



ГРАЖДАНСКАЯ ИНИЦИАТИВА
ИНТЕРНЕТ ПОЛИТИКИ

РИСКИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИТ-ОБОРУДОВАНИЯ В КОНТЕКСТЕ ЗАЩИТЫ ЦИФРОВЫХ ПРАВ ГРАЖДАН



ДЕКАБРЬ 2022
Г. БИШКЕК
КЫРГЫЗСКАЯ РЕСПУБЛИКА



ГРАЖДАНСКАЯ ИНИЦИАТИВА
ИНТЕРНЕТ ПОЛИТИКИ

ИССЛЕДОВАНИЕ ПО ЦИФРОВОМУ АВТОРИТАРИЗМУ



ДЕКАБРЬ 2022

Г. БИШКЕК

КЫРГЫЗСКАЯ РЕСПУБЛИКА

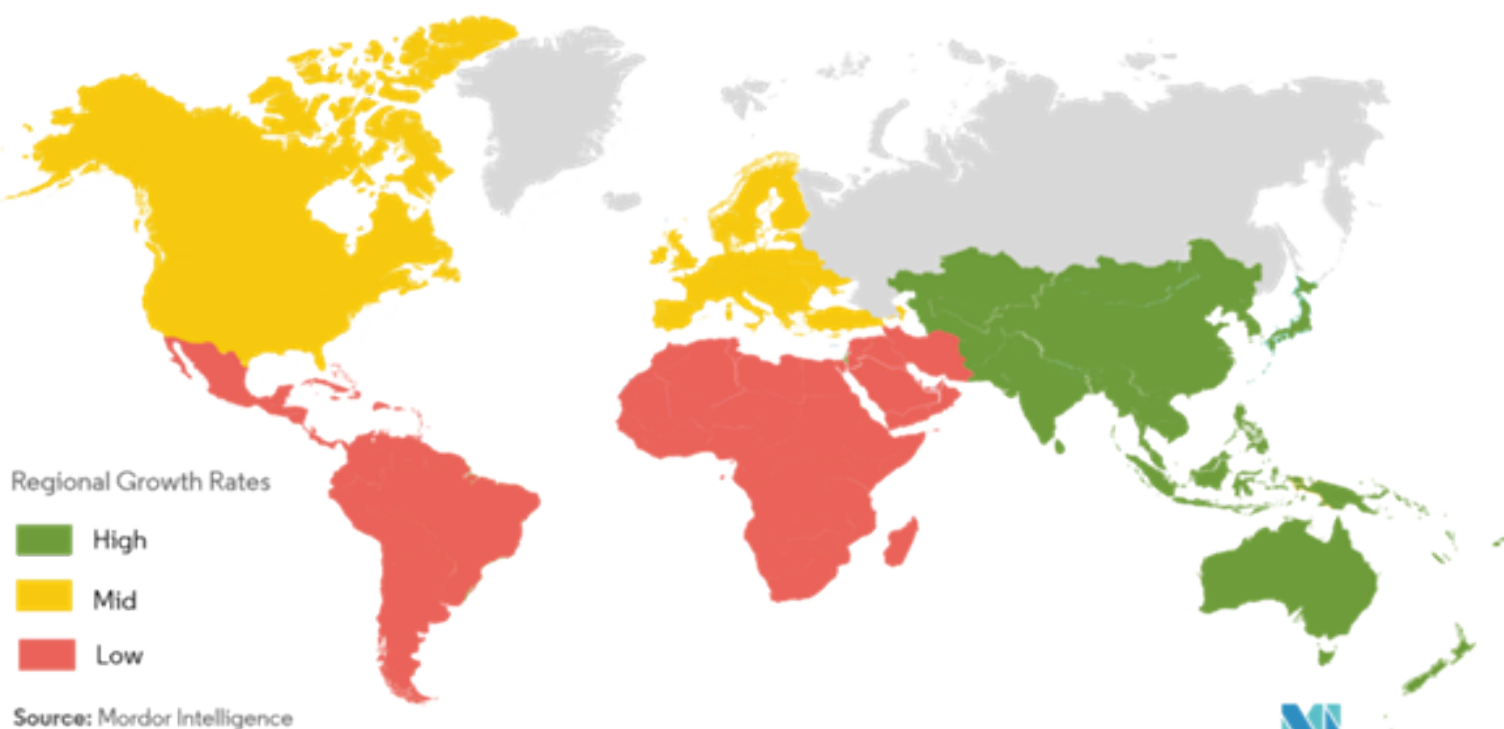
ОГЛАВЛЕНИЕ

География поставок	3
Вычисления, обработка данных, процессорное время, серверы	5
Передача данных, сетевые технологии, коммутация, маршрутизация	6
Хранение данных локальное, сетевое	7
Информационная безопасность, сетевые экраны, защита от угроз, защищённые соединения (аппаратные решения), видеонаблюдение	8
Программное обеспечение системного, прикладного, общего и отраслевого применения	9
Геополитическое влияние	10
Особенности закупок оборудования и программного обеспечения	12
Обзор потенциальных нарушений норм обработки информации	16
Обзор законодательства Кыргызской Республики	19
Выводы	21
Рекомендации	23

