Укрепление доверия и безопасности при использовании ИКТ в странах СНГ

Статья рекомендована А.А. Стрельцовым 20.08.2016.

Татту МАМБЕТАЛИЕВА
Директор Общественного фонда «Гражданская инициатива интернет-политики»

Артем ГОРЯЙНОВ
Старший научный сотрудник, заместитель директора по информационным технологиям Общественного фонда «Гражданская инициатива интернет-политики»

Аннотация
В данной статье предпринимается попытка провести сравнительный анализ выполнения плана действий ВВУИО в сфере укрепление доверия и безопасности при использовании ИКТ в странах СНГ. Эмпирической основой служат данные, собранные Национальным инфокоммуникационным холдингом «Зерде», базовой организацией государств – участников СНГ, которая осуществляет методическое и организационно-техническое обеспечение работ в области информационно-коммуникационных технологий.

Ключевые слова:
ВВУИО, СНГ, доверие и безопасность в сфере ИКТ, электронные транзакции, киберпространство, кибербезопасность, информационная безопасность.

Усиление безопасности и повышение доверия при использовании ИКТ является одним из важных факторов на пути развития информационного общества. В Плане действий ВВУИО этому направлению уделено значительное внимание. Имеются в виду вопросы сетевой безопасности, управления безопасностью данных, защиты частной жизни, прав пользователей, безопасности электронных транзакций, включая аутентификацию электронных документов и защиту от спама. Важно отметить, что в План действий ВВУИО изначально было заложено требование соблюдения баланса: с одной стороны, здесь перечисляются меры по обеспечению безопасности, с другой — говорится о необходимости формирования доверия пользователей к ИКТ. Основной целью этого направления является выстраивание схемы, в рамках которой эти две стороны взаимно усиливают друг друга.

В Обзоре ЮНКТАД по выполнению решений ВВУИО за десятилетний период была подтверждена важность безопасности и доверия, отмечалась необходимость разработки систем оценки готовности стран с точки зрения различных аспектов обеспечения безопасности и доверия при использовании ИКТ. Отмечается отсутствие в настоящее время единого определения термина «кибербезопасность».

Согласно Рекомендации X.1205 МСЭ-Т, «кибербезопасность — это набор средств, стратегии, принципы обеспечения безопасности, гарантии безопасности, руководящие принципы, подходы к управлению рисками, действия, профессиональная подготовка, практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя. Ресурсы организации и пользователя включают подсоединенные компьютерные устройства, персонал, инфраструктуру, приложения, услуги, системы

электросвязи и всю совокупность переданной и/или сохраненной информации в киберсреде. Кибербезопасность состоит в попытке достижения и сохранения свойств безопасности у ресурсов организации или пользователя, направленных против соответствующих угроз безопасности в киберсреде. Общие задачи обеспечения безопасности включают следующее: доступность; целостность, которая может включать аутентичность и неотказуемость; конфиденциальность».

Эксперты отмечают, что определение кибербезопасности МСЭ не охватывает полного спектра угроз при использовании ИКТ, в частности угрозы безопасности детей. Многие виды злоупотреблений в сфере ИКТ являются неспецифичными для интернета и могут решаться только в тесном сотрудничестве всех заинтересованных сторон, включая техническое сообщество, правоохранительные органы и гражданское общество. Одной из проблем на пути успешного межгосударственного взаимодействия является отсутствие согласованного общего терминологического пространства, позволяющего однозначно толковать понятия в национальных, региональных и глобальных документах, касающихся кибербезопасности. В межгосударственных соглашениях, используемых на пространстве СНГ, термин «кибербезопасность» не получил широкого распространения, чаще применяется термин «информационная безопасность», подразумевающий более пространное толкование. Например, в проекте Соглашения о сотрудничестве государств — участников СНГ в области обеспечения информационной безопасности он трактуется как состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве, указывается на наличие угрозы информационного терроризма наряду с информационной преступностью и разработкой и применением информационного оружия. Сходные определения используются в деятельности ОДКБ и ШОС.

