствами из-за отсутствия достаточных стимулов у самих государств и частных игроков ИТ-индустрии, слабых средств атрибуции противоправных действий в киберпространстве, проблематичности верификации и контроля соблюдения выработанных норм.

- Международному сообществу не удается прийти к общему, гармонизированному пониманию и способу адаптации базовых норм международного гуманитарного права и права вооруженного конфликта с учетом специфики ИКТ. Не происходит закрепления в международных документах интерпретации понятий «агрессия» (в том числе с учетом резолюции ГА ООН «Определение агрессии» от 1974 г.), «использование силы», «вооруженная атака» применительно к действиям государств и посредников в киберпространстве. Низкий уровень доверия также может не позволить участникам международного сообщества договориться о международно-правовой оценке действий, не достигающих порога использования силы.

- Растущий ущерб от высокотехнологичной преступности, военно-политической активности в киберпространстве, обострение глобальной конкуренции в интернет-зависимых нишах экономики и другие факторы могут подтолкнуть государства к обеспечению безопасности цифровых активов и инфраструктур, находящихся в их юрисдикции, за счет курса на выборочную изоляцию этих активов и инфраструктур от трансграничного доступа на уровне регулирования трансграничных потоков данных, локализации технических стандартов ИТ-отрасли, а также ограничениям на уровне сетевой и физической инфраструктуры.

С учетом этих составляющих сценария, внешнеполитическая стратегия РФ может быть нацелена на минимизацию военно-политических рисков в сфере использования ИКТ прежде всего за счет наращивания и демонстрации собственных воен-

но-технологических ресурсов в области ИКТ и укрепления жестких двусторонних и региональных альянсов в сфере цифровой безопасности.

Соответственно, стратегия предполагает вынужденное сокращение ресурсов и усилий, инвестируемых в формирование пространства доверия и открытости в области трансграничного использования ИКТ на основе общих норм и правил. Обмен информацией, развитие совместной инфраструктуры реагирования на киберинциденты с США, ЕС и рядом других партнеров отступают на второй план, теряют приоритетный статус. Участие РФ в треках ГПЭ ООН, ОБСЕ, АРФ в части выработки мер доверия и общих норм в сфере использования ИКТ целесообразно сохранить, однако его интенсивность и ожидания от результатов этой работы снижаются.

Резко повышается приоритет задачи по формированию «страховочной сетки», способной решать задачу-минимум — предотвратить эскалацию инцидентов в киберпространстве до уровня дипломатического кризиса и особенно международного конфликта с использованием как ИКТ, так и кинетических вооружений.

МЕРЫ по формированию страховочной сетки и предотвращению эскалации инцидентов в киберпространстве:

1. *Доведение до партнеров и потенциальных противников (США, НАТО, ЕС, Китай) российского одностороннего (либо сформулированного в рамках ОДКБ/ШОС/БРИКС) понимания недопустимых порогов действий в киберпространстве* («красных флажков») и возможной российской реакции.

Обозначение границ действий, способных повлечь военный ответ, логично включать во внешнеполитическую повестку дня по мере проработки и детализации собственного подхода РФ к этим вопросам. До 2020 г. вероятна разработка и публикация отдельной стратегии операций ВС РФ в информационном пространстве (по аналогии с военной киберстратегией Пентагона), резервирующей за РФ право на неограниченное использование своего военного потенциала в ответ на действия с использованием ИКТ, достигающие порога использования силы с точки зрения РФ.

Активизация работы по проведению закрытых консультаций и брифингов между военными РФ и США, НАТО, ЕС, Великобритании, КНР, Израиля и проч. по вопросам интерпретации конкретных норм международного гуманитарного права применительно к действиям в киберпространстве (включая определение порогов применения силы в киберпространстве), совместного управления эскалацией кризисов в киберпространстве и иным мерам обеспечения минимально приемлемого уровня стратегической стабильности в киберпространстве.

2 *Выстраивание сети двусторонних экстренных механизмов информирования и оповещения* об инцидентах и кризисах в киберпространстве как с ключевыми партнерами, так и с вероятными источниками киберугроз (включая прежде всего США) вместо развития экосистемы средств повышения доверия и открытого обмена данными, в том числе через структуры частного сектора.

3 *Поддержка кризисных каналов коммуникации для предотвращения неконтролируемой военной эскалации конфликта* вместо укрепления доверия, совместного расследования трансграничных инцидентов и повышения открытости деятельности в киберпространстве. Примерной моделью для таких каналов кризисной коммуникации служит горячая линия взаимного информирования о кризисах в киберпространстве, организованная на базе инфраструктуры Национальных центров по уменьшению ядерной опасности (НЦУЯО) между США и РФ в рамках пакета двусторонних соглашений от 2013 г.

4 *Формирование коллективных форматов взаимодействия в сфере безопасности использования ИКТ с союзниками и партнерами.* Возможности формирования пространства общих принципов, норм и правил поведения в области использования ИКТ ограничиваются жесткими конструкциями, выступающими в роли провайдеров коллективной безопасности для своих участников и, желательно, связанными общими технологическими стандартами в сфере ИКТ, либо непосредственно общей инфраструктурой. Для РФ таким форматом является прежде всего ОДКБ, однако важной задачей становится вовлечение в ряды союзников КНР как одного из глобальных лидеров в области ИКТ, включая военно-стратегическое применение цифровых технологий. В рамках формата ОДКБ+ (либо ШОС) возможна выработка общего подхода к квалификации и пороговым критериям враждебных внешний воздействий в киберпространстве, а также механизмов обмена информацией и совместных действий в случае кризисов, вплоть до механизмов коллективной обороны в ответ на применение силы/агрессию с использованием ИКТ. Такие механизмы могут предполагать создание кризисных центров ОДКБ, ШОС, а также РФ-КНР для совместного реагирования на серьезные угрозы в киберпространстве, включая атаки на критическую инфраструктуру государств-участников. Существенную роль в создании и наращивании потенциала безопасности и кибероборонны в рамках таких форматов (а также, потенциально, ЕАЭС) могут играть совместные киберучения, в том числе предполагающие сценарий международного кризиса в киберпространстве. Приоритетной задачей масштабных трансграничных учений становится демонстрация партнерам и потенциальным противникам военно-стратегического потенциала РФ в области ИТ, а также показательная отработка управления эскалацией международных кризисов в киберпространстве.

5 *Разработка мер доверия в области использования ИКТ возможна в рамках отдельных региональных форматов,* не имеющих жесткой привязки к обеспечению коллективной безопасности и единому «центру силы», но объединяющих существенное количество развитых цифровых экономик. Примером такого формата в рамках горизонта-2024 выглядит Региональный форум АСЕАН (АРФ), в число участников которого входят РФ, КНР и США. В условиях минимального доверия и ограниченного обмена информацией по вопросам военно-политического использования ИКТ АРФ может использоваться РФ как «пробная площадка» для продвижения и отработки страховочных мер кризисной коммуникации, а также более комплексных мер доверия не только среди своих евразийских партнеров, но и с США, Китаем, Японией, Австралией. В рамках деятельности на площадке АРФ разумно ориентироваться на развитую инфраструктуру национальных и частных центров реагирования на киберинциденты (CERT/CSIRT), а также государственно-частных партнерств в сфере кибербезопасности, сложившуюся в азиатско-тихоокеанском регионе.

6 *Поддержание диалога по общим интерпретациям норм международного гуманитарного права* и правилам ведения военных операций в киберпространстве представляется треком, ведущую роль в развитии которого может сыграть нейтральная международная площадка — Международный Комитет Красного Креста (МККК). Однако площадка МККК в рамках стратегии не предполагает выработки обязывающих международно-правовых документов, а используется для взаимного информирования государств о своих подходах и интерпретациях существующих норм.

7 *Радикальное наращивание собственной технологической базы цифровых активов и инфраструктур, включая КИИ, а также дублирование тех сегментов КИИ, которые не находятся в юрисдикции РФ,* однако жизненно важны для поддержания национальной экономики и обеспечения безопасности (например, система уникальных идентификаторов Интернета).

8 *Укрепление собственного оборонительного и проактивного потенциала в сфере ИКТ, в том числе за счет военно-технологического сотрудничества с технологически развитыми партнерами (КНР).* Поддержание условного аналога «паритета» в киберпространстве и страхование себя от рисков целевых атак со стороны государств и акторов-посредников потребует проактивных, упреждающих действий. Речь идет о формировании собственных баз уязвимостей в продуктах международных вендоров (включая продукцию для КИИ), постоянной «прощупывающей» активности в отношении объектов критической инфраструктуры, госуправления и военного командования потенциальных противников и собственных партнеров, осуществлении трансграничных разведывательных кибероперациях. Для инцидентов, не пересекающих порог исполь-

зования силы, приоритетный формат реагирования подразумевает ответные соразмерные действия — либо упреждающие операции, нацеленные на срыв планируемых недружественных действий.

РИСКИ стратегии включают в себя самоподдержание устойчивого состояния минимального доверия в международной системе и «гонки цифровых вооружений». Позволяя адаптировать российский внешнеполитический курс к негативному сценарию доминирования силовых механизмов над международно-правовыми в части регулирования военно-политического использования ИКТ, стратегия не открывает пути выхода из этого состояния и в долгосрочном смысле является тупиковой. Создание «страховочной сети» и обозначение порогов действий, провоцирующих эскалацию и военный ответ, не закрывает риск нарастания масштабов и интенсивности действий, не достигающих порога использования силы (государственные операции с целью хищения технологических и коммерческих секретов, нанесения финансового ущерба частным и государственным структурам, влияния на общественное мнение и вмешательства в политические процессы и проч.). В условиях стагнации либо слабого прогресса в направлении выработки международных норм и взаимных договоренностей, охватывающих действия ниже порога использования силы, высока вероятность сползания ведущих держав, включая Россию, в состояние перманентного «подпорогового конфликта» в киберпространстве.

2.2. «СТРАТЕГИЯ МАЛЫХ ШАГОВ» И МОБИЛИЗАЦИИ РЕСУРСОВ ЧАСТНОГО СЕКТОРА В УПРАВЛЕНИИ ВЫЗОВАМИ ВОЕННО-ПОЛИТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ ИКТ

В отличие от предыдущего варианта, стратегия исходит из возможности достижения существенного прогресса в формировании основ международно-правового регулирования киберпространства в среднесрочной перспективе. Это стало бы ключевым фактором снижения рисков военно-политического использования ИКТ против РФ. Внешними переменными, способными подтолкнуть ключевые группы интересов к выбору такой стратегии являются:

- Катастрофа как импульс к изменениям. Даже при реализации негативных тенденций, задающих вводные для предыдущей стратегии, возможен их разворот в результате реализации кризисного сценария. Таким сценарием может быть *а)* неконтролируемая эскалация компьютерного инцидента (в ходе военной кибероперации или действий негосударственных акторов с учетом некорректной атрибуции) до уровня серьезного международного кризиса или военного конфликта (в том числе с вовлечением в него РФ); *б)* масштабная техногенная

катастрофа с человеческими жертвами, массовым разрушением инфраструктуры, серьезным ущербом глобальной экономике или окружающей среде в результате ошибки в управлении киберфизическими системами, внеплановых последствий военной кибероперации или иного компьютерного инцидента. Международный эффект такого инцидента может стать триггером для перезапуска и активизации процесса формирования международно-правового режима ответственного поведения в сфере использования ИКТ.

- **Влияние «третьей силы» — частного сектора.** На сегодняшний день прогресс в формировании режима ответственного поведения в киберпространстве сдерживается прежде всего в силу противоречий между подходами различных групп государств (условные США-НАТО, Россия, КНР и проч.). Однако в обозримом будущем ситуация может поменяться за счет существенного повышения роли структур частного сектора. Корпорации ИТ-отрасли не могут формулировать международные нормы, однако могут самостоятельно формировать рыночные практики, стандарты и ограничения, в том числе касающиеся разработки, модификации и торговли ИТ-продукцией. При неготовности государств ограничить подпороговые кибероперации, сдержать рост компьютерных атак на КИИ именно частные компании ИТ-отрасли несут основное бремя расходов, связанное со срочным закрытием уязвимостей, использованных в атаках, обновлением уязвимого оборудования и ПО, а также заменой зараженного оборудования в случаях серьезных атак. Частный сектор также несет издержки в плане доверия и деловой репутации в тех случаях, когда его продукция компрометируется и используется в государственных операциях в киберпространстве. В итоге глобальные игроки ИТ-отрасли могут быть наиболее заинтересованы в выработке реального действующих норм, сдержек и ограничений в части военно-политического использования ИКТ. Крупные холдинги и компании, заняв консолидированную позицию, могут стать самостоятельными полноценными участниками глобального диалога о нормах поведения в области использования ИКТ и развернуть его развитие.

С учетом этих внешних переменных, стратегия РФ может *быть нацелена на формирование сетки международных норм и соглашений, охватывающих безопасность отдельных ключевых отраслей инфраструктуры*. В части реализации контроль и верификация соблюдения этих норм опираются на рыночные стимулы и ресурс государственно-частного взаимодействия.

В рамках стратегии не предполагается работы над комплексным, всеобъемлющим и обязывающим пакетом международных норм ответственного поведения в киберпространстве. В 2011 г. Россия подготовила и представила концепцию глобальной конвенции ООН об обеспечении международной информационной безопасности (МИБ), но до сих пор продвижение документа на международной арене не увенчалось серьезным успехом. Схожим образом развивается и работа над про-

движением обновленной редакции Правил поведения в области обеспечения МИБ, направленной РФ и ее партнерами по ШОС письмом Генеральному Секретарю ООН в январе 2015 г.

Меры по реализации стратегии

1 **Определение приоритетных отраслей критической инфраструктуры (КИ) и критической информационной инфраструктуры (КИИ) и реализация дипломатических инициатив по выработке норм их защиты.** Здесь потребуется учитывать следующие условия: а) в отношении выбранных объектов наиболее высоки риски военно-политического использования ИКТ; б) совместная работа над защитой объектов в наименьшей степени подвержена рискам политизации; в) для защиты объектов представляется реальным задействовать ресурсы и стимулы глобальной и российской ИТ-отрасли.

Достижимой целью в рамках такой стратегии может быть выработка в ближайшие годы сетки международных и многосторонних норм, а также закрепленных в механизмах международного частного права стандартов, требований и практик ИТ-отрасли, ограничивающих военно-политическое использование ИКТ в отношении таких категорий объектов.

Таким образом, в основу подхода к выработке норм ложится принцип защиты ключевых цифровых активов (приоритетные секторы КИИ), отвечающий на вопрос *«что мы защищаем?»*. Параллельно, подключение к процессу выработки норм ресурсов частной ИТ-отрасли дает возможность сформировать международно-правовые механизмы, вводящие ограничения на военно-политическое использование ИКТ в зависимости от последствий тех или иных действий (*«от чего мы защищаем?»*).