ГЕОГРАФИЯ ПОСТАВОК

Кыргызская Республика является 100% импортёром телекоммуникационного, вычислительного оборудования и систем хранения данных, и всех связанных с ними технологий, протоколов обработки или передачи данных. Для обработки информации и решения неспецифичных отраслевых задач потребители Кыргызской Республики также используют тиражируемое программное обеспечение, производимое преимущественно за рубежом. К таким задачам, как правило, относятся проприетарное или свободно-распространяемое системное и прикладное программное обеспечение общего применения: операционные системы, офисные приложения, системы документооборота и обмена сообщениями, системы управления базами данных, программы защиты информации, системы общекорпоративного назначения (кадры, бухгалтерия, логистика и т.д.) и инструменты системного администрирования. Однако, для решения же узко-отраслевых, специфичных для конкретного ведомства, задач в стране сложилась практика заказа индивидуальной разработки программного обеспечения, при этом подавляющее большинство таких продуктов разрабатываются и поддерживаются местными государственными и частными организациями. В этот список можно включить системы управления отраслевыми (ведомственными) реестрами и специфичное программное обеспечение.

Enterprise Server Market - Growth Rate by Region (2019 - 2024)





По оценкам компании **Mordor Intelligence** Кыргызская Республика входит в регион, где в течение пяти лет до 2024 года будет отмечаться рост закупок серверного оборудования и, соответственно, программного обеспечения, систем защиты, хранения и передачи данных к нему. Это обусловлено стремительной цифровизацией как всего макрорегиона в целом, так и Кыргызской Республикой в частности.

Объективно, мировые производители высокотехнологичного оборудования и программного обеспечения, предлагающие свою продукцию в области информационных технологий для свободной продажи, сосредоточены в основном в двух странах — США и Китай — и представлены следующими лидерами по отраслям в порядке убывания популярности:

ВЫЧИСЛЕНИЯ, ОБРАБОТКА ДАННЫХ, ПРОЦЕССОРНОЕ ВРЕМЯ, СЕРВЕРЫ

1.	Dell	США
2.	HP HPE	США
3.	IBM	США
4.	SuperMicro	США
5.	Cisco	США
6.	Oracle	США
7.	Huawei	Китай
8.	Lenovo	Китай
9.	Inspur	Китай
10.	Прочие	Китай

¹ Порядковый номер лидера — наиболее вероятная предполагаемая и условная позиция компании-производителя на рынке Кыргызской Республики, обусловленная относительной популярностью вендора среди заказчиков и ИТ-специалистов. Для каждой отрасли применения (телекоммуникации, крупный бизнес, средний бизнес, государственные ведомства) рейтинг популярности вендоров и их процентные соотношения будут иными.

ПЕРЕДАЧА ДАННЫХ, СЕТЕВЫЕ ТЕХНОЛОГИИ, КОММУТАЦИЯ, МАРШРУТИЗАЦИЯ

1.	Cisco	США
2.	Microtik	ЕС (Латвия)
3.	TP-Link	Китай
4.	D-Link	Тайвань
5.	Huawei	Китай
6.	Brocade	США
7.	ZTE	Китай
8.	HPE	США
9.	ZyXel	Тайвань
10.	Ubiquity	США

ХРАНЕНИЕ ДАННЫХ ЛОКАЛЬНОЕ, СЕТЕВОЕ

1.	QNAP	Тайвань
2.	Dell EMC	США
3.	NetApp	США
4.	HPE	США
5.	Fujitsu	Япония
6.	Hitachi	Япония
7.	Huawei	Китай
8.	Oracle	США
9.	Synology	США
10.	IBM	США

¹ Порядковый номер лидера — наиболее вероятная предполагаемая и условная позиция компании-производителя на рынке Кыргызской Республики, обусловленная относительной популярностью вендора среди заказчиков и ИТ-специалистов. Для каждой отрасли применения (телекоммуникации, крупный бизнес, средний бизнес, государственные ведомства) рейтинг популярности вендоров и их процентные соотношения будут иными.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СЕТЕВЫЕ ЭКРАНЫ, ЗАЩИТА ОТ УГРОЗ, ЗАЩИЩЁННЫЕ СОЕДИНЕНИЯ (АППАРАТНЫЕ РЕШЕНИЯ), ВИДЕОНАБЛЮДЕНИЕ