Сравнительный анализ деятельности в сфере обеспечения доверия и безопасности при использовании ИКТ в государствах — участниках СНГ

В рамках Глобальной программы кибербезопасности МСЭ была проведена оценка уровня кибербезопасности в странах — членах МСЭ. Оценка проводилась по пяти показателям: правовые меры, технические меры, организационные меры, развитие потенциала и международное сотрудничество, на основе которых был сформирован композитный индекс (рис. 1).

Первое место в рейтинге занимает Азербайджан, за ним с небольшим отрывом следует Россия. Из приведенной гистограммы видно, что страны Центральной Азии существенно отстают от большей части стран европейской части СНГ.

Анализируя значения отдельных компонентов индекса для стран СНГ (табл. 1), приходишь к выводу, что с точки зрения развития правовой базы для обеспечения кибербезопасности лидирует Россия с максимальным значением 1, что достигается благодаря четкому распределению обязанностей между государственными органами по вопросам безопасности и повышения доверия при использовании ИКТ. Напротив, самые низкие значения индекса демонстрируют Армения и Кыргызстан.

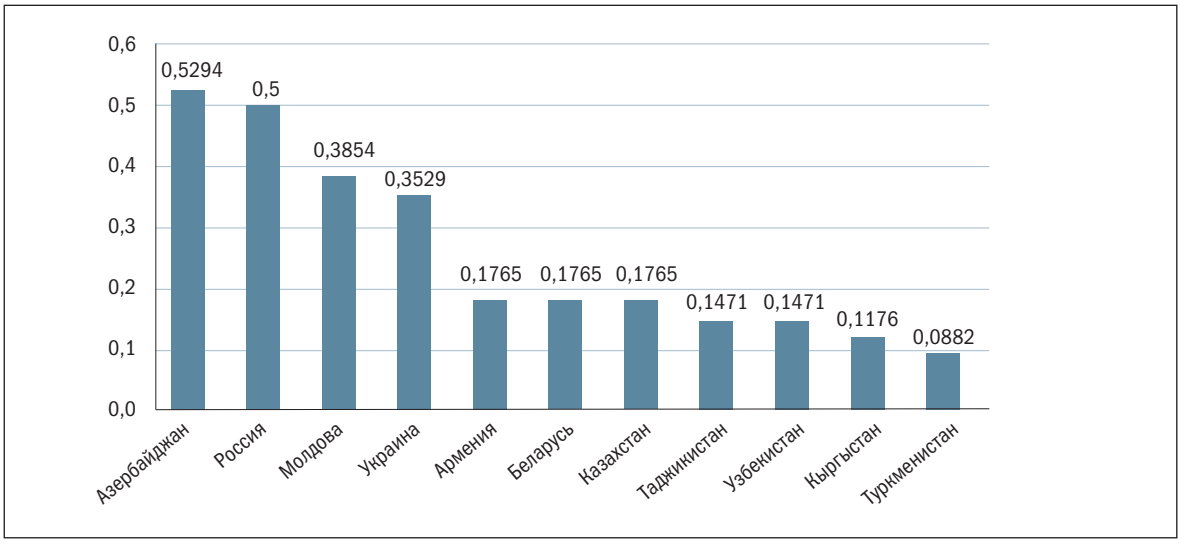

Рис. 1. Глобальный индекс кибербезопасности в странах СНГ, 2014 г.
Источник: [6]