Для среднесрочного горизонта можно выделить как минимум три вида инфраструктуры, которые целесообразно использовать как «отправные точки» для выстраивания международно-правового режима ответственного использования ИКТ и сокращения военно-политических рисков в этой области:

1. ИТ-инфраструктура глобальной финансово-кредитной и банковской отрасли. Инициатива о разработке добровольных многосторонних норм, предполагающей отказ государств от осуществления или содействия компьютерным атакам на крупные объекты банковской инфраструктуры, уже рассматривалась в рамках ГПЭ ООН начиная с 2014 г. Идея нормы не вызывает принципиальных противоречий: банковский сектор является одной из ключевых целей компьютерных атак, осуществляемых как с коммерческой, так и с политической мотивацией. РФ также сталкивается с массированными атаками на инфра-

структуру банковского сектора, хотя большинство инцидентов связаны с киберпреступностью, а не военно-политическим использованием ИКТ. Возможное содержание нормы может быть нацелено на снижение угрозы кибератак, преследующих цель дестабилизации экономики государств через обрушение их финансовых систем. Усилия российских представителей на площадке ГПЭ ООН и иных многосторонних площадках (ОБСЕ, АРФ, БРИКС) могут быть направлены на выработку нормы, запрещающей государствам вести трансграничные атаки на ключевые объекты банковской отрасли либо содействовать им. В интересах РФ выработка классификации «ключевых» объектов: например, бирж и банков с ежедневным оборотом не менее определенной суммы, общей суммой активов или определенным числом клиентов, пользующихся услугами дистанционного банковского обслуживания (ДБО). Механизм обеспечения соблюдения нормы может быть выстроен на взаимодействии и обмене информацией между государственными и частными структурами. Речь идет об обмене данными между центрами управления информационной безопасностью (SOC) самих банков и отраслевыми CSIRT/CERT — и государственными центрами реагирования. Например, в РФ с июня 2015 г. функционирует Центр мониторинг и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) при ЦБ РФ. Частично обмен данными в рамках соблюдения нормы может быть вписан в уже существующие международные форумы и группы CERT, такие как FIRST (международный Форум команд обеспечения безопасности и реагирования на компьютерные инциденты), в котором участвуют CSIRT 17 банков. Кроме того, «техническая поддержка» принятой нормы может быть обеспечена и за счет организации схемы обмена данными об инцидентах и аномалиях трафика в банковских сетях в международном масштабе в стандартизированных форматах (например, FS-ISAC Traffic Light Protocol (TLP)).

2. Инфраструктура мирной атомной энергетики. Объекты мирной атомной энергетики, включая АЭС, все чаще становятся целями государственных кампаний кибершпионажа и киберсаботажа, что затрагивает интересы РФ как одного из лидеров на глобальном рынке атомной энергетики. Механизмы снижения рисков военно-политического использования ИКТ против объектов ядерной энергетики как раз могут включать в себя нормы об обязательном тестировании критических компонентов АСУ ТП на наличие недекларированных возможностей (НДВ), контроль целостности цепочек поставок таких компонентов с участием представителей частной отрасли, вендоров АСУ ТП и компаний сектора информационной безопасности. В интересах РФ и международного сообщества также усиление роли МАГАТЭ в предотвращении и расследовании компьютерных инцидентов на объектах ядерной энергетики. Ресурсы частного сектора, в том числе компаний отрасли ИБ, АСУ ТП и самих операторов ядерных объектов могут быть использованы для органи-

зации единой базы данных об инцидентах кибербезопасности на ядерных объектах, а также создания при МАГАТЭ единого депозитария вредоносного ПО, которое применялось для атак на ядерную инфраструктуру, с информацией об используемых им уязвимостях и возможных векторах атаки. Наконец, целесообразно привлечь частную отрасль и сконцентрировать усилия международного сообщества на задаче создания при МАГАТЭ «кризисного центра реагирования» на инциденты на ядерных объектах.

Такой центр должен быть постоянно доступен для операторов объектов и правоохранительных органов государства, на территории которого произошел инцидент. Задача центра может заключаться в предоставлении имеющейся информации об угрозе, а также консультаций по управлению инцидентом и минимизации его последствий для функционирования ядерного объекта. По сути, речь может идти о создании аналога международного CSIRT для отрасли ядерной энергетики, пользующегося авторитетом МАГАТЭ и поддержкой компаний частного сектора (возможно, на коммерческой основе за счет взносов государств-членов МАГАТЭ). В случае удачной апробации такого механизма в перспективе до 2024 г. следующим шагом может быть выдвижение РФ инициативы принятия международной нормы о запрете/ограничении государственных кибероперaций против объектов мирной ядерной энергетики.

3. Глобальная система уникальных идентификаторов Интернета (УИИ). Систему уникальных идентификаторов Интернета (УИИ) образуют три компонента: глобальная иерархизированная система доменных имен (DNS); система ресурсов нумерации Интернета (включая глобальную систему распределения IP-адресов и систему распределения и присвоения номеров Автономных Систем (ASN)); и система регистров номеров портов и параметров протоколов Интернета. Система УИИ и составляет глобальный Интернет в его прямом понимании и потому является критической информационной инфраструктурой для всех государств. За последние годы инфраструктура УИИ с возрастающей частотой подвергается мощным сетевым атакам, включая DDoS. Также ряд государств, включая РФ, высказывают опасения по поводу возможности политически мотивированного вмешательства отдельных правительств (США) в функционирование системы УИИ (например, для ограничения доступа тех или иных стран к критически важным сервисам Интернета в рамках политики международных санкций). В этих условиях интересам РФ отвечает продвижение идеи нормы, предполагающей запрет на компьютерные атаки государств и акторов-посредников на инфраструктуру УИИ, а также отказ правительств от вмешательства в технические бизнес-процессы, связанные с обеспечением работы УИИ. Такая норма — по крайней мере в узком понимании, только в части запрета компьютерных атак, — имеет высокие шансы стать точкой прорыва в заключении многосторонних соглашений по вопросам регулирования

киберпространства. Причина высоких шансов на успех в том, что в отличие от банковской и ядерной отраслей, поддержка системы УИИ — достаточно прозрачный и открытый технический процесс, за который отвечает техническое сообщество, а не правительства напрямую. В итоге, взаимодействие, сотрудничество и обмен информацией в рамках исполнения возможной нормы не потребуют от государств и частных компаний раскрытия чувствительных данных, угрожающего деловой репутации коммерческим и технологическим секретам, национальной безопасности и проч. В то же время, повышение безопасности системы УИИ напрямую отвечает интересам крупных коммерческих DNS-провайдеров и других компаний интернет-отрасли. В настоящее время идея подобной нормы уже продвигается в рамках ГПЭ ООН правительством Нидерландов, также имеются позитивные отзывы от представителей США и Германии в ГПЭ ООН. Однако для РФ пространство для маневра пока остается открытым, а развитие нормы до реального работающего глобального механизма в любом случае потребует нескольких лет работы.

2 Адаптация и развитие механизмов экспортного контроля для программно-аппаратной ИТ-продукции двойного назначения либо предназначенной конкретно для осуществления специальных операций в киберпространстве

На данный момент, наиболее перспективным образцом подхода в этой области представляются обновленные Вассенаарские договоренности (ВД) по экспортному контролю за обычными вооружениями, товарами и технологиями двойного назначения. Участниками договоренностей являются 40 государств, включая РФ. Цель соглашения состоит в повышения транспарентности и ответственности в области контроля над передачами обычных вооружений и чувствительной номенклатуры продукции двойного назначения, содействуя, таким образом, региональной и международной безопасности и стабильности. Участники ВД каждые полгода направляют в секретариат уведомления о списках обычных вооружений и продукции двойного назначения, поставленной в страны, не участвующие в договоренностях. При этом ведутся списки товаров и технологий, в отношении которых действуют ограничения на поставку третьим странам. В декабре 2013 г. в список таких товаров и технологий было добавлено ПО, использующееся для тайного сбора данных с информационных систем (кибершпионаж), а также средства для скрытного проникновения в IP-сети.

Для РФ в рамках стратегии представляется целесообразным усилить свое участие в дальнейшем развитии ВД в этом направлении — либо, если будет невозможно по политическим соображениям, способствовать развитию сходных механизмов в рамках других международных форматов (ООН, АРФ, БРИКС, ШОС). Принцип и подходы к категоризации и определению технологий и си-

стем, предназначенных для тайного сбора электронных данных и проникновения в компьютерные системы, могут быть распространены на нормы, формируемые на площадке ГПЭ с участием представителей ИТ-отрасли. В частности, целесообразно рассмотреть возможность запрета на трансграничную передачу ПО, предназначенного для неавторизованного доступа в системы АСУ ТП, а также ПО, способного уничтожать/заменять содержимое жестких дисков. Кроме того, реестры «Вассенаара 2.0» могут пополняться за счет включения в них образцов кода или технического описания модулей ПО, наиболее регулярно используемого в компьютерных атаках повышенной опасности.

3 **Разделение повестки дня информационного противоборства (информационно-психологические операции и т.н. «информационные войны») и защиты инфраструктуры в контексте выработки норм, ограничивающих военно-политическое использование ИКТ, на международных многосторонних и в двустороннем формате.**

В ближайшие годы политизация международной дискуссии и нарастание противоречий в части регулирования информационного противоборства с использованием Интернета и других каналов глобального информационного обмена выглядит высоко вероятной. Объединение вопросов военно-политического использования ИКТ в одну корзину с вопросами информационного противоборства несет риск того, что «токсичное», малопродуктивное состояние международной дискуссии об ограничении информационного противоборства сузит коридор возможностей и для обсуждения вопросов военно-политического использования ИКТ, которые не связаны с контентом. Подобного объединения предлагается избегать в рамках стратегии, проактивно формируя отдельные корзины для диалога на международных площадках и с ключевыми партнерами.

Например, применительно к общеевропейскому пространству работа над нормами, мерами доверия и иными механизмами защиты ИТ-инфраструктур может быть сконцентрирована на площадке ОБСЕ, в части технических стандартов защиты КИИ — на площадке ОЭСР, в части адаптации МГП к киберпространству — на уровне диалоговых механизмов РФ-ЕС и РФ-НАТО. В то же время, работа над ограничением «информационных войн» и операций по распространению государствами контента, угрожающего стабильности, может быть сосредоточена на площадке Совета Европы. Аналогичным образом, для эффективного развития площадки ГПЭ ООН с точки зрения интересов РФ также целесообразно не допускать размытия ее мандата за счет вопросов, связанных с регулированием контента. Разведение вопросов контента и инфраструктуры во внешнеполитическом контуре РФ потребует закрепления этого принципа и на уровне внутренних доктринальных и стратегических документов.

4 **Повышение результативности международной работы над сокращением рисков военно-политического использования ИКТ за счет создания механизмов взаимодействия межгосударственных структур и ИТ-отрасли. Обеспечение активного участия российской ИТ-отрасли в таких механизмах. В частности, повышение результативности и реального влияния площадки Группы правительственных экспертов ООН.**

Группа была создана по российской инициативе в 2001 г., Россия была и остается одним из главных генераторов инициатив в рамках ее формата, который к 2015 г. утвердился в роли ключевой площадки по разработке международных норм регулирования киберпространства. Однако на сегодняшний день нарастает риск того, что решения и нормы, вырабатываемые на международных площадках, включая ГПЭ, будут оставаться фиктивными без готовности частного сектора вкладывать ресурсы в обеспечение возможности их соблюдения.

Шаг, который может соответствовать интересам РФ в среднесрочной перспективе — создать механизм взаимодействия ГПЭ ООН и ИТ-отрасли с обеспечением активного участия российской ИТ-отрасли в этом механизме. Такое решение позволит транслировать на уровень ООН интересы российской ИТ-отрасли, где есть компании, заинтересованные и способные внести вклад в сдерживание военно-политических киберугроз.

Учет мнения глобальных ИТ-игроков позволит получить от них то видение норм и сдерживающих механизмов для военных угроз в киберпространстве, над достижением которого они сами готовы работать. Так, в нише киберфизических систем критически важных объектов (например, АСУ ТП (автоматизированные системы управления технологическим процессом) для АЭС и ПО для них) отрасль может сама принять и контролировать выполнение таких мер как контроль целостности цепочек поставок продукции, обязательное прохождение продукцией независимого тестирования на недекларированные возможности (НДВ) перед допуском до конкурса на поставку и проч. По сути, отраслевые стандарты и практики, закрепленные в корпоративных политиках, соглашениях об уровнях сервиса (SLAs) и могут стать реальным дополнением норм ГПЭ ООН, предписывающих, например, отказ государств от сбора уязвимостей и встраивания НДВ в объекты критической инфраструктуры. Но для того, чтобы мобилизовать частную отрасль ИТ на сотрудничество, нужно дать ей право голоса за глобальным столом переговоров. Таким образом необходимо развитие механизмов государственно-частного партнерства как на национальном, так и на международном уровнях.

РИСКИ стратегии связаны с возможной политизацией ее составляющих. Так, допуск частных игроков к процессу формулирования международных норм и правил поведения также может стать заложником политизации, если не удастся обеспечить региональный или национальный баланс их представительства (крен в сторону гигантов ИТ-отрасли из США). Также такая инициатива со стороны РФ может быть воспринята как новая форма протекционистской политики в нише ИТ. Другой риск связан с открытостью, которой потребует предлагаемая в рамках стратегии идея создания отраслевых норм по ключевым секторам КИИ и привнесение опыта частной отрасли в обмене данными об инцидентах в рамках инфраструктуры CSIRT\CERT. Стратегия позволяет задействовать позитивные стимулы для представителей международного сообщества и частной отрасли ИТ для разработки и имплементации норм — однако не предлагает серьезных санкций для «нечестных игроков» и нарушителей достигнутых договоренностей (кроме санкций, связанных с потерей преимуществ от участия в механизмах норм). Таким образом, для РФ существует опасность того, что данные, раскрытые в рамках двустороннего или многостороннего обмена в соответствии с нормами, выработанными на международных площадках, впоследствии могут быть использованы недобросовестным партнером в целях, угрожающих национальной безопасности. Международный режим ответственного поведения в киберпространстве слишком слабо развит, чтобы использовать эффективные механизмы санкций. Кроме того, мотивацию к недобросовестному поведению в определенной мере задает не имеющая краткосрочного решения проблема атрибуции действий в киберпространстве.

3.

ОБЕСПЕЧЕНИЕ **БЕЗОПАСНОСТИ, СТАБИЛЬНОСТИ И ОТКАЗОУСТОЙЧИВОСТИ** (БСО) ИНТЕРНЕТА И ИНФРАСТРУКТУРЫ ЦИФРОВОЙ ПЕРЕДАЧИ ДАННЫХ ДЛЯ РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ, БИЗНЕСА И ГОСУДАРСТВА

Цель:

Обеспечена и поддерживается целостность, устойчивость функционирования и безопасность единой сети электросвязи РФ, в том числе сетей связи общего пользования, в условиях наличия трансграничных рисков и угроз.

Задачи:

- Минимизация внешних трансграничных рисков функционированию инфраструктуры и сервисов сети Интернет, затрагивающих бизнес-процессы и интересы российских граждан, бизнеса и государства.

- Разработка и реализация концепции регулирования жизненно важных услуг (жизненно важных для граждан, бизнеса и государства цифровых сервисов) параллельно и независимо от развития регулирования в области защиты критической информационной инфраструктуры.

- Полноправное участие представителей государственных органов РФ, технического сообщества, а также иных заинтересованных сторон в деятельности международных рабочих процессов, форумов, технических и международных правительственных организаций по обслуживанию глобальной инфраструктуры Интернета, управлению Интернетом и стандартизации в области БСО, бесперебойности и непрерывности функционирования Интернета и других трансграничных сетей передачи данных.

В ближайшие годы в целом адекватной остается модель экстраполяции сегодняшних базовых характеристик глобальной инфраструктуры сетей связи и сетей передачи данных, в том числе глобальной сети Интернет. Радикальные технологические и архитектурные изменения в долгосрочном временном горизонте обуславливают вероятную трансформацию логики ключевых бизнес-процессов в секторе связи и ИТ. В совокупности эти изменения снижают эффективный горизонт выстраивания стратегии и делают предпочтительным фокус на среднесрочном горизонте стратегического планирования.