1.	Cisco	США
2.	HikVision	Китай
3.	Dahua	Китай
4.	Checkpoint	Израиль
5.	Microsoft	США
6.	Fortinet	США
7.	VIPNet	Россия
8.	Palo Alto	США
9.	InfoWatch	Россия
10.	Huawei	Китай

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СИСТЕМНОГО, ПРИКЛАДНОГО, ОБЩЕГО И ОТРАСЛЕВОГО ПРИМЕНЕНИЯ

1.	Microsoft Системное ПО, офисное ПО, ИБ, коммуникации	США
2.	Open Source ПО с открытым исходным кодом	—
3.	1С Управление финансами, кадрами, логистикой	РФ
4.	Отраслевое ПО Разрабатываемое или приобретаемое по требованиям заказчика ПО	(КР)
5.	VMWare Системы виртуализации	США
6.	Kaspersky Системы безопасности и защиты	РФ
7.	Amazon Виртуальные облачные системы	США
8.	Oracle Системы управления базами данных	США
9.	SAP Системы управления предприятием	ФРГ (ЕС)
10.	Veeam Системы управления резервным копированием	США
11.	Zimbra Системы коммуникаций и документооборота	США

ГЕОПОЛИТИЧЕСКОЕ ВЛИЯНИЕ

География стран производителей, выпускающих востребованное в Кыргызской Республике ИТ-оборудование и программное обеспечение, на первый взгляд кажется достаточно конкурентной и обширной. Однако, фактически производство средств обработки информации аппаратного и программного уровня сосредоточено буквально в двух странах — в США и Китае. Другие страны имеют нишевую представительность в списке ИТ-производителей: Израиль традиционно силен в системах обеспечения безопасности, также как и Россия, но в силу особых, отличающихся от общемировых, законодательных требований, предъявляемых к информационной безопасности. Из стран Евросоюза лишь латвийская продукция смогла получить широкое распространение на территории Кыргызской Республики. Японские производители ИТ-оборудования закрепились в нише систем хранения данных.

Учитывая происходящие в мире масштабные геополитические события, к 2023 году уже сформировалось условное двухполярное разделение мировых производителей. С одной — «западной» — стороны сосредоточено подавляющее количество производителей ИТ-оборудования и программного обеспечения, рыночная доля которых может с лёгкостью достигнуть 100% в конкретной отрасли применения. При этом под условным «Западом» подразумеваются государства, которые включены в список недружественных стран Российской Федерации. Вторая же полярность, сформировавшаяся за последние месяцы, представлена странами, не попавшими в этот список, соответственно.

На текущий момент «западные» производители продемонстрировали новые угрозы, которые могут коснуться их потребителей в результате воздействия меняющейся геополитической конъюнктуры. Добросовестные потребители оборудования и программного обеспечения могут столкнуться с непреодолимым препятствием в виде отказа от поставки оборудования, его поддержки или ремонта (**Cisco, IBM, Dell, Nokia и другие**), а также невозможности покупки, обновления или сопровождения программного обеспечения (**Microsoft, Oracle, SAP, Amazon, SWIFT, Adobe, Visa и т.д.**). На примере Cisco Meraki, добросовестный пользователь, находящийся на условной «восточной» стороне, уже столкнулся с принудительным удалённым отключением оборудования этого производителя.

Несколько десятков волн первичных, вторичных и третичных взаимных, одно-, двух- и многосторонних санкций, нарушившие мировые цепи поставок и производства, подкрепляемые политическим давлением на правительства «внеблоковых» государств, в том числе на руководство частных производителей оборудования и программного обеспечения, сформулировали новую парадигму для нейтральных или условно-нейтральных стран, к которым относится и Кыргызская Республика.

Исторически сложившееся макрорегиональное деление сфер продаж и производства международных изготовителей программного обеспечения и оборудования включало Кыргызскую Республику в такие экономические регионы как «Европа и СНГ», «СНГ», «Россия и Центральная Азия». Административным центром этих условных регионов, где размещались представительства зарубежных производителей, традиционно выбирался город Москва. В результате геополитического шторма внутренние потребители КР уже столкнулись с тем, что сроки поставок оборудования в лучшем случае увеличились втрое, а для некоторых позиций — в десять раз.