Страны СНГ	Правовые вопросы	Тех. вопросы	Орг. вопросы	Создание потенциала	Сотрудничество	Индекс	Рег. рейтинг
Азербайджан	0,7500	0,5000	0,5000	0,5000	0,5000	0,5294	1
Россия	1,0000	0,3333	0,5000	0,3750	0,5000	0,5000	2
Молдова	0,7500	0,5000	0,2500	0,2500	0,3750	0,3824	3
Украина	0,7500	0,3333	0,2500	0,1250	0,5000	0,3529	4
Армения	0,5000	0,5000	0,0000	0,0000	0,1250	0,1765	5
Беларусь	0,7500	0,3333	0,0000	0,0000	0,1250	0,1765	5
Казахстан	0,7500	0,3333	0,0000	0,0000	0,1250	0,1765	5
Таджикистан	0,7500	0,0000	0,0000	0,0000	0,1250	0,1471	6
Узбекистан	0,7500	0,1667	0,0000	0,0000	0,1250	0,1471	6
Кыргызстан	0,5000	0,0000	0,0000	0,0000	0,2500	0,1176	7
Туркменистан	0,7500	0,0000	0,0000	0,0000	0,0000	0,0882	8

Табл. 1. Глобальный индекс кибербезопасности для стран СНГ, 2014 г.
Источник: [6]

В техническом отношении, согласно данным индекса, наиболее подготовленными оказались Азербайджан, Армения и Молдова с индексом 0,5, что заметно выше среднемирового значения (0,27). В организационных вопросах, касающихся принимаемых мер по обеспечению кибербезопасности, первые места занимают Азербайджан и Россия. Лидером среди стран СНГ в создании потенциала стал Азербайджан, запустив целый ряд проектов по кибербезопасности с использованием передовых практик, основанных на международных

принципах, подготовке национальных стандартов и организации подготовки кадров в этой области. В разделе сотрудничества в первых рядах оказались Азербайджан, Россия и Украина.

Из приведенной таблицы видно, что самыми слабыми звеньями на пространстве СНГ являются вопросы организационного характера и создания потенциала, причем в большинстве стран они никак не решаются. Сильной стороной является правовое обеспечение вопросов кибербезопасности, которыми занимаются во всех без исключения странах СНГ.

Национальным инфокоммуникационным холдингом «Зерде», базовой организацией государств-участников СНГ, осуществляющей методическое и организационно-техническое обеспечение работ в области информационно-коммуникационных технологий, было проведено полномасштабное исследование, основные результаты которого изложены в отчете «Информационное общество в странах СНГ: анализ развития информационного общества в странах — участниках СНГ по приоритетным направлениям Плана действий Всемирной встречи на высшем уровне по вопросам информационного общества». Представленный здесь анализ базируется на исследованиях, легших в основу указанного отчета.

Одним из важных элементов организационных мер в обеспечении кибербезопасности государства является последовательно проводимая политика и наличие государственных программ, направленных на принятие мер в целях ее развития и укрепления. Из анализа государственных программ в сфере ИКТ (рис. 2) видно, что наиболее проработаны разделы по информационной безопасности в государственных программах Азербайджана, Казахстана и России, что в целом подтверждается лидирующим положением Азербайджана и России в рейтинге глобального индекса кибербезопасности. Самые слабые позиции у Армении, Таджикистана и Украины, несмотря на то, что дискуссии и работа в этом направлении в них ведутся с разной степенью интенсивности.