Наиболее вероятными и реалистичными представляются два подхода:

1. стратегия национализации трансграничных рисков (полуостров «Рунет»)

2. стратегия распределения рисков между государством и частным сектором

3.1. СТРАТЕГИЯ «НАЦИОНАЛИЗАЦИЯ» ТРАНСГРАНИЧНЫХ РИСКОВ — ПОЛУОСТРОВ РУНЕТ

Стратегия «национализации» трансграничных рисков исходит из развития сценария, предполагающего выделение целостного национального сегмента сетей связи, управление и обеспечение БСО которого осуществляются в рамках российского юрисдикции при активном участии государства. Такой подход обозначен в российских документах стратегического планирования. Он основан на представлении о том, что внешние, трансграничные риски и угрозы нарушения БСО имеют приоритет перед внутренними, и должны купироваться в первую очередь. Интернет рассматривается прежде всего, как технологическая система, которая обеспечивает связность между национальными сегментами сетей электросвязи, крупнейшие и наиболее развитые из которых (включая российский) в части контроля над физической инфраструктурой и управления рисками БСО стремятся к самодостаточности, хотя и не достигают ее полностью.

Сценарий предполагает значительную вероятность сохранения / возобновления режима санкций в отношении РФ со стороны США и государств Западной Европы.

Исходными внешними условиями служат сохранение тренда на фрагментацию киберпространства по национальным юрисдикциям и неблагоприятная внешнеполитическая конъюнктура, включая наряженные отношения с США, НАТО и отдельными государствами Европы. Ключевым внешним риском для БСО российского сегмента Интернета в этих условиях является политизация технической экосистемы глобального Интернета, в частности, нарастающее давление национальных правительств на деятельность находящихся в их юрисдикции технических и коммерческих организаций, предоставляющих различные трансграничные сервисы, в том числе связанные с обслуживанием инфраструктуры глобального Интернета. Фундаментальным риском такого процесса является снижение взаимного доверия в глобальной экосистеме технологических сервисов Интернета и частичная фрагментация такой системы по крупнейшим национальным/региональным сегментам с сопутствующим торможением развития.

Принимаются во внимание среднесрочные и долгосрочные политические риски, связанные с нахождением в юрисдикции США большей части организаций: Корпорации Интернета по распределению имен и адресов (ICANN), Общества Интернета (ISOC), Рабочей группы по проектированию Интернет (IETF), выступающей юридической оболочкой для рабочего процесса, Совет по архитектуре Интернет (IAB), а также дочерней структурой ICANN, отвечающей за распределение ресурса имен и делегирование ресурсов нумерации Региональным регистратурам Интернет (Public Technical Identifiers, PTI). Независимость этих организаций в части выполнения технических функций от влияния американской юрисдикции не является достаточной страховкой от политических рисков в условиях серьезного кризиса в отношениях РФ и США. Принимается во внимание низкий, однако неприемлемый риск распространения инструментария зарубежных санкций на деятельность технических организаций в юрисдикции США и других государств, обеспечивающих распределение и делегирование уникальных идентификаторов российским физическим и юридическим лицам.

Осуществление данной стратегии является целесообразным лишь в условиях негативных внешних сценариев, когда обеспечение безопасности является приоритетом даже ценой торможения развития ИТ-отрасли и всей социально-экономической сферы.

Управление перечисленными рисками в рамках подхода строится на обеспечении технологической и инфраструктурной самодостаточности российского сегмента Интернета в той мере, в которой это возможно. Подход не предполагает курса на выстраивание полностью автономного национального сегмента Интернета в пределах юрисдикции РФ и его изоляции от глобальной сети. Однако с точки зрения обеспечения БСО обязателен прямой контроль критически важных элементов ин-

фраструктуры, функционирование которой обеспечивает интересы и бизнес-процессы государственных структур, бизнеса и граждан.

Конечную цель в рамках подхода отражает концепция полуострова, который относительно надежно связан с материком, однако связующая территория ограничена и находится под контролем, призванным обеспечить безопасность. Ведущим субъектом и инициатором преобразований в рамках такого подхода выступает государство, которое расширяет объем и сферу своего регулирования прежде всего в части деятельности операторов связи и иных участников отрасли электросвязи.

Следует отметит, что подход некорректно позиционировать как «китайский», поскольку приоритетом является не контроль контента, передаваемого через сети связи, прежде всего через Интернет, а управление рисками на инфраструктурном уровне (физические каналы и связность, межсетевая маршрутизация трафика, система уникальных идентификаторов, распределенные платформы передачи данных).

Основные меры в рамках реализации данной стратегии:

1. *Государство осуществляет идентификацию и категорирование критической информационной инфраструктуры (КИИ) электросвязи* и разрабатывает четкую систему количественных параметров и пороговых значений для определения критически важных субъектов в отрасли связи, в том числе по критерию пропуска трансграничного интернет-трафика. Круг субъектов регулирования в полной мере охватывает частный сектор и может включать как крупных операторов связи, так и других субъектов с учетом их роли в трансграничном пропуске трафика и развитии единой топологии российского сегмента Интернета.

Возможна разработка и закрепление в федеральном законодательстве системы требований и обязательств для субъектов КИИ электросвязи для обеспечения ими повышенного уровня БСО для своей инфраструктуры. Для отдельных организаций, признанных критически важными, обеспечивается механизм прямого государственного контроля в форме государственной собственности либо юридически закрепленного участия государственных органов в принятии ключевых решений по техническим бизнес-процессам, которые обеспечивает такая структура.

2. *В отношении физической инфраструктуры, обеспечивающей глобальную связность российского сегмента Сети, ужесточается государственный контроль над пограничными переходами, используемыми операторами связи в РФ для трансграничного пропуска трафика.* Проводится курс на максимально возможное сокращение объема интернет-трафика, маршрутизация которого осуществляется между автономными системами, которые принадлежат российским субъектам, но через промежуточные узлы (АС) за рубежом.

Наращивание «вертикальной» связности в пределах национального сегмента Интернета, а также ключевых интеграционных объединений с участием РФ за счет инвестирования ресурсов в развитие инфраструктуры крупнейших национальных операторов связи. Параллельной вспомогательной стратегией является укрепление регионального инфраструктурного присутствия российских игроков, в том числе опосредованно контролируемых государством. Оптимальный результат такой работы — трансформация региональной топологии и карты связности в рамках магистральных каналов с целью повышения ее зависимости от высокоскоростной инфраструктуры российских операторов связи в части трансграничного пропуска трафика.

В отношении операторов и провайдеров трансграничного доступа к Сети государство настаивает на создании ими представительств в юрисдикции РФ. Реализация такого механизма возможна путем продвижения модели государственно-частных партнерств. Подобные ГЧП могут быть ориентированы прежде всего на обеспечение беспроводного доступа для жителей российских регионов, где широкополосный доступ не обеспечен, а современная высокоскоростная инфраструктура не развита либо отсутствует.

3. *Государство во взаимодействии с операторами связи создает дублирующие базы данных и обеспечивающее их работу оборудование (серверы) для элементов системы DNS, используемых российскими пользователями, бизнесом и государственными органами.* Сюда входят адресные зоны DNS первого уровня .RU и .РФ , а также иные зоны первого уровня, связанные с Российской Федераций или ее субъектами. Такие базы данных и оборудование должны иметь функцию автономного функционирования и поддержания доступа к ресурсам DNS для российских пользователей в случае чрезвычайных ситуаций — в т. ч. нарушения функционирования глобальной системы DNS.

Обеспечивается создание аналогичных баз данных и поддерживающего их оборудования для получения информации о делегировании ресурсов нумерации российским юридическим и физическим лицам, а также маршрутно-адресной информации о пропуске трафика в российском сегменте Интернета.

4. *На основе дублирования баз данных о ресурсах нумерации и пропуске трафика, описанных выше, возможно также создание единой системы мониторинга маршрутизации трафика в пределах российского сегмента Интернета.* Такая технологическая система может быть создана крупнейшими операторами связи и добровольно пополняться всеми участниками рынка пропуска интернет-трафика с целью предоставить каждому ее участнику максимально полную информацию о доступных альтернативных маршрутах пропуска трафика. Доступ к полной картине маршрутизации интернет-трафика в Рунете поможет выявить участки сети со слабой связностью и более эффективно реагировать на DDoS-атаки и аномальные нагрузки, а также

идентифицировать критические точки (bottlenecks) российского сегмента Сети. В настоящее время создание такой системы уже предлагается Минкомсвязи России, но для эффективного функционирования система должна наполняться таким количеством и выборкой данных, которые будут давать участникам рынка пропуска трафика необходимую «глубину» и детализацию картины связности в пределах Рунета для принятия оптимальных решений. При этом государство может оставлять за собой функцию вмешательства в пропуск трафика операторами связи в РФ, используя данные из системы для направления указаний о выборе оптимальных маршрутов операторам связи. Такой функционал может применяться в случае глобальных нарушений маршрутизации трафика в Интернете, как в результате сбоев и технических ошибок, так и намеренных воздействий.

Активное вмешательство государства в процессы маршрутизации трафика неизбежно затрагивает бизнес-процессы операторов связи, так как пропуск трафика осуществляется прежде всего из оптимальных параметров с точки зрения себестоимости. Таким образом, инвестирование в обеспечение БСО идет за счет сокращения доходов и ресурсов операторов связи, что накладывает ресурсные ограничения.

5. *Для проработки дальнейших возможностей повышения БСО Рунета на уровне маршрутизации интернет-трафика могут быть созданы механизмы, которые позволят не только агрегировать полные данные о пропуске трафика в рамках общей системы, но и удостоверять их аутентичность.* Одним из вариантов обеспечения таких возможностей является инвестирование ресурсов государства и технического сообщества в проработку программных надстроек, обеспечивающих криптографическое подтверждение аутентичности маршрутно-адресной информации. Перспективные проработки в данном направлении уже ведутся на площадке Рабочей группы по проектированию Интернета (IETF).

6. В отношении участия правительства и технического сообщества РФ в рабочих процессах, связанных с обслуживанием глобальной инфраструктуры Интернета, задачи ставятся исходя из низкого уровня доверия к существующей экосистеме технических организаций. В ближайшие годы в рамках данной стратегии потребовалось бы оказывать давление на существующую экосистему технических структур, основанную на концепции участия всех заинтересованных сторон в рамках некоммерческих технических организаций (ISOC, ICANN, PTI и проч.) с целью решения локальных задач и получения преференций сугубо в рамках действующей экосистемы управления Интернетом.

В среднесрочной перспективе внешнеполитические и иные ресурсы РФ в этом смысле весьма ограничены и пропорциональны участию представителей российского сообщества в технических рабочих процессах — например на площадке IETF. Поэтому инициативы РФ не могут выступать триггером глобальных изменений —

реалистичным потолком в этой связи видится активная деятельность в рамках существующей экосистемы (ICANN-PTI-ISOC) с целью решения локальных задач и получения преференций сугубо в ее рамках. Исключения, предоставляющие более широкие окна возможностей, крайне ограничены.

Одним из них может быть *инициатива по созданию новой региональной структуры распределения ресурса нумерации, отражающей потребности сообщества и государств того или иного региона, включающего РФ* (например, Региональной регистратуры Интернет-сообщества государств ЕАЭС/ШОС). Такой шаг может обеспечить опосредованный контроль РФ над политиками делегирования и контроля использования ресурсов нумерации российским физическим и юридическим лицам.

В долгосрочной перспективе развитие принципиально новых децентрализованных архитектур, платформ и систем цифровых уникальных идентификаторов могло бы стать основой совместного проекта РФ с ресурснообеспеченными и технологически развитыми государствами, заинтересованными в создании альтернативных систем для обеспечения самодостаточности собственных сегментов сетей передачи данных. Однако вовлечение в такие проекты с высокой вероятностью будет нести риск впадения РФ в зависимость от технологически и экономически более развитого партнера, а точнее его ИТ-рынка, так как создание альтернативных «корней» системы уникальных идентификаторов влечет фрагментацию глобальной онлайн-экономики и интернет-бизнеса. Так, примерное моделирование такого проекта в рамках партнерства России с КНР показывает крайне высокую вероятность практически полного замыкания российской интернет-отрасли на рынок партнера с ее последующим поглощением и переводом в статус сателлита.

РИСКИ варианта стратегии «национализации трансграничных рисков» в основном связаны с возможностью снижения конкурентоспособности представителей отрасли связи на глобальном рынке, а также общим увеличением административной нагрузки на отрасль, прежде всего на организации, обслуживающие инфраструктуру, относимую к критически важной (доменные зоны .RU, .РФ, точки обмена трафиком, сети крупнейших операторов, информационные системы крупнейших ОРИ и проч.). Специфические риски связаны со сценарием государственного вмешательства в технические бизнес-процессы операторов связи с целью обеспечения БСО Рунета. Россия находится на первом месте по количеству автономных систем среди национальных сегментов Интернета, а значит управлять ГИС, аккумулирующей данные от всех сетей, будет непросто — необходима база с обширными данными, которую необходимо обновлять в режиме, приближенном к реальному времени.

С принципом обязательного распространения российской юрисдикции на инфраструктуру, поддерживающую критически важные / жизненно необходимые сервисы для российских пользователей связан и риск ужесточения контроля над транс-

граничными переходами на сетях операторов связи, а также введения ограничений на маршрутизацию трафика через зарубежные узлы. Такие меры с инженерной точки зрения представляют собой централизацию систем и их архитектуры, в том числе за счет ограничения их распределенности. Подобный архитектурный принцип позволяет решить проблемы БСО с краткосрочной точки зрения, однако в фундаментальном плане неизбежно снижает устойчивость системы и ведет к росту риска «каскадных эффектов». Иными словами, ограничение связности за счет отсечения части трансграничных маршрутов и физических каналов как потенциально небезопасных неизбежно ведет к росту рисков, обусловленных наличием единых точек отказа в системах и деградацией связности с точки зрения топологии.

Наконец, наиболее фундаментальный риск связан с тем, что регулирование инфраструктуры передачи данных в рамках концепции национального сегмента как географически определенной юрисдикции способно затормозить развитие цифровой экономики РФ за счет запрета/консервативного регулирования распределенных технологий и сервисов нового поколения. Такой риск создает угрозу позициям РФ на глобальном рынке высокотехнологичных экономик, и, с учетом полной цифровизации глобальной экономики будущего может вести к замедлению социально-экономического развития РФ в целом.

С учетом озвученных выше рисков, подход выглядит целесообразным лишь в условиях максимально негативных внешних сценариев, когда обеспечение безопасности является приоритетом даже ценой торможения развития ИТ-отрасли и всей социально-экономической сферы.

В нейтральных либо благоприятных внешних условиях такой подход не является оптимальным. С точки зрения требуемых ресурсов подход реалистичен лишь при форсированном сценарии с эксплуатацией благоприятной внешней конъюнктуры цен на углеводородное сырье и активацией новых внутренних драйверов роста экономики РФ. При этом сам по себе подход не способствует росту, ставя во главу угла императив безопасности.