Помимо задержек с поставкой, вызванных косвенными причинами, которые повлияли на закрытие московских представительств, нарушили логистику и производство, в будущем равновероятно возникновение и прямого влияния на рынок Кыргызской Республики. В случае усиления «реэкспорта» зарубежных (подразумевается, «западных») технологий, оборудования и программного обеспечения российским компаниям, даже не находящимся под прямыми санкциями, Кыргызская Республика рискует столкнуться с тем, что появившиеся с 24 февраля 2022 года экономические ограничения могут быть быстро распространены и на территорию КР. А это, очевидно, существенно затруднит, если сделает вообще возможным, дальнейшую эксплуатацию уже приобретённого «западного» оборудования и программного обеспечения.

ОСОБЕННОСТИ ЗАКУПОК ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Местные потребители останавливают свой выбор на том или ином производителе высокотехнологичного оборудования и программного обеспечения исходя из двух, зачастую взаимоисключающих, критериев:

1. Минимальная закупочная стоимость
2. Высокая (абсолютная) совместимость с имеющейся инфраструктурой

При этом в сложившейся на территории страны практике приобретения оборудования и программного обеспечения нередки ситуации, когда низкое ценовое предложение является решающим фактором вопреки объективным техническим ограничениям. Дальнейшая эксплуатация такого приобретения зачастую оказывается низкоэффективной в силу того, что штатные специалисты не могут его настроить (проинтегрировать), или настраивают минимально-возможный набор функций, или же само оборудование/ПО является принципиально несовместимым с используемой у потребителя информационной инфраструктурой. Противоположной особенностью является и тот факт, что полная совместимость² оборудования и программного обеспечения зачастую возможна только при использовании продукции от одного производителя. А это можно отнести к общему недостатку тендерных технических документов, которые публикуются частными и государственными организациями при закупке телекоммуникационного, вычислительного оборудования или систем хранения данных. В проанализированных за 2022 год публичных документах, содержащих техническое задание к тендеру на приобретения ИТ-оборудования, программного обеспечения или ИТ-услуг, повсеместно содержатся требования к конкретным моделям (версиям, услугам) от конкретных производителей. В редких случаях закупающая организация отражает в тендерной документации широкий диапазон требований, которым мог бы удовлетворять практически любой производитель.

² Совместимостью следует считать следующие особенности эксплуатации:

- модернизация или расширение функциональности, или увеличение эффективности;
- масштабирование или увеличение количества эксплуатируемых единиц в том числе для повышения производительности;
- сопровождение или обновление до следующей версии, оказание услуг технической поддержки, ремонта и восстановления.

Такой подход обусловлен спецификой эксплуатации инфокоммуникационного оборудования и почти всегда связан с уже устоявшимися процессами эксплуатации такого оборудования и программного обеспечения. Процессы администрирования, мониторинга, обслуживания, профилактики и эксплуатации такого оборудования и ПО не стандартизированы и в большинстве случаев полностью зависят от разработанных компанией-производителем процедур, специфичного программного обеспечения и проприетарных сетевых протоколов. В силу этих обстоятельств, аналогичные по своим функциям единицы оборудования с высокой долей вероятности являются несовместимыми для указанных эксплуатационных целей.

С другой стороны, если критерием приобретения оборудования выступает минимальная закупочная цена, то у покупающей организации происходит увеличение совокупной стоимости владения, TCO³.

Структура затрат совокупной стоимости владения, помимо непосредственно закупочной (балансовой) стоимости самого оборудования, включает в себя также все связанные расходы за весь период эксплуатации приобретённого оборудования. Как правило, речь идёт про пять-семь лет. К таким расходам относится:

- 1.** 10% — эксплуатация (пропорциональные траты на монтаж, электроэнергию, охлаждение, пожаробезопасность, охрану, связность);
- 2.** 10% — модернизация и ремонт (замена вышедших из строя запчастей);
- 3.** 20-40% — обслуживание (пропорция от фонда оплаты труда задействованных сотрудников, системных администраторов);
- 4.** 30-60% — сопровождение и поддержка (стоимость ежегодных лицензионных платежей, доработки программного обеспечения, доступа к обновлениям или к службе технической поддержки вендора).

³ Совокупная стоимость владения, или TCO (Total Cost of Ownership) — сумма всех затрат, которые владелец вынужден нести в связи с приобретением программного или программно-аппаратного решения.



Некоторые вендоры⁴, плохо представленные на конкретном рынке, используют следующую тактику вхождения на такой рынок:

1. Существенное занижение закупочной стоимости оборудования и тиражируемого программного обеспечения, ниже себестоимости, для предложения потребителям и участия в тендерах. Предлагаемая цена может составлять до 50%, а то и до 20% от цены прямых конкурентов.