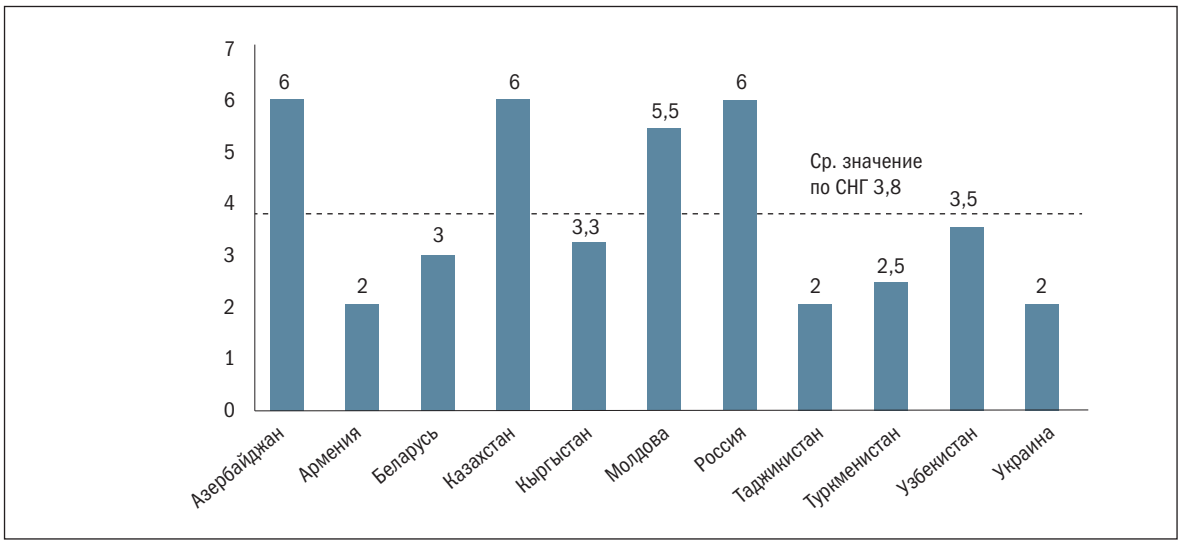

Рис. 2. Наличие и проработанность разделов, посвященных информационной безопасности в государственных программах в сфере ИКТ

Источник: Расчеты Национального инфокоммуникационного холдинга «Зерде» на основе данных экспертных опросов

Помимо наличия в государственных программах разделов по кибербезопасности, немаловажным фактором успеха является соответствующая современным требованиям нормативная правовая база и ее исполнение. Анализ эффективности нормативно-правового регулирования информационной безопасности (рис. 3) позволяет заключить, что в целом эффективность законодательной базы следует трендам, представленным на рисунке 2. Сильное отставание от значений, представленных на рисунке 2, как в случае Молдовы, может объясняться задержками в выполнении государственных программ, направленных на повышение эффективности законодательного регулирования в области кибербезопасности.

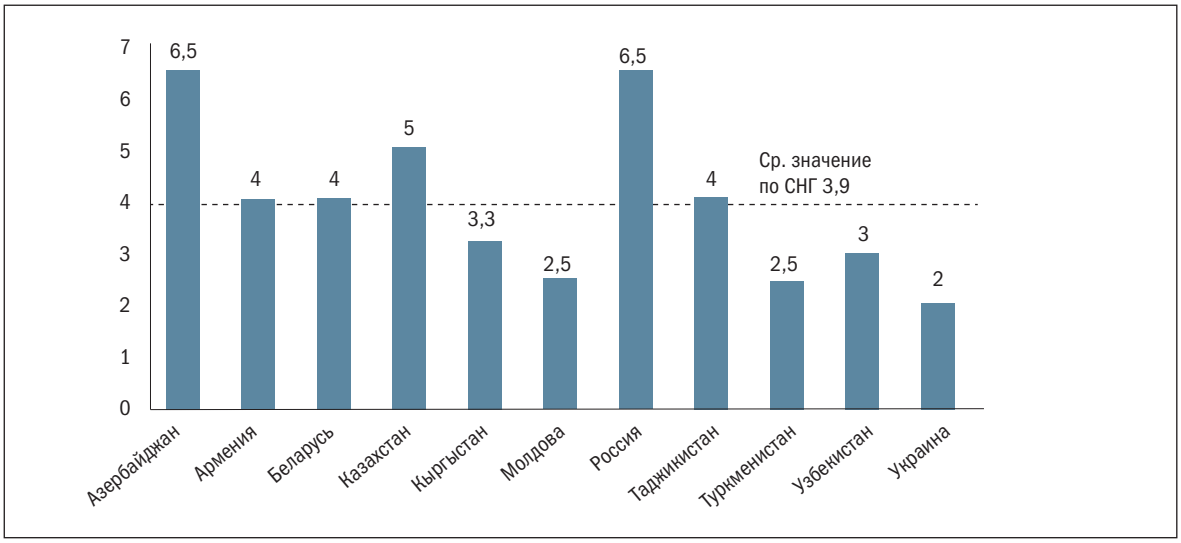

Рис. 3. Эффективность нормативного правового регулирования информационной безопасности