3.2. РАСПРЕДЕЛЕНИЕ РИСКОВ МЕЖДУ ГОСУДАРСТВОМ И ЧАСТНЫМ СЕКТОРОМ И «РАЗМЫВАНИЕ» КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР

Важными условиями реализации подхода является отсутствие крупных внешнеэкономических шоков, сопоставимых по масштабам с финансово-экономическим

кризисом 2007-2009 гг. и новых масштабных международных конфликтов, удержание отношений с ключевыми акторами (США, ЕС, КНР) от серьезной деградации. При этом допустимо и вероятно сохранение нынешних региональных очагов нестабильности и турбулентности в отношениях РФ с США и отдельными государствами Европы.

Риски государства и частной отрасли в плане обеспечения БСО инфраструктуры электросвязи и сетей передачи данных распределяются, исходя из различий в базовых приоритетах каждого из этих акторов. Отрасль электросвязи и интернет-отрасль РФ в подавляющем большинстве состоит из частных игроков, что вполне соответствует мировой практике. В то же время, выполнение функций государственных органов исполнительной власти в России также обеспечивается за счет сложного и развитого комплекса инфраструктур электросвязи, в том числе информационных систем, информационно-телекоммуникационных сетей и конкретно сети Интернет. Однако карта рисков БСО и базовые потребности в этой области у государства и частной отрасли отличаются, что дает возможность сформулировать для каждого из этих субъектов собственные стратегии и задачи.

Одной из ключевых проблем на сегодняшнем этапе развития госрегулирования Рунета выглядит отсутствие у самого регулятора четких ориентиров и понимания того, где пролегают границы его собственных интересов и необходимого участия в обеспечении безопасного функционирования цифровых сервисов.

Преобладает стремление государства напрямую охватить и предметно урегулировать все сферы отношений, бизнес-модели и процессы интернет-отрасли для нивелирования рисков и вызовов безопасности. Однако такой подход в значительной степени носит компенсаторный характер — государство форсированными темпами закрывает разрыв, образовавшийся за вторую половину 1990-х гг. и 2000-е гг. в результате бурного развития отрасли электросвязи и инфраструктуры интернет-сектора на территории РФ в условиях почти полного отсутствия регулирования в области БСО либо его точечного, «лоскутного» характера. К настоящему моменту «разрыв» преимущественно преодолен, а отдельные нормативно-правовые инициативы носят явно опережающий характер по отношению к технологическим и экономическим возможностям отрасли («пакет Яровой»). Таким образом, на ближайшую перспективу просматривается вероятность завершения цикла «компенсирующей гиперактивности» регулятора и выравнивания инициативы между государством и отраслью.

Разведение повестки дня и карты рисков в области обеспечения БСО выглядит своевременным вариантом проактивной стратегии, которая позволит избежать избыточной регулирующей нагрузки на отрасль и, с другой стороны, позволит государству

более четко идентифицировать свои собственные приоритеты в плане обеспечения БСО цифровых инфраструктур и сконцентрировать ресурсы на их обеспечении.

Краткая формула такого подхода звучит следующим образом: государство определяет инфраструктуры и бизнес-процессы, БСО которых критически важна для его собственных функций (в том числе для обеспечения национальной безопасности в целом), оставляя отрасли ИТ и связи пространство для маневра в управлении частными рисками — в том числе и трансграничными рисками БСО отдельных субъектов и цифровых инфраструктур — в пределах общего рамочного регулирования.

В отличие от концепции «полуострова Рунет», ставка делается на обеспечение БСО через децентрализацию ключевых элементов инфраструктуры, наращивание связности за счет использования дублирующих каналов и альтернативных маршрутов, деконцентрацию узлов, которые потенциально могут выступать в качестве «горловин» (bottlenecks) и точек отказа (points of failure) в случае кризисов, сбоев и иных сетевых инцидентов, способных затронуть всю сеть электросвязи или ее крупные и критически важные сегменты. Идея подхода может быть определена как «размывание», рассредоточение КИИ сетей электросвязи до статуса некритической. Основным механизмом при этом выступает резервирование ресурсов (resource overprovisioning) и наращивание связности, в том числе количества связующих каналов, инфраструктурных провайдеров РФ как между собой, так и с трансграничными инфраструктурами. При этом повышение БСО сетей связи обеспечивается как на уровне топологии физических каналов связности, так и маршрутизации трафика и укрепления интеграции сетевой инфраструктуры Рунета с глобальной системой УИИ и ее инфраструктурой.

В ближайшие годы предлагаемые в рамках подхода меры будут сконцентрированы в большей степени на инфраструктуре и архитектурах, составляющих основу сетей в РФ и в мире на сегодняшний день (ВОЛС, система УИИ в ее сегодняшнем виде).

Для более отдаленного горизонта актуальными становятся меры, направленные на реализацию проектов на основе распределенных платформ и альтернативных каналов передачи данных, в т.ч. глобальной инфраструктуры высокоскоростного беспроводного доступа (WWAN и проч.).

В сумме подход определяет идея о том, что наращивание связности и степени интеграции инфраструктуры Рунета в глобальную инфраструктуру Интернета (и в перспективе иных сетей передачи данных) и вытекающий из этого «перенос» рисков в области БСО с национального на глобальный уровень обеспечивает преимущество по сравнению с попыткой монопольного управления рисками в рамках национального сегмента сетей электросвязи и в пределах тех ресурсов, которые доступны государству и отрасли в РФ.

В соответствии с концепцией разведения рисков и повестки дня в области обеспечения БСО между государством и частным сектором агентами этих изменений выступают по большей части игроки частного сектора телекоммуникаций и ИТ. Подход позволяет учитывать интересы частной отрасли как в плане безопасности, так и с точки зрения оптимизации и конкурентного развития их трансграничных бизнес-процессов. При этом за счет реализации интересов государства в области БСО, идентификации государственного сегмента КИИ электросвязи и концентрации ресурсов государства на обеспечении БСО государственного сегмента КИИ, актуальной становится выработка альтернативной модели регулирования для частной отрасли, определяющей рамочные нормы, меры и требования в части БСО и предоставляющей частным игрокам коридор возможностей для определения своей роли, политики и интересов в этой сфере с учетом самостоятельного несения ими основного бремени рисков.

Стимулом для продвижения предлагаемых изменений выступает высвобождение ресурсов для проведения активных политик в области обеспечения БСО инфраструктуры электросвязи. Для государства высвобождение ресурсов обеспечивается за счет уточнения сферы его ответственности и частичного делегирования рисков сектора ИТ и телекоммуникаций его же субъектам. Для отрасли вспомогательным стимулом может выступать оптимизация принятого на сегодня регулирования в сфере безопасности, сочетающего риски избыточной ресурсозатратности и низкой эффективности.

Наконец, в части участия государства и других заинтересованных сторон в международных рабочих процессах, диалоговых площадках, деятельности международных, в том числе технических организаций в рамках задач по обеспечению БСО подход предлагает сохранение статус-кво в среднесрочной перспективе и открытость к участию в выработке новых площадок и переформатированию существующих в дальнейшем. Необходимо по возможности избегать политизации и «поляризации» повестки дня, рассматривая и продвигая вопросы обеспечения БСО в качестве сугубо технической и бизнес-задачи.

Основные предлагаемые в рамках подхода шаги и меры:

1. ***Смещение фокуса от концепции национального сегмента Интернета к государственному сегменту Интернета*** в управлении трансграничными рисками БСО. В настоящий момент подход, формирующийся в рамках последней волны стратегических документов (Доктрина ИБ РФ, государственная программа «Информационное общество до 2020 г.» и др.) предполагают центральную роль государства в управлении рисками БСО в масштабах всего национального сегмента Интернета в РФ. В национальный сегмент при этом включаются все информационные системы, сети и иные инфраструктуры отрасли электросвязи в российской юрисдикции, опе-

раторами которых является как государственные органы, так и частные субъекты. Такой подход несет двоякий риск перенапряжения и чрезмерного рассредоточения государственных ресурсов в рамках стратегии комплексного управления рисками БСО, а также ограничения инициативы и угнетения драйверов роста частной отрасли связи и ИТ вследствие негибкого регулирования. В рамках рассматриваемого подхода предлагается осуществить перенацеливание государственной политики в области обеспечение БСО на круг объектов и инфраструктур, бизнес-процессы которых критически важны для обеспечения базовых функций самого государства в сфере обеспечения безопасности, обороноспособности и реализации управленческих функций, таких как предоставление услуг гражданам и бизнесу, взаимодействие государственных органов между собой и информирование населения.

Решение этой задачи обеспечивается за счет *идентификации и нормативного закрепления понятия российского государственного сегмента единой сети электросвязи и Интернета.* Техническая реализация концепции государственного сегмента возможна за счет инфраструктурной интеграции и обеспечения прямой связности между информационными системами, сетями связи специального назначения, выделенными сетями связи и иной информационной и телекоммуникационной инфраструктурой государственных органов. На сегодняшний день сегменты сетей электросвязи российских государственных органов по большей части не интегрированы на уровне общей физической инфраструктуры, архитектуры информационных систем и сетей. Существующее понятие государственного сегмента сети Интернет относится к инфраструктуре ведомственного уровня, которая включает сети связи и информационные системы ФСО (согласно Указу Президента РФ от 17 марта 2008 г. N 351, Указу Президента РФ от 22 мая 2015 г. N 260 и ряду других документов). Принятые НПА обязывают до конца 2017 г. подключить к государственному сегменту (краткое наименование RSNet) свои информационные системы и сети Администрацию Президента, Аппарат Правительства и Следственный комитет РФ, ФОИВ и органы исполнительной власти субъектов РФ.

В рамках предлагаемого подхода предлагается существенно форсировать создание государственного сегмента Интернета, расширив и сместив его функции в сторону обеспечения БСО инфраструктуры электросвязи в общегосударственном масштабе, в т.ч. для более эффективного управления трансграничными рисками БСО. Такой подход потребует не только подключения систем и сетей государственных органов к оператору госсегмента, но и создания единой интегрированной инфраструктуры такого сегмента, начиная с уровня физических каналов и линий связи, а также стандартизации оборудования и обмена данными между его участниками. Для обеспечения единой инфраструктурной базы и связности в масштабе РФ к развертыванию единого государственного сегмента может быть подключен и Ростелеком как «национальный чемпион» — магистральный телекоммуникационный оператор с государственным участием, который уже предоставляет инфраструктуру для

ряда государственных проектов и сервисов (создание и развитие инфраструктуры электронного правительства, включая портал госуслуг; телекоммуникационное обеспечение избирательного процесса — функционирование ГАС «Выборы», организация системы видеонаблюдения за выборами; выделение сегментов для государственных киберучений и проч.).

Следует отметить, что как намеченная сегодня, так и предлагаемая в рамках настоящего исследования концепция государственного сегмента Интернета (электросвязи) не затрагивает военные сети связи в управлении Минобороны, которые с конца 2016 г. уже объединены в физически отделенный от единой сети электросвязи Закрытый сегмент передачи данных (ЗСПД).

Создание и развертывание единого государственного сегмента электросвязи и Интернет в рамках предлагаемого подхода служит решению нескольких задач.

Во-первых, государство, формируя на уровне ведомственной конфигурации и — что не менее важно — инфраструктуры собственный сегмент в единой сети электросвязи РФ, получает возможность более четко определить, что для него самого является критической информационной инфраструктурой связи и на чем следует сконцентрировать усилия и ресурсы в плане обеспечения БСО. Во-вторых, интеграция систем и сетей ряда госорганов в госсегмент с единым периметром, стандартами и процедурами безопасности может сама по себе способствовать повышению его БСО. В-третьих, развертывание государственного сегмента с единым оператором поможет снизить имеющую место межведомственную конкуренцию за ресурсы на развитие собственных сегментов сети связи и обеспечение их безопасности.

Ключевой долгосрочный результат — разграничение повестки дня государства в области защиты его собственной критической инфраструктуры электросвязи от обеспечения БСО Рунета в целом. Базовый принцип при этом — те инфраструктуры и акторы, которые напрямую не отнесены к госсегменту, остаются вне его, не только формально, но и в плане методологии и подхода к обеспечению БСО. Таким образом, для государства развертывание единого государственного сегмента электросвязи и Интернета позволяет сконцентрировать внимание и ресурсы на защите активов, критически важных для его собственных функций, и избежать ресурсного и регуляторного перенапряжения, которым чревато прямое участие в обеспечении БСО всего национального сегмента Интернета. Часть рисков и задач при этом в рамках рамочного регулирования «перекладывается» на операторов вне государственного сегмента — т.е. в основном на частную отрасль, прежде всего телекоммуникационных операторов. Для последних такой подход дает возможность гибкого управления трансграничными рисками БСО без понижения эффективности их бизнес-модели и конкурентных позиций на рынке трансграничных услуг связи и передачи данных.

При этом внутри госсегмента могут быть реализованы практически все меры и программы, предусмотренные в предыдущем сценарии: обязательное управление маршрутизацией трафика через оператора государственной информационной системы (ГИС), дублирование баз данных уникальных идентификаторов и создание автономных серверов, поддерживающих предоставление услуг ресурса имен (DNS) и, в перспективе, нумерации, на случай кризисных ситуаций, контроль подключений госсегмента к узлам сетей связи общего пользования, обязательные меры по обеспечению и резервированию межсетевой связности и проч. Однако везде, где возможно, такие меры распространяются только на инфраструктуру организаций, непосредственно включенных в государственный сегмент Интернета (электросвязи).

2. ***Рамочное регулирование, основанное на концепции жизненно важных услуг для субъектов отрасли телекоммуникаций и ИТ, которые не входят в государственный сегмент, но также формируют единую сеть электросвязи РФ*** (операторы сетей связи общего пользования, точки обмена трафиком, контент-провайдеры со своей инфраструктурой и проч.). Для управления рисками БСО предлагается рамочное регулирование, основанное на концепции жизненно важных услуг (ЖВУ, essential services). Понятие ЖВУ, адаптированное к регулированию отрасли ИТ и связи в ЕС в 2005-2016 гг., предлагает более гибкую альтернативу концепции управления рисками БСО по сравнению с регулированием критической информационной инфраструктуры. Регулирование КИИ, в том числе в отрасли связи, активно разрабатывается в настоящее время. Однако здесь решаются вопросы не обеспечения БСО, а более узкого и специфического параметра безопасности — защиты КИИ от компьютерных атак и управление иными компьютерными инцидентами на таких объектах. Очевидна потребность в разработке системы обеспечения БСО единой сети электросвязи РФ и Рунета. Такая система должна складываться как из государственных норм, так и из практик и политик частных операторов, в том числе в отношении трансграничных рисков.

Для ЖВУ «точкой отсчета» выступают бизнес-процессы массовых потребителей тех или иных услуг (сервисов), предоставляемых через инфраструктуру электросвязи — в отличие от КИИ, где критическая важность определяется по отношению к безопасности государства и общества в целом, обеспечению функциональности государственного механизма и реализации управленческих функций, поддержанию социальной стабильности и проч. Критерием жизненной важности услуги (сервиса) выступает количество ее пользователей, а также вклад данного сервиса в обеспечение и поддержание пользовательских бизнес-процессов, будь то граждане или юридические лица. Таким образом, к операторам ЖВУ могут быть причислены контент- и сервис-провайдеры, телекоммуникационные (в т.ч. мобильные) операторы, сети распределенной доставки контента (CDNs), точки обмена трафиком, дата-центры и сервисы распределенного (облачного) хранения и обработки данных, удостове-

ряющие центры (УЦ), поддержка и хостинг доменов и др. Роль операторов ЖВУ в обеспечении социальных и экономических интересов общества и государства различна, однако жизненно важными их делает именно критическая масса потребителей их услуг (например, доля от экономически активного населения страны либо суммарная доля юрлиц-клиентов в ВВП).