2. Закрепление на рынке за счёт повсеместной закупочной политики «Выигрывает наименьшая цена».

3. Резкое или постепенное повышение ежегодной стоимости сопровождения и поддержки на 100-300% для покрытия убытков от продажи по заниженной стоимости.

⁴ Вендор — это физическое или юридическое лицо, которое производит и поставляет или оказывает логистическое содействие поставке товаров под собственным брендом. Моновендорность — покупка и использование оборудования и программного обеспечения исключительно от одного производителя, одного бренда

Особенности использования инфокоммуникационного оборудования для корпоративных целей конечного заказчика, с одной стороны, в форме моновендорности приводят к тому, что закупающая организация становится «заложником» единственного поставщика, который может испытывать проблемы с логистикой или отсутствием свободных производственных мощностей, а также применять меры экономического давления и шантажа за счёт резкого повышения цен на оборудование и, что особенно часто происходит, услуги сопровождения, поддержки и обновления.

С другой стороны, мультивендорность, представленная пятью-шестью и более производителями, приводит к резкому удорожанию стоимости эксплуатации такого многообразия за счёт усложнения эксплуатации, увеличения количества точек отказа, необходимости оплаты труда специалистов соответствующей квалификации, использования проприетарных систем администрирования и мониторинга, приобретения подписок на техническую поддержку у каждого из вендоров.

Оптимальным же количеством вендоров в составе одной информационной инфраструктуры, сети или информационной системы, оборудование и ПО которых приобретается для выполнения аналогичных функций⁵, является значение в диапазоне от двух до трёх.

⁵ Аналогичные функции — исключительное функциональное свойство оборудования или программного обеспечения, предназначенное для решения какой-то производственной задачи: вычисления (серверы), передача данных (коммутаторы, маршрутизаторы), хранение данных (СХД, ленточные библиотеки), обеспечение безопасности (файрволы, SIEM, IDS/IPS, DLP и т.д.)

ОБЗОР ПОТЕНЦИАЛЬНЫХ НАРУШЕНИЙ НОРМ ОБРАБОТКИ ИНФОРМАЦИИ

В сфере телекоммуникаций и ИТ курсирует множество мифов, полуправды и доказанных случаев, когда защищаемая информация становилась уязвимой или публичной в результате несовершенства оборудования или программного обеспечения. В таких случаях всегда необходимо разделять потенциальные способы реализации угроз, которые могут нарушить конфиденциальность или целостность информации.

Современный ландшафт киберугроз к 2023 году представляет собой следующую триаду, где первое место — наиболее часто реализуемый вектор атаки и нанесения ущерба, а последнее, соответственно, — самые редкие случаи:

1. Человеческий фактор, или ситуации, связанные с умышленными или неосторожными действиями пользователя, среди которых в порядке убывания количества случаев:

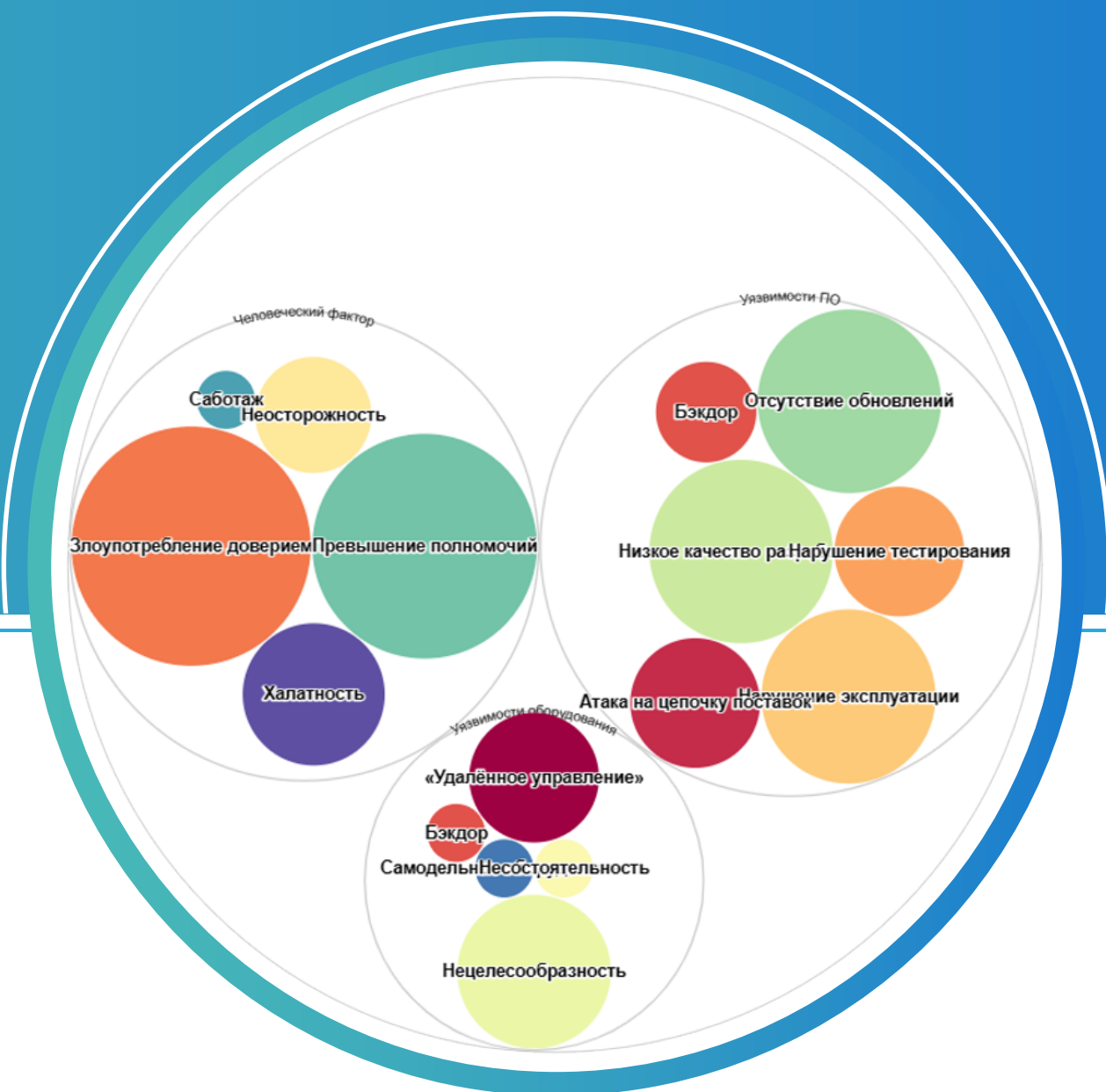
- 1.1.** Злоупотребление доверием и превышение полномочий по личным мотивам
- 1.2.** Превышение полномочий в результате шантажа, подкупа или запугивания
- 1.3.** Неосмотрительность, халатность, игнорирование инструкций
- 1.4.** Неосторожность вследствие низкой компетенции
- 1.5.** Саботаж

2. Уязвимости программного обеспечения:

- 2.1.** ПО, приобретаемое на заказ, своими силами: низкое качество разработки ПО или нарушение процессов жизненного цикла программного обеспечения (тестирование, ввод в эксплуатацию)
- 2.2.** Тиражируемое ПО: слабый контроль за процессами эксплуатации и обновления
- 2.3.** Внедрённые уязвимости в результате атаки на цепочку поставок
- 2.4.** Внедрённые разработчиком уязвимости (бэкдоры)

3. Уязвимости оборудования:

- 3.1.** Самодельные, кустарные конструктивы и приборы
- 3.2.** Конструктивная несостоятельность или нецелесообразность защиты (оборудование из класса Интернета вещей, бытовые приборы с ИТ-компонентом, промышленные датчики, элементы управления SCADA)
- 3.3.** Функционал «Удалённое управление» (IPMI, iLO, DRAC), включая функционал «Software/Cloud-defined»
- 3.4.** Внедрённые разработчиком уязвимости (бэкдоры)



Очевидно, что наибольшее количество рисков, связанных с угрозой нарушения конфиденциальности или целостности информации, возникает в результате действий инсайдеров, или сотрудников эксплуатирующей организации — злоупотребление доверием, превышение полномочий и нарушение процессов эксплуатации программного обеспечения. К сожалению, совершенной защиты от действий внутреннего нарушителя не существует — сотрудник, обязанный работать с защищаемой информацией в рамках должностных обязанностей, является самой уязвимой точкой системы обеспечения информационной безопасности. Поэтому недопущение ущерба в результате инсайдерской атаки до сих пор является нерешённой задачей в мировом масштабе.

Риски внешнего воздействия в результате действий третьих лиц гораздо ниже внутренних рисков. А риск злонамеренного вмешательства зарубежного вендора в процессы обработки информации, осуществляемые с помощью его оборудования или программного обеспечения, является самым минимальным. К счастью, любое внешнее воздействие очень легко минимизировать или же вовсе исключить за счёт изолирования систем обработки критичной информации от публичных сетей передачи данных.