Источник: Расчеты Национального инфокоммуникационного холдинга «Зерде» на основе данных экспертных опросов

Важной частью построения информационного общества является развитие электронных услуг и в целом электронных коммуникаций. Идентификация пользователя и стороны, оказывающей услугу, становится одним из условий обеспечения доверия к электронным транзакциям. В первую очередь речь идет о развитии электронных методов аутентификации, обеспечении безопасности их инфраструктуры. Немаловажным фактором является доступность методов для бизнеса и граждан. На рисунке 4 представлена сравнительная картина развития электронных методов аутентификации в странах СНГ.

На первых местах по данному показателю оказались Азербайджан и Казахстан. В обеих странах действуют порталы электронного правительства и центры выдачи электронной цифровой подписи (ЭЦП). В Азербайджане был запущен проект мобильной ЭЦП «Azan imza», благодаря которому существенно повысилась доступность электронных услуг для пользователей и в очень короткие сроки число пользователей ЭЦП увеличилось. Большая работа по продвижению ЭЦП была проделана в Казахстане, где количество действующих ЭЦП по информации Национального удостоверяющего центра РК на сентябрь 2016 г.

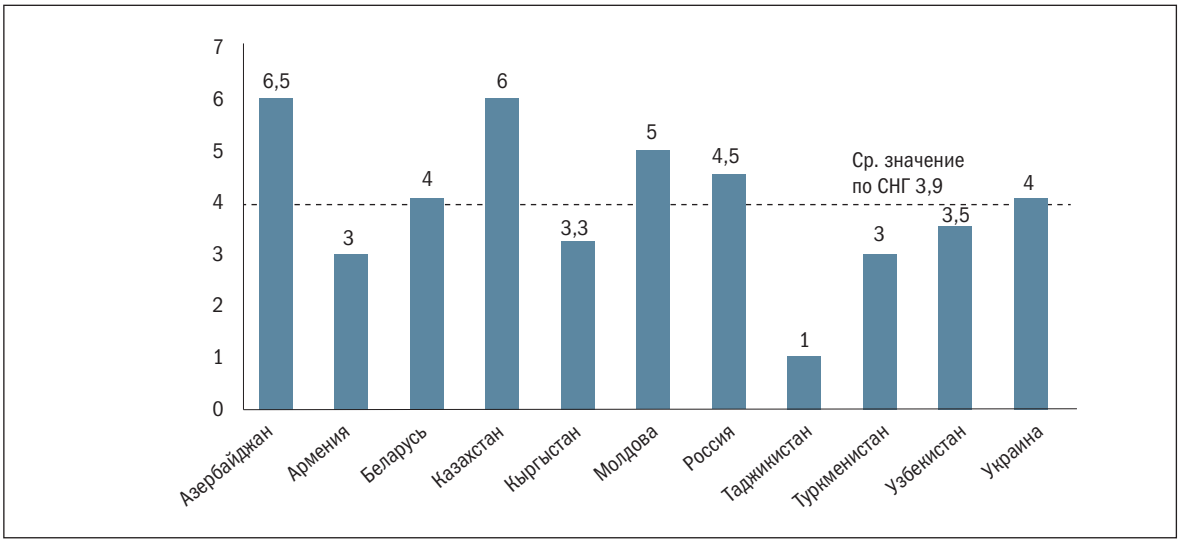

Рис. 4. Развитие электронных методов аутентификации

Источник: Расчеты Национального инфокоммуникационного холдинга «Зерде» на основе данных экспертных опросов.