Разница между регулированием единого госсегмента и его КИИ и, с другой стороны, операторов ЖВУ в рамках предлагаемого подхода в том, что ключевой задачей для операторов ЖВУ является непрерывность их предоставления. При этом существенная часть таких услуг изначально является трансграничной, а в будущем трансграничными станут почти все потенциальные ЖВУ (выпуск цифровых сертификатов удостоверяющих центров, доставка контента, облачное хранение и обработка данных, обмен трафиком, поддержка резолверов и авторитативных серверов DNS и проч.). Таким образом, базовый принцип обеспечения БСО для операторов ЖВУ, в отличие от участников единого госсегмента электросвязи, не допускает отключения их сервисов и инфраструктуры от глобальных сетей передачи данных — в том числе от Интернета. Бизнес-процессы, необходимые для оказания ЖВУ, должны поддерживаться при любых условиях — а значит, должна обеспечиваться трансграничная передача данных даже в условиях внешних рисков и угроз БСО. Оказание ЖВУ за редким исключением нельзя замкнуть в пределах РФ даже в случае чрезвычайных ситуаций — можно лишь прекратить оказывать их, что ударит по пользователям.

Соответственно, для регулирования ЖВУ, операторы которых преимущественно принадлежат к частному сектору (могут быть и исключения наподобие портала госуслуг и иных государственных сервисов), в среднесрочной перспективе может быть выстроена гибкая рамочная модель, сочетающая государственное регулирование с саморегулированием и формированием отраслью лучших практик. Государство устанавливает базовые рамочные критерии отнесения тех или иных субъектов к операторам ЖВУ (категорирование по видам услуг и оценка по количественным параметрам деятельности). Однако точные параметры и значения критериев определяются с учетом мнений в отрасли, что в ряде случаев позволяет субъектам самим решать, декларировать ли себя как оператора ЖВУ или нет. Регуляторы также устанавливают рамочные требования и обязательства операторов ЖВУ в части резервирования ресурсов модернизации инфраструктуры, аудита и оценки защищенности и иных мер по обеспечению БСО, в том числе в условиях внешних рисков и угроз. Однако конкретную карту рисков БСО и программу управления ими каждый оператор ЖВУ определяет опять же самостоятельно с учетом особенностей своих бизнес-процессов и инфраструктуры. Операторы ЖВУ могут пользоваться сервисами и функциями, предусмотренными для госсегмента (служба управления маршрутизацией трафика), но не обязаны делать этого.

Важно отметить, что соблюдение повышенных требований в части БСО, резервирования ресурсов и наращивания инфраструктуры в рамках такого регулирования может рассматриваться в качестве «входной платы» для зарубежных инфраструктурных и контент-провайдеров, желающих расширять свое присутствие на российском рынке, при условии либерализации и снижения иных барьеров к доступу на него (получение лицензии оператора связи, запретительное регулирование аудиовизуальных сервисов, выборочная интерпретация норм ФЗ-242 о локализации обработки персональных данных и проч.). Таким образом, может быть сформирована модель, стимулирующая инфраструктурную модернизацию российской отрасли электросвязи: крупные иностранные игроки допускаются на рынок РФ на относительно мягких условиях в плане лицензирования, сертификации и налогового режима, однако подпадая под статус операторов ЖВУ, должны вкладывать ресурсы в резервирование и наращивание своей инфраструктуры на территории РФ — или, в рамках партнерства, активов местных инфраструктурных провайдеров, которыми они пользуются для доставки своих сервисов клиентам на территории страны.

В технологическом плане управление трансграничными рисками БСО частных операторов, не включенных в единый госсегмент Интернета (электросвязи), основывается на стратегии децентрализации инфраструктуры и «размывания» потенциальных точек отказа. Такая стратегия включает в себя:

- установку множественных инсталляций оборудования, поддерживающего инфраструктуру уникальных идентификаторов (установка «зеркал» корневых серверов DNS на сетях операторов связи и точек обмена трафиком (IXP)), развитие глобальной инфраструктуры серверов DNS верхнего уровня, поддерживающих российские домены;

- наращивание точек присутствия (points of presence, PoPs) в зарубежных телехаузах, а также на инфраструктурных узлах зарубежных точек обмена трафиком;

- маршрутизацию интернет-трафика с учетом критерия устойчивости и наличия резервов у канала, который используется для пропуска трафика, даже если такой канал предоставляют зарубежные операторы;

- развитие сервисов обработки и обмена данными на базе распределенных архитектур (включая блокчейн — например, проработка возможностей развертывания сервисов DNS на блокчейне);

- развитие трансграничной инфраструктуры дата-центров;

- резервирование, дублирование и наращивание количества физических каналов связности с глобальным Интернетом (что потребует облегчения регулирования

в части обустройства и использования трансграничных переходов операторами связи).

Отдельно необходимо отметить, что разведение моделей регулирования единого государственного сегмента электросвязи и частной отрасли телекоммуникаций и ИТ, включая частных операторов ЖВУ, создает базу для активного включения российской частной отрасли в реализацию транснациональных проектов по обеспечению глобального доступа и развертыванию параллельных Интернету глобальных децентрализованных сетей передачи данных, особенно в долгосрочной перспективе. В отличие от предыдущего подхода, речь не идет лишь о механизме ГЧП с обязательным созданием представительств иностранных субъектов в российской юрисдикции — возможно и прямое партнерство российских операторов связи и контент-провайдеров с зарубежными и международными операторами таких проектов.

РИСКИ подхода связаны, в частности, со сложностью преодоления межведомственных противоречий и ресурсной конкуренции в части создания интегрированного госсегмента Интернета (сети электросвязи). Практическую сложность представляет собой выбор «инфраструктурного провайдера» для развертывания единого госсегмента Рунета. Наиболее подходящим кандидатом на эту роль выглядит Ростелеком, однако с учетом его роли в обеспечении связности в РФ, статуса магистрального провайдера и кандидата в клуб Tier 1, инфраструктура Ростелекома не может быть полностью отнесена к госсегменту. Возможен вариант, при котором координатор госсегмента привлекает Ростелеком в качестве инфраструктурного подрядчика к его развертыванию, поддержке и обслуживанию, при этом часть инфраструктуры Ростелекома рассматривается как КИИ электросвязи, в то время как отдельные сервисы оператора могут подпадать под регулирование в области ЖВУ.

В будущем при анализе рисков на первый план выйдет потенциальная сложность поддержания и обеспечения эффективности работы инфраструктуры «отдельного» госсегмента в условиях нарастающей децентрализации сетей информационного обмена, их конвергенции и взаимопроникновения на уровне инфраструктуры. Отсутствие адаптации единого госсегмента как концепции и как технологической системы электросвязи к этим изменениям может повлечь его технологическую консервацию, снижение эффективности в условиях технологически изменившихся вызовов БСО. Для нивелирования этого риска потребуется поэтапная технологическая модернизация единого госсегмента и, возможно, его частичная интеграция с новым поколением сетевой инфраструктуры частной отрасли.

Что касается рисков с точки зрения предложений для частной отрасли, здесь главным опять же является сопротивление такому подходу со стороны ряда государственных органов, желающих расширить или по крайней мере сохранить объем своих регулирующих функций.

Еще одним риском для реализации подхода в отношении частной отрасли и воплощения регуляторной концепции ЖВУ выступает дефицит свободных ресурсов у участников отрасли телекоммуникаций и ИТ на выполнение требований по обеспечению БСО их информационных систем, сетей и иной инфраструктуры. Нейтрализация риска потребует высвобождения ресурсов отрасли. Одним из инструментов для этого выступает заложенная в подходе либерализация регулирования в части развития трансграничных инфраструктурных проектов, обустройства трансграничных переходов и проч. В ближайшие годы не менее значимым средством высвобождения ресурсов может стать коррекция (оптимизация) регулирования, требующего от операторов связи и организаторов распространения информации в сети Интернет (ОРИ) чрезмерных затрат, угрожающих развитию отрасли. Таких затрат (в размере до 2,2 трлн руб. до 2021 г.) требует реализация антитеррористических НПА, обязывающих участников рынка хранить пользовательский интернет-трафик (принятый в 2016 г. «пакет Яровой»). Несмотря на то, что предметная область регулирования в рамках «пакета Яровой» не связана с обеспечением БСО, принятые НПА все же оказывают влияние на эту область. Во-первых, изъятие у операторов связи свободных ресурсов уже к 2020 г. рискует повлечь коллапс инвестиций в модернизацию, обновление и наращивание магистральной инфраструктуры связи — что несет прямые риски БСО сети электросвязи РФ. Во-вторых, формирование, по сути, параллельной канальной инфраструктуры для съема трафика с сетей связи и его передачи в центры обработки данных представляет собой парадокс с точки зрения обеспечения БСО: несмотря на удвоение инфраструктуры, роста БСО не происходит в силу различного функционального назначения каналов связи и невозможности эффективно использовать созданную под «пакет Яровой» параллельную канальную инфраструктуру для резервирования основной. В итоге, в рамках подхода дополнительным пунктом в повестке дня может быть серьезная оптимизация «пакета Яровой» с учетом лучших практик и соображений практической эффективности (например, хранение операторами связи и организаторами распространения информации только метаданных).

4.

ОБЕСПЕЧЕНИЕ РОССИЙСКИХ ИНТЕРЕСОВ В СФЕРЕ БЕЗОПАСНОЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ, БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ, А ТАКЖЕ РАЗВИТИЯ ТЕХНОЛОГИЙ И РЫНКА ИБ

Цель:

- Наличие эффективного механизма международного взаимодействия в сфере борьбы с компьютерной (высокотехнологичной) преступностью, включая механизмы трансграничного обмена информацией о компьютерных инцидентах, общие нормативные рамки для трансграничного сотрудничества.

- Высокий уровень развития и конкурентоспособности российской отрасли информационной безопасности (ИБ) на уровне глобальных лидеров.

- Обеспечение безопасности на уровне регулирования, технологий и стандартов в процессе цифровой трансформации экономики РФ и ЕАЭС.

Речь может идти о проработке следующих направлений:

А Обеспечение ИБ в рамках создания гармонизированного правового пространства ЕАЭС, ориентированного на внедрение и перспективных цифровых технологий, и новой цифровой инфраструктуры (НЦИ: промышленный Интернет

вещей (IoT), промышленное и бытовое применение ИИ, системы интеллектуального частного и общественного транспорта, сделки на распределенных реестрах, формирование и использование 3D-моделей в аддитивных производственных технологиях и проч.).

Б Высокий уровень компьютерной грамотности и культуры ИБ среди пользователей ИТ (end-users), бизнеса и государственных служащих РФ и государств-партнеров ЕАЭС с целью снижения рисков ИБ, обусловленных человеческим фактором. Формирование модельных норм, гармонизация национальных законодательств и продвижение отраслевых практик в области специализации кадровой политики организаций с учетом рисков и задач обеспечения ИБ, в том числе создания обязательных позиций и структурных подразделений по обеспечению сетевой безопасности и ИБ. Модернизация систем высшего и среднего профессионального образования для подготовки новых кадров, специализирующихся в области ИБ, с учетом междисциплинарного измерения проблемы и опережающего развития ИТ по отношению к внедрению ИБ.

Для движения к обозначенным целям могут быть идентифицированы следующие развилки:

1. Противодействие киберпреступности и трансграничное взаимодействие:

- Первая развилка определяется конфигурацией внешнеполитических условий в ближайшие годы, в том числе отношений России с США и государствами Европы. Первый вариант прохождения развилки — исходя из консервативно-пессимистичного сценария сохранения режима санкций и напряженности в отношениях, обмен информацией и совместная работа по противодействию компьютерной преступности поддерживаются на низком уровне. Прямые контакты и совместная работа на уровне государственных правоохранительных органов между РФ и Западом свернута до минимума, рабочие взаимодействия на уровне частных структур также существенно ограничены. В результате фокус приложения усилий и ресурсов смещается на узкорегиональные форматы, где уже есть наработанная нормативная база и практический опыт: ОДКБ, ШОС, в перспективе — ЕАЭС и БРИКС. В остальном трансграничная работа ведется на уроне двустороннего взаимодействия, где важную роль играет КНР и государства АРФ.

  Второй вариант прохождения развилки — частичная нормализация рабочих контактов в сфере борьбы с компьютерной преступностью между РФ и Западом в среднесрочной перспективе. Просматривается вариант, когда межправительственное взаимодействие на уровне РФ-США и РФ-ЕС по-прежнему ограничено и не в полной мере эффективно, однако активно осуществляются контакты

и обмен информацией а) с отдельными государствами Западной Европы; б) на уровне международных ассоциаций, форумов и иных площадок, центров реагирования на компьютерные инциденты (CSIRT/CERT), где участвуют представители как российской, так и западной отрасли. В результате ресурсы и усилия вкладываются не только в узкие региональные форматы, но и в работу в рамках глобальных сетей обмена информацией и содействия в предупреждении и расследовании компьютерной преступности.

- Вторая развилка ставит вопрос развития международных норм и обязывающих совместных механизмов. Что целесообразнее для российских интересов: разрабатывать и продвигать с нуля новый механизм трансграничной борьбы с компьютерной преступностью либо развивать инициативы по модернизации уже существующих механизмов. Одним из механизмов является Конвенция Совета Европы о борьбе с компьютерной преступностью от 2001 г. Вместе с тем, для развития конвенции необходимо расширение числа ее участников, обновление составов преступлений и ряд других мер.

  Альтернативой может быть новая конвенция о борьбе с компьютерной преступностью, которая будет предлагать иной порядок трансграничного обмена данными в рамках расследования. Проект такой конвенции был разработан в России в 2012-2016 гг., однако до сих пор не был утвержден и одобрен для широкого международного продвижения. Другим вариантом может быть отказ от попытки сформировать универсальный механизм, и, опять же, концентрация усилий в рамках региональных форматов с участием РФ (ШОС, ОДКБ, ЕАЭС).

  Наконец, третий вариант прохождения развилки предполагает, что по крайней мере в среднесрочной перспективе РФ будет объективно лишена возможности существенно повлиять на международную повестку дня в области общих правовых механизмов и норм борьбы с компьютерной преступностью, а потому внимание должно уделяться развитию частных механизмов обмена информацией и наращиванию собственного потенциала.

- Третья развилка более актуальна для долгосрочной перспективы и учитывает необходимость серьезного пересмотра нынешних определений и составов компьютерных преступлений в связи с развитием новых технологий. Так, уже в ближайшие годы необходимо выработать подход к квалификации, предупреждению и расследованию инцидентов, связанных с атаками на активные киберфизические системы, в том числе способные повлечь не только финансовый и репутационный ущерб, но и ущерб здоровью и гибель (атаки на «умное» медицинское оборудование, автопилоты автомобилей и иных транспортных средств и проч.). В будущем вероятно придется учитывать риск целенаправленных атак на «цифровую личность», включая хищение всех персональных данных пользователя,

в том числе биометрических, нарушение процессов нейроинтерфейса «компьютер-мозг», манипуляции с ИИ, обеспечивающим персональные и корпоративные бизнес-процессы, необратимое разрушение данных в результате вторжения в системы, защищенные квантовым шифрованием, и проч. С высокой вероятностью будет формироваться тренд тотальной информатизации преступности и отмирания барьера между «традиционной» и высокотехнологичной преступностью. Такой сценарий сделает востребованным участие России в международном механизме оперативного реагирования и расследования преступлений вообще (Интерпол 2.0). Запуск и развитие глобального механизма расследования трансграничных инцидентов зависят от того, насколько в будущем окажется выражена тенденция инфраструктурной фрагментации интернета, а также от уровня международного доверия.