Тиражируемое программное обеспечение, ИТ-оборудование известных производителей находится под микроскопом мирового сообщества экспертов, инженеров, профессионалов и любителей в отрасли информационной безопасности и технологий. Имеющиеся в распоряжении практически любого ИТ-специалиста технические средства позволяют определить наличие паразитной или вредоносной активности, которая могла бы быть тайно реализована в поставляемом на рынок оборудовании или программном обеспечении. В случае, если в программно-аппаратном комплексе предусмотрен необъявленный публично функционал, позволяющий производителю скрытно управлять устройством или перехватывать обрабатываемую на устройстве информацию, то это возможно только при подключении такого устройства к сети Интернет. При этом подобная сетевая активность неизбежно будет обнаружена при помощи несложных средств и даже в результате случайного обнаружения в составе корпоративной сети, что приведёт к разоблачению такого производителя и полностью подорвёт доверие к любым выпускаемым устройствам или программному обеспечению.

ОБЗОР ЗАКОНОДАТЕЛЬСТВА КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Законодательство Кыргызской Республики, регулирующее вопросы применения информационных технологий, оборудования и программного обеспечения, не ставит своей целью обеспечение защиты прав и интересов гражданина. Во главу угла поставлена защита преимущественно государственной информации от внешних угроз, в том числе и «от гражданина». Способы обработки и защиты данных, находящихся в ведении частных организаций, не регулируются вовсе⁶.

В нормативно-правовом поле Кыргызской Республики не существует ни одного действующего на момент проведения исследования документа или нормы, которые бы так или иначе обеспечивали подлинную защиту персональной информации, в том числе биометрических данных. Несмотря на усилия недавно созданного Государственного агентства по защите персональных данных, ни одна из принятых норм регулятивного воздействия пока ещё не заработала в полную силу и в масштабе всей страны.

Общим недостатком законодательного подхода в Кыргызской Республике в области защиты информации является отсутствие норм, обеспечивающих прозрачность и подотчётность. Особенностью реализации процесса обеспечения информационной безопасности является независимое подтверждение его эффективности. Процесс информационной безопасности — это не некий результат, которого нужно достичь, а совокупность циклично выполняемых действий, направленных на выявление, пресечение и профилактику инцидентов информационной безопасности. И эффективность процесса обеспечения информационной безопасности достигается за счёт регулярного подтверждения, что все необходимые действия выполняются полностью и своевременно. В современных реалиях зачастую и сам первый руководитель государственного органа не в состоянии определить, насколько эффективно обеспечена информационная безопасность в его ведомстве, так как вынужден полагаться на отчёты специалистов информационной безопасности, которые, в свою очередь, не мотивированы сообщать о собственных упущениях в работе

⁶ За исключением коммерческих банков и частных микрофинансовых организаций, регулируемых постановлениями НБКР.

или злоупотреблениях, несмотря на то, что Постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 762 предусматривается проведение внутреннего и/или внешнего аудита информационной безопасности, однако эти нормы не имеют подкрепления и не исполняются.

Действующие законодательные нормы также не способствуют защите интересов организаций-покупателей. Поставляемое на рынок КР ИТ-оборудование обязано пройти лишь одну проверку, предусмотренную Техническим регламентом ЕАЭС ТР ТС 020—2011 на предмет электромагнитная совместимости, который регулирует сугубо физические аспекты обеспечения безопасности окружающей среды, электросетей и радио-эфира.

Пункт 80 Постановления ПКР №762 «Системное программное обеспечение предоставляется с открытым исходным кодом» утратил силу с выходом постановления Кабинета Министров КР от 31 января 2022 года № 45. А пункт 82 того же Постановления о том, что системное программное обеспечение должно поддерживаться сообществом (ассоциацией) разработчиков или проходить экспертизу/сертификацию программного кода, фактически не применяется.

ВЫВОДЫ

1. Потребителям Кыргызской Республики невозможно избежать зависимости от внешних поставщиков оборудования и программного обеспечения. Зависимость от поставщиков программного и программно-аппаратного обеспечения будет сохраняться до тех пор, пока их полноценные аналоги не будут разрабатываться и производиться на территории страны.

2. Моновендорность (использование оборудования и ПО от одного производителя) всегда приводит к абсолютной зависимости. Международные санкции, сбои в логистике, аварии и забастовки на заводах производителя, необоснованное завышение цен на сопровождение, уход с местного рынка или банкротство производителя — все эти ситуации равновероятны и неподвластны потребителю.