составило более 3,8 млн. регистрационных свидетельств (сертификатов). Одним из показателей успешности опыта Казахстана является количество сертификатов, выданных физическим лицам, которое почти в 10 раз превышает значение этого показателя для юридических лиц, что свидетельствует о широком вовлечении общества в процессы предоставления и использования электронных услуг.

Значения ниже среднего по СНГ зафиксированы в Армении, Кыргызстане, Таджикистане, Туркменистане и Узбекистане, в которых электронные методы аутентификации и, соответственно, электронные услуги не получили должного распространения ввиду недостаточности технической инфраструктуры и необходимой поддержки со стороны государства.

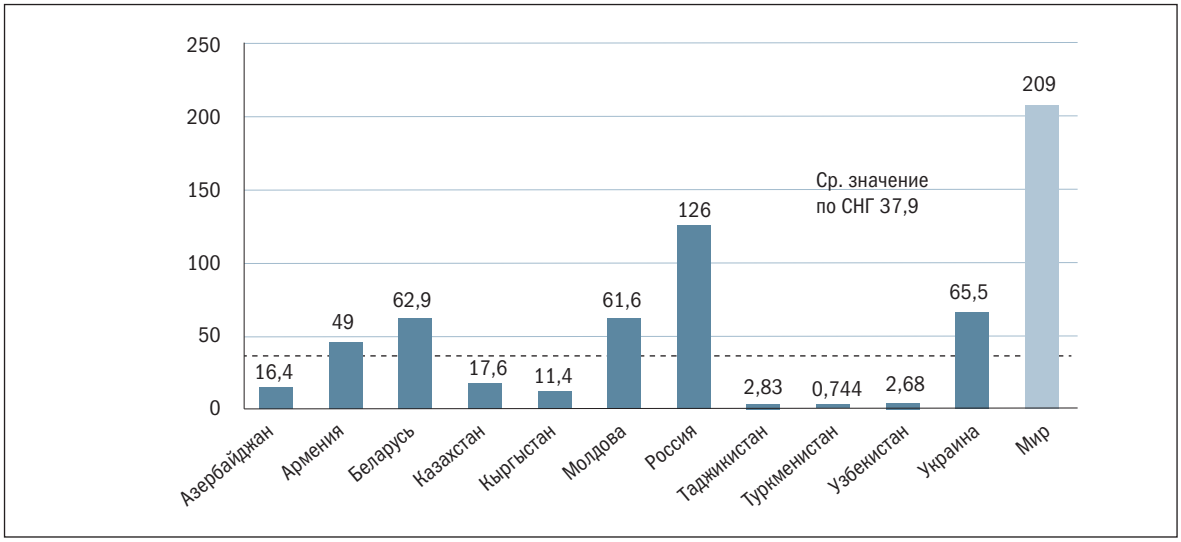

Рис. 5. Количество защищенных интернет-серверов на миллион населения

Источник: [8]

Еще одним важным показателем успешного развития электронной коммерции является количество защищенных интернет-серверов в расчете на миллион населения. Защищенными считаются серверы, в которых для электронных транзакций используется шифрование. Как видно из рисунка 5, составленного на основе данных Всемирного Банка, среди стран СНГ лидерство удерживает Россия. Тем не менее ее показатель значительно уступает среднемировому.

Помимо России, уровень выше среднего по СНГ зафиксирован в Армении, Беларуси, Молдове и на Украине. Все страны Центральной Азии и Азербайджан в этом рейтинге значительно от него отстают. Необходимо отметить, что показатель количества защищенных интернет-серверов входит в различные индексы развития электронной коммерции, к примеру, в Индекс готовности к электронной торговле «предприятие–потребитель» (B2C) ЮНКТАД, поэтому он сильно влияет на положение страны в рейтинге. Низкие показатели могут говорить о недостаточно развитой среде для электронной коммерции, включая и технические вопросы, и регуляцию.

Подготовка квалифицированных кадров в области информационной безопасности и повышение уровня готовности работников бюджетной сферы и государственных служащих являются одним из двигателей успешного развития сферы электронных государственных услуг, обеспечения их безопасности и повышения доверия к ним населения.