2. Обеспечение развития и глобальной конкурентоспособности российской отрасли ИБ (речь идет о таких нишах как СКЗИ, программно-аппаратные технологии защищенных микропроцессоров, средства сетевой безопасности и управления компьютерными инцидентами, средства обнаружения компьютерных атак (СОКА), системы и сервисы обнаружения и предотвращения вторжений (IDS/IPS), системы и сервисы предотвращения утечек данных (DLP), программные и программно-аппаратные межсетевые экраны (МСЭ), защищенные системы хранения данных (СХД), сетевое оборудование (маршрутизаторы, коммутаторы), средства анализа сетевого трафика и его аномалий, защищенные ОС, в том числе для корпоративных и промышленных систем, автоматизированные системы управления технологическими процессами (АСУ ТП), средства борьбы с целевыми компьютерными атаками (AntiAPT) и проч.).

Основная развилка активируется уже в ближайшие годы и связана с определением принципиального подхода к выбору ресурсов для достижения поставленных задач:

А Опора на собственные ресурсы и реализация концепции обеспечения ИБ через наращивание собственной технологической базы и развитие курса на стратегическое импортозамещение в отрасли ИТ, включая нишу ИБ по большинству ключевых направлений. Прохождение развилки в пользу такого варианта во многом определяется внешними переменными. В части внешнеполитических условий решающим доводом в пользу выбора этого варианта служит сохранение ограничений на доступ российского бизнеса и государства к передовым технологиям и решениям в области ИТ США, Японии и государств Западной Европы. В то же время, с точки зрения экономических вводных выбор варианта неоднозначен: реализация стратегии импортозамещения по широкому спектру технологических ниш с учетом нынешних «стартовых позиций» является скорее ресурсозатратной, чем прибыльной.

Б Второй вариант прохождения развилки предполагает, что реализация курса на импортозамещение в ИБ может быть ограничена системами и решениями, обеспечивающими функционирование КИИ и инфраструктур государственных органов, в т.ч. обеспечивающих обработку сведений конфиденциального характера либо сведений, содержащих гостайну. При этом конкурентные позиции российской отрасли ИБ и ее развитие обеспечиваются также за счет интеграции и более активного вовлечения российских компаний и технических структур в а) работу международных консорциумов и иных площадок, ведущих разработку перспективных решений в области ИБ; б) реализацию проектов решений на основе открытого кода (Open Source); в) эффективную интеграцию, локализацию и доработку существующих зарубежных решений; г) разработку своими силами не готовых решений, а перспективных технических стандартов и исходного кода (в т.ч. открытого), ориентированных на использование на глобальном рынке. При этом по отношению к обеспечению ИБ для российских пользователей и бизнеса (а частично и государства) использование российских решений не является самоцелью и подчинено задаче обеспечения качества внедряемых разработок вне зависимости от их происхождения.

3. Обеспечение безопасности на уровне регулирования, технологий и стандартов в процессе цифровой трансформации экономики РФ и ЕАЭС.

Базовая развилка: насколько успешным оказывается ЕАЭС как интеграционный проект с точки зрения выстраивания единого пространства цифровой трансформации государств, участвующих в нем. Развилка лишь частично зависит от действий и стратегии руководства РФ и в значительной степени определяется внутренними и внешнеполитическими установками участвующих в ЕАЭС стран. Так, в качестве одного из потенциальных препятствий стоит рассматривать наличие у отдельных государств ЕАЭС собственных программ цифровой трансформации. Примером является Казахстан, вторая по размерам после РФ цифровая экономика ЕАЭС, где в 2016 г. была принята программа «Цифровой Казахстан–2020», в значительной степени охватывающая вопросы, которые составляют повестку дня цифровой трансформации ЕАЭС. Прохождение развилки с формированием в ближайшие годы реально функционирующего пространства цифровой трансформации в масштабах ЕАЭС открывает окно возможностей для реализации предложений в области обеспечения ИБ. Альтернативный вариант прохождения развилки — пробуксовка проекта совместной цифровой трансформации в рамках ЕАЭС, либо его реализация в крайне неполном, «лоскутном» варианте. Это заставит Россию обеспечивать цифровую трансформацию экономики преимущественно своими силами в пределах своей же юрисдикции, что ограничивает и окна возможностей в части обеспечения ИБ в рамках этого процесса.

Исходя из указанных развилок сформулированы две стратегии:

- концентрация на собственных ресурсах и рынке ЕАЭС, консервация рисков за счет усиления регулирования.

- гибкое управление рисками, локальные прорывы за счет опережающих решений.

4.1. ОПОРА НА СОБСТВЕННЫЕ РЕСУРСЫ И РЫНОК ЕАЭС, КОНСЕРВАЦИЯ РИСКОВ ЗА СЧЕТ УСИЛЕНИЯ РЕГУЛИРОВАНИЯ

Подход ориентирован на сохранение неблагоприятных внешнеполитических условий в обозримом будущем, прежде всего в плане отношений со странами Запада. Даже если нынешний виток обострения будет локализован и частично пройдет в перспективе 1-3 лет, вероятность новых всплесков напряженности в отношениях слишком высока, чтобы выстраивать стратегию развития отрасли ИТ и ниши ИБ без их учета.

В подход заложен высокий риск повторного либо продолжающегося применения в отношении государственных структур и бизнеса РФ санкций, подразумевающих ограничение доступа к технологиям и передовым решениям в области ИТ и конкретно ИБ. В более отдаленном будущем сохранение этого фактора толкает к фрагментации глобального ИТ-рынка по национальным юрисдикциям и стратегическим альянсам, что приведет к росту протекционизма и ограничений на обмен технологиями в отрасли ИТ и нише ИБ.

В то же время, подход предполагает сохранение и развитие отношений РФ с государствами БРИКС, отсутствие серьезных кризисов в отношениях со странами Юго-Восточной Азии. Кроме того, важной предпосылкой подхода служит по крайней мере частичный успех ЕАЭС как интеграционного формата, в том числе в части цифровой трансформации. Сценарий фрагментации глобальной экономики и системы международных отношений в целом предполагает более четкое очерчивание и более тесную внутреннюю интеграцию региональных альянсов, в роли которого в случае РФ выступает прежде всего ЕАЭС.

Основные меры и решения в рамках подхода:

1. ***В области противодействия компьютерной преступности подход предполагает окончательный отказ от попыток выстраивания многосторонних механизмов трансграничного взаимодействия с Западом на основе обязывающих норм***

(таких как Будапештская конвенция Совета Европы 2001 г.). Также консервируются «до лучших времен» усилия дипломатии РФ по продвижению проектов глобального нормативного механизма борьбы с компьютерной преступностью (проект универсальной конвенции ООН). Центр тяжести смещается на двустороннее взаимодействие с ключевыми партнерами. В отношении США контакты и обмен запросами по инцидентам компьютерной преступности поддерживаются лишь по мере необходимости и по линии отдельных ведомств (АНБ, регуляторы финансово-кредитного сектора, US-CERT). Чуть большая открытость обеспечена в отношении Европола, который в перспективе может серьезно нарастить свои уже имеющиеся компетенции и стать наиболее репрезентативным и активным международным форматом борьбы с компьютерной преступностью в мире. В целом среди двусторонних взаимодействий наибольший уровень сотрудничества и раскрытия информации обеспечивается в отношениях с КНР: речь может идти о расширении и практическом наполнении двустороннего соглашения о сотрудничестве в области обеспечения МИБ от 8 мая 2015 г. в части оперативного обмена информацией об инцидентах компьютерной преступности.

Возможно активное использование региональных форматов постсоветского пространства (ЕАЭС, ОДКБ) и ШОС. Центральным форматом в ближайшие годы остается ОДКБ, где сохраняется и расширяется практика регулярных операций по выявлению ресурсов с противоправным контентом (операции ПРОКСИ). С подачи и за счет РФ за несколько лет можно выстроить в рамках ОДКБ полноценный механизм обмена данными и реагирования на инциденты ИБ. Базой для развертывания такого механизма может послужить решение о Консультационном координационном центре ОДКБ по вопросам реагирования на компьютерные инциденты, подписанное на саммите организации в декабре 2014 г. За счет инвестирования собственных ресурсов и работы с партнерами РФ имеет возможность продвинуть решение о превращении такого центра в полнофункциональный центр реагирования на компьютерные инциденты CSIRT, работающий в режиме 24/7 и обеспечивающий оперативное реагирование на информацию об инцидентах. В рамках подхода допустимо привлечение к такому проекту частных компаний РФ, имеющих опыт создания инфраструктуры CSIRT и надежную репутацию в глазах государства.

Обмен информацией между отраслевыми CSIRT и частными организациями РФ и западных стран, прежде всего США, напротив, существенно ограничивается в силу низкого уровня доверия к контрагентам. В этом смысле ситуация в рамках подхода представляет собой застывший срез ситуации по состоянию на 2017 г., когда серьезно сократилась интенсивность и объем обмена информацией между российскими и западными компаниями, специализирующимися в нише ИБ и управления инцидентами.

В целом обмен информацией и реагирование на компьютерные инциденты в рамках подхода развиваются с учетом постепенного, но существенного роста контроля государства над частными и неправительственными механизмами в этой сфере. Так, для операторов объектов КИИ РФ закрепляется возможность обмена информацией об атаках и инцидентах только в порядке и формате, установленном регулятором и фактически с его санкции. В то же время, государство поддерживает вовлечение частной отрасли в налаживание контактов и выстраивание взаимодействий с CSIRT и регуляторами ключевых партнеров, таких как КНР и государства БРИКС. В рамках БРИКС в ближайшие годы возможно продвижение российской инициативы о развертывании общего центра реагирования на компьютерные инциденты (BRICS-CERT) — однако в качестве скорее межправительственного, чем отраслевого механизма.

Наконец, в рамках опоры на ключевые региональные альянсы с подачи РФ трек межгосударственного взаимодействия в сфере борьбы с компьютерной преступностью и обменом информацией может быть встроен в формат ЕАЭС — например, в рамках повестки дня обеспечения безопасного развития цифровой экономики ЕАЭС и нейтрализации рисков цифровой трансформации. Запуск такого трека в горизонте 2020-2022 гг. может быть обеспечен с использованием механизмов, наработанных ранее в рамках СНГ (Соглашение «О сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации» от 1 июня 2001 г., а также модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности» от 2014 г.).

2. ***Развитие технологической базы в области ИТ и ИБ осуществляется в рамках стратегии поэтапного, или «ступенчатого» импортозамещения.***

- В краткосрочном горизонте приоритетной целью является повышение защищенности систем, обеспечивающих функционирование КИИ и инфраструктур государственных органов, ответственных за обработку конфиденциальных сведений и сведений, содержащих гостайну. Главным риском является зависимость операторов таких систем от западных технологий, доступ к которым может быть перекрыт в рамках санкций либо иных последствий ухудшения отношений. В отношении таких систем вырабатывается и принимается дорожная карта их приоритетного импортозамещения.

- Параллельно стратегической целью сотрудничества с КНР в сфере ИБ признается получение доступа к лицензиям на приоритетные в рамках импортозамещения технологии и решения, прежде всего аппаратные. Другим источником решений, не подпадающих под политические риски отношений с Западом, выступают доступные на рынке проекты на основе открытого кода. Добавляя эти источники технологий к своей технологической базе, государство во взаимодействии с отраслью запускает ряд долгосрочных проектов по импортозамещению в сфере

ИТ. Ключевым приоритетом является разработка собственных конкурентных технологий микропроцессоров и обеспечение для них базы в отрасли микроэлектроники. Это направление может быть выделено в отдельное направление сотрудничества с КНР в качестве стратегического приоритета.

3. ***За рамками продвижения российских стандартов обеспечение безопасной цифровой трансформации пространства ЕАЭС подчиняется той же логике, что и внутреннее регулирование РФ в области обеспечения ИБ в рамках предлагаемого подхода.*** Ключевой посыл — ужесточение регулирования, в том числе в части повышения требований к сертификации, выработка комплексной линейки требований и обязательств операторов КИИ и государственных систем. В отношении цифровой трансформации ЕАЭС важный посыл в управлении рисками ИБ состоит в консервативном подходе к внедрению новых решений и легализации новых технологий и основанных на них сервисов (финансовые и иные сервисы на распределенных реестрах, беспилотный интеллектуальный транспорт, промышленные применения Интернета вещей, «умные» энергосети и энергосистемы (Smart Grid) и проч.). Консервативный подход к регулированию предполагает практическую реализацию концепции «обеспечение ИБ перед внедрением ИТ», которая позволяет снизить риски, связанные с непродуманным в части безопасности внедрением технологии (например, массовое внедрение незащищенных устройств Интернета вещей, используемых для организации масштабных DDoS-атак). Также, выступая с позиций консервативного регулятора в нише ИБ в рамках ЕАЭС, РФ получает возможность «фильтровать» непрерывный поток ИТ-инноваций, достигающих рынков Союза, давая зеленый свет прежде всего тем из них, которые уже охвачены регулированием на ее национальном рынке, и тем, внедрение которых в масштабах ЕАЭС опять же может быть выполнено с опорой на уже имеющиеся и сертифицированные решения российской отрасли. Таким образом, Россия может стать для ЕАЭС и источником модели регулирования в нише ИБ, и одновременно закрепить свою ИБ-отрасль как ключевого инфраструктурного и технологического провайдера для реализации проектов цифровой трансформации, прошедших регуляторный фильтр.

Такие проекты, опирающиеся на российский задел в стандартизации и технологиях, могут включать в себя создание единой экосистемы безопасной электронной идентификации граждан и бизнес-субъектов государств ЕАЭС (в том числе внедрение единых технических стандартов идентификации, унификация оборудования, процедур, языков и форматов данных в рамках бизнес-процессов G2B, G2C, G2G в масштабах ЕАЭС), а также внедрение единой системы «электронного паспорта» и связанной с ней инфраструктуры обработки данных, развертывание единой электронной инфраструктуры таможенных служб и проч.

Наконец, для государств ЕАЭС Россия в случае успешного продвижения своих стандартов ИБ в рамках совместной цифровой трансформации становится ключе-

вым источником компетенций в области ИБ, включая вопросы КЗИ и связанные с ними стандарты. Используя этот фактор, российские госучреждения и частные организации могут расширить спектр образовательных услуг в сфере ИБ, ориентированных на граждан ЕАЭС. Кроме того, аналогичные программы можно реализовать для граждан стран БРИКС, прежде всего Индии и КНР. Для самой России источником лучших практик и компьютерной грамотности могут выступать специалисты и программы Сингапура, Малайзии и базирующихся в регионе проектов ГЧП в области ИБ, а также программы ОЭСР и европейских государств.

РИСКИ подхода главным образом связаны с замедлением инновационного развития российской отрасли ИТ и ИБ вследствие ужесточения регулирования и отказа от передовых решений глобального рынка в рамках импортозамещения. Описанное «ступенчатое» импортозамещение — «стратегия марафонца», которая дает результаты в отложенной перспективе (3-5-8 лет в зависимости от конкретной ниши). То есть в ближайшие годы ее реализация при всех перечисленных возможностях может повредить как реальному уровню ИБ инфраструктур России и ЕАЭС, так и эффективности бизнес-процессов тех отраслей, где применяются импортозамещаемые решения. Так, несмотря на очевидные преимущества решений на основе открытого кода, их качество и вытекающий из него уровень ИБ для систем, в которые внедряется такое решение, может быть неудовлетворителен. Кроме того, опора на доступ к технологиям КНР как альтернативе западным на начальных этапах импортозамещения несет риск сползания российской отрасли в технологическую и лицензионную зависимость от стратегического партнера, особенно если его роль как технологического донора будет близка к монопольной.

