

[Поиск](#)

- [О ПИР-Центре](#)
- [Публикации](#)
- [Научные проекты](#)
- [Образование](#)

[Вход](#)[Версия для печати](#)[Карта сайта](#) | [Обратная связь](#) | [Архив сайта](#)[English](#)

Письмо: Future of Information Security: Global Trends and Scenarios for Russia – New Report of CSR and PIR Center

25.12.2017

Future of Information Security: Global Trends and Scenarios for Russia – New Report of CSR and PIR Center



МОСКВА, 25 ДЕКАБРЯ 2017. ПИР-ПРЕСС — Как развивать цифровую экономику и при этом обеспечить безопасность в контексте трансграничных цифровых рисков и угроз? Центр стратегических разработок опубликовал доклад «Будущее информационной безопасности: глобальные трансформации и сценарии для России», подготовленный направлением ЦСР «Внешняя политика и безопасность» и ПИР-Центром.

Центр стратегических разработок (ЦСР) опубликовал доклад [«Будущее информационной безопасности: глобальные трансформации и сценарии для России»](#), подготовленный направлением ЦСР «Внешняя политика и безопасность» и ПИР-Центром. Автор доклада – консультант ПИР-Центра Олег Демидов, редакторы – директор ПИР-Центра Альберт Зульхарнеев и руководитель направления «Внешняя политика» ЦСР Сергей Уткин. В

обсуждении положений доклада на этапе его подготовки [принимали участие](#) члены [Рабочей группы ПИР-Центра по международной информационной безопасности и глобальному управлению интернетом](#) и другие российские эксперты.

Ключевой вопрос доклада – каким образом развивать цифровую экономику, и цифровые технологии и при этом обеспечить безопасность в контексте трансграничных цифровых рисков и угроз.

В докладе выделены три основные задачи:

- Снижение рисков военно-политического использования информационно-коммуникационных технологий (ИКТ) и формирование основ международно-правового режима ответственного поведения государств в киберпространстве;
- Обеспечение безопасности, стабильности и отказоустойчивости Интернета и инфраструктуры цифровой передачи данных для российских пользователей, бизнеса и государства;
- Обеспечение российских интересов в сфере безопасной цифровой среды, борьбы с компьютерной преступностью, а также развития технологий и рынка информационной

Для каждого направления автором предложены возможные стратегии и конкретные меры, которые осуществляются в зависимости от реализации того или иного сценария развития международной обстановки и технического прогресса.

При разработке решений указанных задач учитывались существующие технологические и политико-правовые условия. Первое – трансграничный характер киберпространства, что делает невозможным комплексное обеспечение безопасности в рамках отдельного государства и за счет лишь собственных ресурсов.

Второе – технологические ограничения по достоверной атрибуции, что снижает возможности выстраивания эффективных международно-правовых механизмов регулирования киберпространства.

Третье – высокие темпы развития цифровых технологий и появления новых угроз снижают эффективный горизонт планирования государственной политики.

Включенность в международные связи и технологические цепочки ставит Россию перед дилеммой: обеспечивать ИТ-безопасность, инвестируя ресурсы в повышение конкурентоспособности своих технологий и бизнес-решений на глобальном рынке, или же делать ставку на снижение зависимости от зарубежных ИТ-экосистем и инфраструктур, создавая их локальные аналоги.

В качестве оптимальных направлений решения поставленных задач автор видит:

- мобилизацию ресурсов частного сектора в управлении вызовами военно-политического использования ИКТ;
- распределение рисков между государством и частным сектором и децентрализацию критически важных инфраструктур;
- адаптацию к нестабильным альянсам и дефициту ресурсов за счет гибкого управления рисками, а также достижение локальных прорывов за счет опережающих решений в развитии концептуально новой правовой базы для борьбы с высокотехнологичной преступностью, разработку стандартов квантовой и постквантовой криптографии, а также стандартизацию сервисов и решений новой цифровой инфраструктуры с упором на безопасность.

Каждое из этих решений должно корректироваться в зависимости от более или менее благоприятной внешнеполитической обстановки.

Подробнее о направлениях работы, стратегиях и конкретных предлагаемых мерах по решению существующих проблем в сфере информационной безопасности читайте в докладе [ЦСР и ПИР-Центра](#).

[Центр стратегических разработок \(ЦСР\)](#) был создан в 1999 г. по инициативе будущего президента России Владимира Путина как площадка для разработки программы развития на ближайшее десятилетие. В 2016 – 2017 гг. по поручению Президента России под руководством Алексея Кудрина ЦСР разработал стратегию развития России на 2018 – 2024 годы.

С программой ПИР-Центра «Глобальное управление интернетом и международная информационная безопасность» можно ознакомиться в ее [разделе на сайте ПИР-Центра](#).

Тел.: +7 (495) 987-19-15

Адрес для писем: Россия, 119019, Москва, а/я 147

ПИР-Центр 2022 год. Все права защищены.
Разработан ИССАрт.

loading