На рисунке 6 показаны результаты сравнения государств — участников СНГ по показателю наличия и проработанности мероприятий, нацеленных на подготовку и переподготовку работников бюджетной сферы в области кибербезопасности. Самые высокие значения данного показателя — у России, где в целом предъявляются очень высокие требования к квалификации госслужащих и работников бюджетных учреждений. Не на много отстает от лидера Молдова, реализовавшая успешное сотрудничество с эстонской Академией электронного управления по подготовке государственных служащих в области

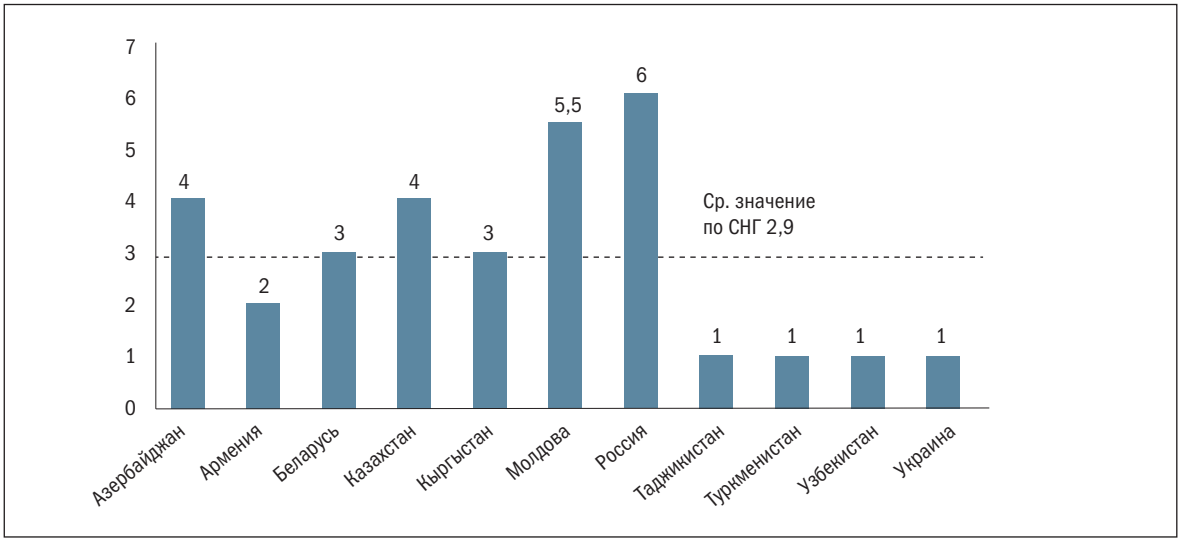

Рис. 6. Наличие и проработанность мероприятий, нацеленных на подготовку и переподготовку работников бюджетной сферы по вопросам информационной безопасности

Источник: Расчеты Национального инфокоммуникационного холдинга «Зерде» на основе данных экспертных опросов

кибербезопасности и проводящая кампании по повышению информированности населения в этих вопросах.

Показатели выше среднего демонстрируют Азербайджан и Казахстан. Центр электронной безопасности при Министерстве связи и высоких технологий Азербайджанской Республики занимается координацией деятельности субъектов информационной инфраструктуры в сфере кибербезопасности, информированием на уровне страны о существующей и возможной электронной опасности, просвещением населения, частных и других структур и оказанием им методической помощи. В Казахстане при канцелярии премьер-министра создано государственное учреждение «Центр подготовки и повышения квалификации специалистов в области информационной безопасности».

Самый низкий уровень по показателю подготовки бюджетных кадров в области кибербезопасности зафиксирован в Таджикистане, Туркменистане, Узбекистане и на Украине, их значения по этому показателю заметно отстают от среднего по СНГ. Это говорит о недостаточном внимании со стороны этих государств к вопросам безопасности в киберпространстве, в то время как создание кадрового потенциала является неотъемлемым условием повышения киберпотенциала государства.