Еще один риск обусловливается сокращением возможностей контактов и обмена информацией для российских частных компаний и негосударственных CSIRT, в том числе с западными коллегами из частной отрасли. Узкие региональные форматы типа ОДКБ, ШОС и ЕАЭС по охвату не заменяют сотрудничества с ЕС, США и западными компаниями, являющимися глобальными лидерами в области ИБ и сетевой безопасности. Несмотря на бурный рост восточноазиатской ниши этого рынка, западное отраслевое лидерство будет оставаться неоспоримым как минимум в среднесрочной перспективе. Следует также помнить, что сокращение контактов с евроатлантическим сообществом по умолчанию распространяется и на Японию, обладающую весьма богатым опытом и серьезными наработками в области реагирования на инциденты и обмена информацией. Вынужденно замыкаясь в кругу узких региональных партнерств со слаборазвитыми в нише ИБ государствами и осуществляя длительную перенастройку сети контактов и сотрудничества на АТР и страны БРИКС, РФ рискует в процессе столкнуться с серьезным ростом угроз своей экономике и безопасности в части трансграничной киберпреступности, компьютерных атак и иных инцидентов.

Наконец, наиболее фундаментальный риск в рамках подхода связан со ставкой на ЕАЭС как ключевую площадку международного продвижения российских интересов в отрасли ИБ. Безусловно, технологическое и ресурсное лидерство России делают шансы на успех в решении перечисленных задач (использование повестки ИБ в рамках цифровой трансформации ЕАЭС для расширения присутствия на рынках стран Союза) достаточно высокими. Однако давление на партнеров в этом направлении может привести к падению ценности самого формата в глазах его участников и, в конечном счете, торпедированию ими всей повестки цифровой трансформации. При этом даже в долгосрочной перспективе рынков стран ЕАЭС явно недостаточно для того, чтобы Россия успешно завершила комплексное импортозамещение за счет них и собственного внутреннего рынка.

4.2. АДАПТАЦИЯ К НЕСТАБИЛЬНЫМ АЛЬЯНСАМ И ДЕФИЦИТУ РЕСУРСОВ: ГИБКОЕ УПРАВЛЕНИЕ РИСКАМИ, ЛОКАЛЬНЫЕ ПРОРЫВЫ ЗА СЧЕТ ОПЕРЕЖАЮЩИХ РЕШЕНИЙ

Как и в предыдущем варианте подхода по данному направлению, предполагается продолжающееся в рамках горизонта охлаждение и частичное проседания сотрудничества с США. Однако в отличие от предыдущего варианта напряженность в российско-американских отношениях менее выражена и не носит перманентного характера. Подход скорее ориентирован на дефицит стабильности и отсутствие длинного горизонта планирования, в том числе в части применения к РФ санкционных механизмов, затрагивающих отрасль ИТ. Возможно умеренное ослабление ЕС и выдвижение на первый план повестки двусторонних отношений с ключевыми западноевропейскими государствами.

Также предполагается усиление региона АТР как двигателя глобального экономического роста и технологического развития, в том числе в области ИТ. Центральную роль в этих процессах будет играть КНР, отношения России с которой будут скорее следовать амплитуде прагматичного торга по насущным вопросам, чем стабильному стратегическому партнерству.

Наконец, в подход заложен сценарий «слабого» ЕАЭС, в рамках которого для ряда членов Союза участие в совместной повестке, в том числе в сфере цифровой трансформации, будет являться предметом внешнеполитического торга и балансирования между различными центрами силы. Такой сценарий не означает коллапса ЕАЭС, однако заставляет РФ, как заинтересованную в сохранении формата сторону, тщательно выбирать точки приложения усилий в рамках проектов Союза, концентрируясь на первоочередных задачах.

Основные меры и решения в рамках подхода:

1 В части международного сотрудничества в области борьбы с компьютерной преступностью подход предусматривает два решения для разных временных горизонтов: ускоренная гармонизация национальных законодательств стран ЕАЭС для формирования регионального механизма в среднесрочной перспективе; разработка и продвижение как специфичных для ЕАЭС, так и глобальных многосторонних форматов новой концепции борьбы с высокотехнологичной преступностью в долгосрочном плане.

Учитывается нестабильность международной обстановки и отсутствие у РФ ресурсов для самостоятельного продвижения масштабных инициатив, таких как проект универсальной конвенции ООН. В то же время, принципиальные возражения ключевых групп интересов внутри РФ и внешние объективные факторы обуславливают отказ от попыток присоединиться к механизму Будапештской конвенции Совета Европы от 2001 г. Реалистичной альтернативой в части формирования пространства общих норм для борьбы с компьютерными преступлениями становится площадка ЕАЭС. Как и в предыдущем подходе, продвижение этой повестки с подачи России выделяется в отдельную корзину обеспечения безопасного развития цифровой экономики ЕАЭС и нейтрализации рисков цифровой трансформации. В ближайшие годы упор делается на гармонизацию национальных законодательств (в т.ч. УК и УПК государств ЕАЭС) в части составов компьютерных преступлений, мер ответственности и порядка возбуждения и ведения дел по таким статьям. Базой служат документы, наработанные в рамках СНГ (Соглашение «О сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации» от 1 июня 2001 г., модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности» от 2014 г.), а также международные лучшие практики и рекомендации международных организаций (ООН, Европол, ИМПАКТ-МСЭ).

Параллельно в России осуществляется разработка концепции снижения угроз высокотехнологичной преступности как подхода, отражающего изменения преступности под влиянием развития ИКТ и всеобъемлющей цифровизации взаимодействий в обществе. Концепция играет роль инструмента упреждающей работы с трансграничными вызовами и опережающего формирования повестки дня в условиях, когда ряд рассматриваемых вызовов и угроз еще не активирован в полной мере. С содержательной точки зрения, концепция высокотехнологичной преступности и борьбы с ней предполагает несколько ключевых моментов:

- ***Отражение в законодательствах технологически новых способов совершения противоправных действий с использованием ИКТ и квалификация их с учетом***

возможных последствий. Прежде всего речь идет о противоправных действиях в отношении киберфизических систем, таких как перехват управления и провоцирование катастрофы умного транспорта, нанесение ущерба медицинскому оборудованию при помощи компьютерной атаки, вывод из строя систем оказания жизненно важных услуг и так далее.

- ***Выработка новых принципов к определению понятия места совершения преступления, что важно для трансграничных высокотехнологичных преступлений.*** Проработка смычки технических и правовых механизмов атрибуции противоправных действий, в том числе осуществляемых через распределенные трансграничные инфраструктуры.

- ***Обновление и систематизация понятий «цифровых доказательств» (digital evidence),*** а также закрепление того или иного подхода к их рассмотрению в процессе следствия в судах в качестве значимых улик.

- Принципиально важный момент: ***проработка вопроса о смене принципа формулирования квалифицирующих статей в отношении противоправных действий, совершенных с использованием высокотехнологичных средств.*** Исходя из ожидаемых тенденций цифровизации в будущем, может быть предложен отказ от выделения отдельных статей по компьютерным преступлениям в УК и, взамен, та или иная квалификация действий с использованием высокотехнологичных средств в рамках «традиционных» статей и составов преступлений (например, приведение в негодность объектов жизнеобеспечения; умышленные уничтожение или повреждение имущества; манипулирование рынком; мошенничество и проч.).

Концепция могла бы лечь в основу долгосрочных преобразований российского законодательства (модернизация УК и УПК РФ) и стать базовой для следующего цикла модернизации и гармонизации национальных норм в сфере борьбы с преступностью. Проработка концепции high-tech crime органично примыкает к цифровой трансформации; формат ЕАЭС компактен по составу и удобен России для продвижения инициатив. Положительный опыт разработки гармонизированного видения угроз и методов борьбы с высокотехнологичной преступностью в рамках ЕАЭС может быть синхронизирован с обсуждением этих вопросов на площадках Управления ООН по наркотикам и преступности, Совета Европы, Европола, ОЭСР, Всемирного экономического форума (WEF).

2 В ближайшие годы, в отсутствие пространства общих норм и единой трансграничной юрисдикции для борьбы с компьютерной преступностью Россия делает упор на ***обмен информацией и взаимодействие с партнерами***. Предпосылкой для этого служит активизация частных механизмов CSIRT, которая

обеспечивается за счет частичного смягчения регулирования в этой нише со стороны федеральных органов власти. В рамках увязки с подходом, основанным на разделении рисков БСО между государством и частным сектором, предполагается, что ограничения на обмен информацией по негосударственным и международным каналам распространяются только на госорганы и иные субъекты, отнесенные к единому государственному сегменту электросвязи. При этом ограничения не распространяются на частных операторов объектов КИИ, что позволяет увеличить объем российского рынка услуг CSIRT и обмена информацией.

В отношении CSIRT ставка делается на развитие российской ниши и вывод ее на международный уровень за счет углубления отраслевой специализации центров реагирования на компьютерные инциденты и активного внедрения в отрасли механизмов государственно-частного партнерства. Первые проекты могут быть реализованы в рамках адаптации под условия и механизмы ГЧП проекта CII-CERT, запущенного Лабораторией Касперского в 2016 г. для операторов КИИ, и формирования центра реагирования и обмена информацией для телекоммуникационной отрасли (Telecom-CSIRT). В сходной перспективе может быть запущен проект центра реагирования на инциденты на энергосетях и иных объектах отрасли распределения электроэнергии, где также довольно органичен формат ГЧП. Еще одним направлением поддержки ниши обмена информацией и реагирования на инциденты может быть необходимое ослабление регулирования и создание стимулов для того, чтобы компании-лидеры различных отраслей предлагали функционал CSIRT и обмена информацией, развернутый на базе их внутренних центров реагирования, внешним клиентам. Сбербанк с 2016 г. реализует проект создания центра управления информационной безопасностью (SOC) на базе инфраструктуры IBM с учетом лучших мировых практик. Учитывая масштабы ИТ-инфраструктуры самого Сбербанка, функционал SOC после его запуска может быть дополнен набором услуг в формате CSIRT для внешних клиентов — банковских организаций в РФ, а возможно и за рубежом. Такой частный CSIRT сможет дополнять функции государственного FinCERT при ЦБ РФ.

С отраслевой специализацией CSIRT/CERT и их поддержкой за счет ГЧП российские игроки смогут более активно участвовать в ведущих мировых ассоциациях CSIRT/CERT (FIRST, Trusted Introducer) и иных механизмах обмена информацией о компьютерных инцидентах (в рамках Европола, ИМПАКТ-МСЭ). В среднесрочной перспективе актуальны вопросы создания механизмов регулярного обмена информацией между CSIRT/CERT в рамках региональных и иных многосторонних форматов, таких как БРИКС, ЕЭАС, ШОС. В отличие от предыдущего сценария, в пределах постсоветского пространства предлагается делать упор на развитие механизмов регулярного обмена информаци-

ей между частными и частно-государственными CSIRT/CERT в рамках ШОС и ЕАЭС, отказавшись от создания единого полнофункционального CSIRT ОДКБ как недостаточно гибкой и ресурснооправданной. В условиях дефицита ресурсов критерием необходимости механизмов управления инцидентами и обмена информацией должна в том числе выступать их востребованность на рынке.

Россия в ближайшие годы могла бы поддержать и запуск пилотных инициатив по созданию депозитариев инцидентов, уязвимостей и иных механизмов обмена информацией при международных структурах. Возможно продвижение государством и отраслью единого депозитария уязвимостей объектов ядерной инфраструктуры и образцов вредоносного ПО при МАГАТЭ. При поддержке механизмов ГЧП российские игроки смогут подключиться к подобным международным инициативам в других отраслях (энергораспределение за счет «умных сетей», гидроэнергетика, ТЭК, нефтехимическая промышленность). Вместе с тем, продвижение подобных инициатив любыми средствами не является целью, речь идет лишь о готовности российской дипломатии и отрасли оперативно подключиться к их продвижению и наполнению при благоприятных условиях.

3 ***Развитие технологической базы в области ИТ и ИБ исходит из концепции ограниченного импортозамещения,*** которое распространяется только на военные системы и инфраструктуры, частично — КИИ «гражданских» секторов, а также госструктуры, инфраструктура которых отнесена к единому государственному сегменту Интернета (электросвязи) в рамках увязки с подходом распределения рисков БСО между государством и частным сектором. Ставится задача продвижения российских решений и технологий в условиях повышения гибкости, а не ужесточения регулирования. Предлагаются следующие решения:

- ***Проводится всеобъемлющая «инвентаризация» технологических активов, которыми обладает государство и отрасль РФ в области ИБ.*** Такая работа охватывает все уровни ИТ начиная от компонентной базы микроэлектроники и криптографических стандартов, заканчивая полной инвентаризацией готовых решений, права на которые принадлежат российским компаниям. По итогам инвентаризации, во-первых, составляется комплексная дорожная карта решений, подлежащих импортозамещению в различных временных горизонтах. Во-вторых, частью инвентаризации является запуск проекта по систематизации существующих и применяемых в РФ стандартов ИБ и соотнесения их с имеющимся и перспективным регулированием и отраслевыми практиками. Ближайшим аналогом такого проекта является Рамочная программа по уменьшению рисков ки-

бербезопасности Национального института стандартов и технологий США (NIST Cybersecurity Framework). Практическая важность такой программы состоит в упорядочивании национальной политики в области стандартизации ИБ и применении наработанных стандартов. По завершении такой программы дальнейшая политика ИБ-регуляторов и развитие отраслевых практик может осуществляться с учетом и на основе созданной «базовой матрицы», соотносящей действия и политики ИБ со стандартами.

- Ключевой задачей является развитие стандартизации и поддержание передового уровня российских решений в области ИБ на уровне стандартов. Подход опирается на 2 тезиса: а) выработка стандартов и решений в области ИБ с опорой лишь на собственные ресурсы неэффективна в условиях глобальных угроз и активной кооперации глобальных разработчиков; б) продвижение российских стандартов на внешние рынки административно-политическими методами (см. продвижение стандартов шифрования ГОСТ на рынок ЕАЭС в предыдущем подходе) несет высокие риски отказа партнеров от кооперации в условиях наличия альтернатив. Для эффективного продвижения решений на основе российских стандартов на внешние рынки необходимо повышение их рыночной привлекательности. ***Решается задача активизации участия отраслевых компаний и технического сообщества РФ в работе международных площадок по стандартизации в области ИБ и безопасных ИТ-платформ.*** Важный момент: при этом приоритетом является не участие в работе площадок, где собственно происходит оформление разработанного решения/технологии в качестве стандарта (IEEE, ISO, МСЭ), а участие непосредственно в трансграничных кооперациях и партнерствах, где создаются новые решения, алгоритмы, протоколы, которые позднее стандартизируются. В настоящее время одним из ключевых форматов таких кооперации являются международные консорциумы (в нише программно-конфигурируемых сетей (SDN): консорциум OpenDaylight; консорциум UNH-IOL; в нише решений на базе блокчейна: проект Hyperledger, консорциум R3 (R3 CEV LLC); в нише квантовой криптографии: консорциум SECOQC, и др.) со смешанным составом из представителей НПО, крупных корпораций, университетов и исследовательских лабораторий, в том числе государственных. В рамках подхода для российских компаний и особенно государственных университетов, НИИ и лабораторий за счет механизмов господдержки и ГЧП обеспечиваются стимулы для участия в деятельности глобальных консорциумов по наиболее перспективным нишам ИБ. При этом устраняются неформальные и полуформальные ограничения на участие в таких форматах представителей НИИ и иных компаний, тесно взаимодействующих с госорганами, в том числе в области безопасности. При этом для российских компаний частного сектора создаются благоприятные условия для внедрения разрабатываемых решений на

своей инфраструктуре. Один из шагов в этом плане — отход от концепции консервативного регулирования в отношении сервисов на распределенных платформах (блокчейн) и «режим зеленого света» для проектов российских компаний по реализации сервисов на базе блокчейна. Само государство прорабатывает возможность переноса на инфраструктуру на базе блокчейна ряда своих сервисов в рамках их цифровизации (кадастровая служба, регистрация актов гражданского состояния, регистрация сделок с государственными ценными бумагами, госзакупки и проч.).