3. Мультивендорность — обратная сторона моновендорности, возникающая при использовании однотипного оборудования, произведённого тремя и более различными производителями. В этом случае организация-потребитель сталкивается с удорожанием совокупной стоимости владения инфраструктурой, вынужденно оплачивая стоимость технической поддержки каждому из производителей, гонорары и заработную плату отдельным специалистам. Стоимость эксплуатации будет увеличиваться за счёт необходимости использования индивидуально-разрабатываемых систем мониторинга и администрирования, а также относительно высоких периодов восстановления в случае аварий из-за заведомо несовместимых проприетарных протоколов и системного ПО, применяемого различными вендорами.

4. Смена вендора — непростой процесс. Процесс миграции с типового оборудования — серверы и коммутаторы — в большинстве случаев является достаточно предсказуемым, технически несложным, хотя и трудозатратным. Но в случае с «интеллектуальным» оборудованием и программным обеспечением миграция к другому вендору в отдельных случаях может быть фактически невозможной. К такому «интеллектуальному» оборудованию всегда относятся

программно-аппаратные решения, в котором аппаратная часть имеет наименьшую ценность, а основной и наиболее ценный функционал реализован за счёт программных (и, как правило, проприетарных) алгоритмов: маршрутизаторы, системы хранения данных, системы информационной безопасности. Системное или прикладное программное обеспечение само по себе всегда является «интеллектуальным» продуктом, ценность которого заключается в наработанном пользовательском опыте и высокому соответствию решаемым на предприятии задачам, в силу чего замена устоявшегося в отрасли или в конкретном ведомстве программного обеспечения — не то, чтобы невозможная, но близкая к невозможной ситуация.

5. Геополитическая ситуация может сильно повлиять на возможности внутренних потребителей эксплуатировать зарубежное оборудование и программное обеспечение в силу разрушения логистики, производства или введения прямых или косвенных санкций.

6. У производителей тиражируемого программного обеспечения и оборудования нет технической возможности внедрять бэкдоры и иные скрытые возможности оборудования для тайного получения информации без последующего неминуемого разоблачения.

7. Наибольшая угроза нарушения конфиденциальности и целостности критической информации, персональных данных граждан проистекает от действий внутренних сотрудников.

8. Риски нарушения конфиденциальности и целостности информации в результате воздействия третьих лиц возрастают в тех организациях, где отсутствуют или нарушены процессы обеспечения информационной безопасности.

9. Законодательство КР в вопросах обеспечения прав граждан и соблюдения информационной безопасности не подкреплено нормами, которые бы обеспечивали независимое подтверждение эффективности обеспечения информационной безопасности.

10. Имеющиеся нормы, направленные на защиту интересов организаций-потребителей, не исполняются.

РЕКОМЕНДАЦИИ

Для снижения зависимости от зарубежных производителей программного обеспечения и оборудования:

1. Однотипное оборудование должно быть представлено как минимум двумя различными вендорами, но не более трёх.
2. Юрисдикция производителей должна быть географически диверсифицирована в пропорции, близкой к 50/50, и распределена между «западными» и «восточными» производителями, соответственно.
3. Применение программного обеспечения, условия поставки которого не предусматривают доступ к исходным кодам с надлежаще подготовленной сопроводительной документацией, должно быть минимизировано.
4. Решения в пользу внедрения программного обеспечения, распространяемого с открытым исходным кодом и по открытым лицензиям, должны поощряться.
5. Решения о заказе разработки специфичного программного обеспечения должны быть основаны на стоимостном анализе совокупной стоимости владения в течение как минимум пяти лет, подтверждены анализом с применением метода «затраты/экономический эффект от внедрения», подкреплены анализом наличия уже разработанных аналогов с открытым исходным кодом.

Для обеспечения защиты информации при использовании оборудования и программного обеспечения любого уровня доверия:

6. Исключить техническую возможность бесконтрольного подключения оборудования и программного обеспечения, обрабатывающего критичную информацию, к публичным сетям передачи данных.
7. (для государственных органов) Обеспечить эффективное функционирование процессов информационной безопасности в соответствии с требованиями ППКР №762.
8. (для частных организаций, кроме финансово-кредитных учреждений) Способствовать скорейшему завершению разработки, утверждению и вступлению в силу законодательных инициатив Госагентство по защите персональных данных.

Для совершенствования законодательной базы и защиты прав граждан

9. Повысить прозрачность и подотчётность департаментов информационной безопасности за счёт независимого внутреннего или внешнего подтверждения эффективности процессов обеспечения информационной безопасности.
10. Ввести ответственность за неисполнения уже принятых норм в области защиты информации и прав граждан.



ГРАЖДАНСКАЯ ИНИЦИАТИВА ИНТЕРНЕТ ПОЛИТИКИ



ул. Рыскулова 79-Б
3 Этаж Офис №13



+996 312 54 04 40



info@gipi.kg



@internet_policy



+996 770 700 300



internetpolicy.kg