* * *

В СНГ в рамках реализации межгосударственных программ достаточно большое внимание уделяется информационной безопасности. Некоторые страны Содружества параллельно участвуют в различных инициативах мирового масштаба. Вместе с тем, учитывая глобальный характер сети Интернет и угроз кибербезопасности, отсутствие единой общепризнанной терминологии, в рамках которой возможно полномасштабное глобальное взаимодействие по противодействию киберугрозам, представляет собой достаточно серьезное препятствие. Активизация усилий по выработке такой терминологии в рамках мандата ООН, в частности МСЭ, по признанию ее всеми странами позволит облегчить сотрудничество в общемировом масштабе. По-видимому, всем государствам — членам СНГ можно рекомендовать усилить взаимодействие с МСЭ в рамках Глобальной инициативы по кибербезопасности, проработать терминологические вопросы и принять меры по гармонизации соответствующих разделов законодательства.

Несмотря на то, что все страны СНГ предпринимают шаги с целью обеспечения информационной безопасности, особенно в правовом поле, между странами сохраняется выраженное цифровое неравенство, в том числе в области реализуемых государственных программ и эффективности законодательного регулирования. Необходимым шагом по преодолению такого неравенства должна стать подготовка национальных стратегий в области кибербезопасности, основанных на лучших зарубежных и международных аналогах, с обязательным включением пункта о систематизации законодательной базы и приведении ее в соответствие с принятыми обязательствами в рамках международных соглашений.

Для развития электронной коммерции и полноценного включения в нее как можно большей части населения необходимо создать условия для

использования методов электронной аутентификации, в том числе обеспечив их доступность для широких слоев населения.

Органам государсвенной власти, ответственным за формирование политики кибербезопасности, рекомендуется, основываясь на международном опыте, проработать и принять национальные стратегии кибербезопасности с планом действий, учитывающим организационно-технические мероприятия и отражающим современное состояние технологического развития. Процесс проработки стратегии должен проходить с участием и учетом мнений всех заинтересованных сторон, включая бизнес и гражданское общество. Стратегия должна отражать прозрачность и подотчетность процесса обеспечения кибербезопасности и учитывать необходимость обеспечения доверия, включая защиту персональных данных и охрану частной жизни.

Слабым местом практически всех стран СНГ являются вопросы повышения потенциала в сфере кибербезопасности. В связи с этим можно рекомендовать в проекте Стратегии сотрудничества государств — участников СНГ в построении и развитии информационного общества на период до 2025 г. уделить этому вопросу приоритетное внимание. Особо необходимо отметить необходимость подготовки специалистов не только технической специализации, но также организационной и правовой. План действий по реализации Стратегии должен включать пункты по организации мероприятий по подготовке и повышению квалификации специалистов, обмену опытом.

Важным моментом является повышение грамотности государственных служащих и осведомленности всего населения в области кибербезопасности. Государственным органам, ответственным за кадровый потенциал, рекомендуется организовывать курсы по повышению квалификации государственных служащих в области кибербезопасности. Национальные стратегии кибербезопасности должны предполагать повышение осведомленности населения в этих вопросах, включая защиту персональных данных. Обеспечение зашиты персональных данных граждан и неприкосновенности частной жизни — непременное условие обеспечения доверия людей к информационно-коммуникационным технологиям. В рамках конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных предусматривается создание уполномоченного государственного органа по защите персональных данных. Подобная практика хорошо зарекомендовала себя во многих странах. Обеспечение прозрачности доступа к персональным данным также является немаловажным фактором в процессе укрепления доверия граждан к использованию ИКТ.

Работа выполнена в рамках проекта «Информационное общество в странах СНГ: Анализ развития информационного общества в государствах — участниках СНГ по приоритетным направлениям Плана действий Всемирной встречи на высшем уровне по вопросам информационного общества». Астана, 2015-2016.