- Отдельная задача включает продвижение на внешние рынки российских систем криптографической защиты информации (СКЗИ). В ближайшие годы в России проводится ***реформа регулирования в области СКЗИ с целью повышения его гибкости и частичного устранения барьеров к более активному рыночному использованию российских решений.*** Во-первых, упрощается процедура вывоза сертифицированных СКЗИ за пределы РФ, в том числе для их коммерческой реализации. Смягчаются ограничения на разработку средств шифрования на базе ГОСТ без получения лицензии ФСБ и продажу таких средств на территории России и за рубежом как российскими, так и зарубежными разработчиками. Повышается прозрачность процедур и требований регулятора к разработке, ввозу-вывозу и сертификации СКЗИ. В результате должно быть обеспечено повышение привлекательности СКЗИ на базе стандартов ГОСТ для разработчиков в России и за рубежом, прежде всего в странах БРИКС и ЮВА. Во-вторых, вырабатывается и внедряется концепция разделения сферы применения СКЗИ на «государственную» и «гражданскую» с целью создания рынка массового потребителя СКЗИ, свободного от сертификации ФСБ. В категорию сервисов массового рынка попадает использование гражданами криптографических средств для личных целей (хранение электронных данных при помощи токенов и иных носителей, поддерживающих шифрование, личные коммуникации при помощи защищенных программно-аппаратных средств и проч.), а также ввоз и реализация на российском рынке продукции с поддержкой функций шифрования, рассчитанной на массового коммерческого потребителя (например, роутеры для домашних и офисных сетей). В результате бизнес-процессы граждан и ряда категорий коммерческих пользователей упрощаются в части легального использования средств шифрования; сокращается зарегулированность ввоза на территорию РФ зарубежных СКЗИ.

- Параллельно со смягчением регулирования СКЗИ решается задача подготовки технологического и рыночного прорыва РФ в области квантовой и постквантовой криптографии. В рамках долгосрочной повестки речь идет об упреждающем управлении вызовами, связанными с перспективой резкого увеличения вычислительных мощностей квантовых компьютеров.

Ожидается повышение эффективности т.н. «квантовых атак». Результатом может стать полная утрата стойкости большинством нынешних асимметричных криптоалгоритмов (в том числе использующихся для формирования сертификатов цифровой подписи) и снижение стойкости блочных алгоритмов симметричного шифрования. Такой сценарий поставит под угрозу всю глобальную экосистему безопасности и доверия в Интернете (защита данных в ключевых протоколах Сети обеспечивается за счет цифровых подписей, сформированных при помощи асимметричных криптоалгоритмов). Для предупреждения такого сценария необходим заблаговременный запуск программы замены существующих алгоритмов генерации общего секретного ключа (асимметричное шифрование на основе схемы Диффи-Хэллмана). В рамках предлагаемого «перезапуска» регулирования в нише СКЗИ Россия может ***развернуть подобную программу и приступить к разработке нового поколения алгоритмов, стойких к квантовым атакам,*** используя свою научно-технологическую базу и опыт в сфере криптографии. Речь идет о масштабном долгосрочном (4-8 лет) проекте, который оптимально реализовывать в рамках масштабного международного консорциума со смешанным участием. Россия вместе с заинтересованными партнерами по ЕАЭС и КНР может выступить с инициативой такого консорциума, рассчитанного на широкое международное, прежде всего западное участие, либо подключиться к работе на чужих площадках. Вовлеченность и итоговый вклад России в разработку постквантовых стандартов шифрования во многом определяет ее место на глобальном рынке СКЗИ и услуг цифровых сертификатов в долгосрочной перспективе.

РИСКИ стратегии прежде всего связаны со сложностью обеспечения необходимого аппаратного ресурса для проведения предлагаемых решений с учетом возможного сопротивления регуляторов. Переломным моментом для преодоления таких рисков является период, когда предлагаемые меры должны начать приносить устойчивый эффект в плане развития отрасли ИТ и ИБ в России, а также позитивно влиять на макроэкономическую динамику в целом.

РЕЗЮМЕ

Можно выделить варианты стратегии, которые представляются оптимальными для достижения поставленных целей:

1 Укрепление международной безопасности и стабилизация системы международных отношений за счет ограничения использования ИКТ в военно-политических целях, а также снижения риска возникновения и эскалации международных конфликтов с использованием ИКТ.

Для достижения данной цели предлагается «стратегия малых шагов» и мобилизации ресурсов частного сектора в управлении вызовами военно-политического использования ИКТ. В рамках стратегии предполагаются следующие шаги:

- Определение приоритетных отраслей критической информационной инфраструктуры (КИИ) и реализация дипломатических инициатив по выработке норм ограничения военно-политического использования ИКТ конкретно против объектов из этих отраслей. В качестве наиболее вероятных отраслей для достижения договоренностей и краткосрочной и среднесрочной перспективе рассматриваются:

  - Банковская и финансово-кредитная отрасль;
  - Мирная атомная энергетика;
  - Система уникальных идентификаторов Интернета (УИИ).

  При этом точечные конкретные договоренности по приоритетным нишам КИ рассматриваются как более гибкая и жизнеспособная альтернатива идее комплексных рамочных норм по регулированию поведения в киберпространстве.

- Адаптация и развитие механизмов экспортного контроля для программно-аппаратной ИТ-продукции двойного назначения либо предназначенной конкретно для осуществления специальных операций в киберпространстве. Отправной точкой для создания такого механизма в международном формате могут быть уже существующие нормы в части ограничения экспорта ИТ-продукции двойного назначения, действующие с декабря 2013 г. в рамках Вассенаарских договоренностей.

- Отделение повестки дня информационного противоборства от вопросов защиты инфраструктуры в контексте выработки норм, ограничивающих военно-политическое использование ИКТ, на международных многосторонних форумах и в двустороннем формате.

- Повышение результативности международной работы над сокращением рисков военно-политического использования ИКТ за счет создания механизмов взаимодействия межгосударственных форматов и ИТ-отрасли. Обеспечение активного участия российской ИТ-отрасли в таких механизмах. В частности, повышение результативности и реального влияния площадки Группы правительственных экспертов ООН.

2 Обеспечение безопасности, стабильности и отказоустойчивости (БСО) Интернета и инфраструктуры цифровой передачи данных для российских пользователей, бизнеса и государства.

Для достижения этой цели в качестве оптимальной предлагается стратегия распределения рисков между государством и частным сектором и «размывание» критически важных инфраструктур. Такая стратегия включает в себя следующие меры:

- Смещение фокуса подхода к управлению трансграничными рисками БСО единой сети электросвязи РФ и Рунета от концепции национального сегмента Интернета к государственному сегменту Интернета. Решение этой задачи обеспечивается за счет идентификации и нормативного закрепления понятия российского государственного сегмента единой сети электросвязи и Интернета.

- Государство осуществляет идентификацию и категорирование критической информационной инфраструктуры (КИИ) электросвязи и разрабатывает четкую систему количественных параметров и пороговых значений для определения критически важных субъектов в отрасли связи, в том числе по критерию пропуска трансграничного интернет-трафика.

- Для субъектов отрасли телекоммуникаций и ИТ, которые не входят в государственный сегмент, но также формируют единую сеть электросвязи РФ, вырабатывается и осуществляется рамочное регулирование, основанное на концепции жизненно важных услуг. Для управления рисками безопасности, стабильности и отказоустойчивости (БСО) предлагается рамочное регулирование, основанное на концепции жизненно важных услуг (ЖВУ).

- Управление трансграничными рисками БСО частных операторов, не вклю-

ченных в единый государственный сегмент Интернета, основывается на децентрализации критической инфраструктуры и «размывании» потенциальных точек отказа.

3 Обеспечение российских интересов в сфере безопасной цифровой трансформации, борьбы с компьютерной преступностью, а также развития технологий и рынка ИБ.

Целевое состояние для данного направления стратегии включает в себя:

- Наличие эффективного механизма международного взаимодействия в сфере борьбы с компьютерной (высокотехнологичной) преступностью, включая механизмы трансграничного обмена информацией о компьютерных инцидентах, общие нормативные рамки для трансграничного сотрудничества.

- Высокий уровень развития и конкурентоспособности российской отрасли информационной безопасности (ИБ) на уровне глобальных лидеров.

- Обеспечение безопасности на уровне регулирования, технологий и стандартов в процессе цифровой трансформации экономики РФ и ЕАЭС.

Приоритетным вариантом стратегии видится адаптация к нестабильным альянсам и дефициту ресурсов за счет гибкого управления рисками, а также достижения локальных прорывов за счет опережающих решений в развитии концептуально новой правовой базы для борьбы с высокотехнологичной преступностью, разработки стандартов квантовой и постквантовой криптографии, а также стандартизации сервисов и решений новой цифровой инфраструктуры (НЦИ) с упором на безопасность.

В части борьбы с компьютерной преступностью реализуются следующие меры:

- Отражение в законодательствах технологически новых способов совершения противоправных действий с использованием ИКТ и квалификация их с учетом возможных последствий.

- Выработка новых принципов к определению понятия места совершения преступления, что важно для трансграничных высокотехнологичных преступлений.

- Обновление и систематизация понятий «цифровых доказательств» (digital evidence), а также закрепление того или иного подхода к их рассмотрению в процессе следствия в судах в качестве значимых улик.

При отсутствии прогресса в создании новых широких многосторонних механизмов борьбы с киберпреступностью Россия делает ставку на повышение роли и эффекта механизмов обмена информацией, включая инфраструктуру CSIRT/CERT, прежде всего за счет ресурсов частного сектора. Решение задачи достигается за счет углубления отраслевой специализации центров реагирования на компьютерные инциденты и активного внедрения в отрасли механизмов государственно-частного партнерства

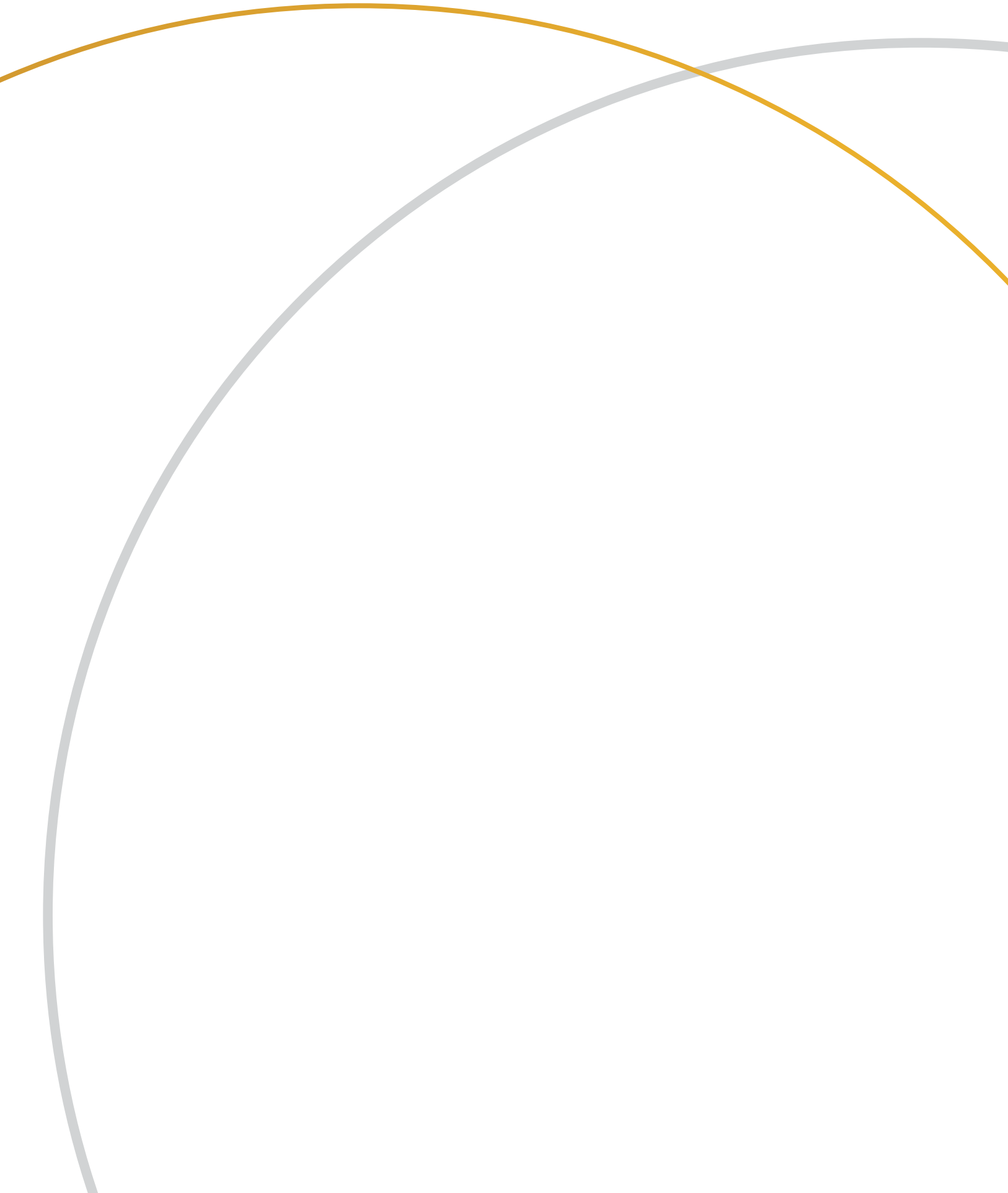
Развитие технологической базы в области ИТ и ИБ исходит из концепции ограниченного импортозамещения, которое распространяется только на военные и критически важные государственные системы и инфраструктуры. В рамках такого подхода обеспечивается решение следующих подзадач:

- Комплексная «инвентаризация» технологических активов государства и частной отрасли в сфере ИБ.

- Активизация участия отраслевых компаний и технического сообщества РФ в работе международных площадок по стандартизации в области ИБ и безопасных ИТ-платформ, прежде всего в нише новой цифровой инфраструктуры (НЦИ).

- Реформа регулирования в области СКЗИ с целью повышения его гибкости и частичного устранения барьеров к более активному рыночному использованию российских решений.

- Разработка нового поколения алгоритмов, стойких к квантовым атакам, на базе имеющейся российской научно-технологической базы в сфере шифрования.



ЦЕНТР
СТРАТЕГИЧЕСКИХ
РАЗРАБОТОК

125009, Москва, ул. Воздвиженка, дом 10
тел.: **(495) 725 78 06, 725 78 50**
e-mail: **info@csr.ru**
web: **csr.ru**